**Практическая работа**

**«Работа с антивирусными программами. Установка и настройка антивируса»**

ЦЕЛИ РАБОТЫ:

1. Ознакомление с видами антивирусных программ.

2. Научиться устанавливать и настраивать антивирусное ПО.

3. Научиться с помощью антивирусного программного обеспечения обнаруживать и устранять последствия вирусного заражения.

4. Научиться работать с Защитником Windows.

ОБОРУДОВАНИЕ: ПК, Windows 10, Антивирусная программа Avast.

ВРЕМЯ ВЫПОЛНЕНИЯ: 90 минут

КРАТКАЯ ТЕОРИЯ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ:

**Антивирусом** называют специализированную программу, в функции которой входит обнаружение и удаление вредоносных приложений на компьютере. Кроме этого антивирусы выполняют функцию восстановления зараженных файлов.

Большинство компаний, разрабатывающих антивирусное программное обеспечение, выпускают свою продукцию под операционные системы Windows. Связано это с тем, что большая часть вирусных программ разрабатывается именно под эту платформу, просто потому что Windows, это наиболее популярная и наиболее распространенная система.

**Вредоносными программами** уголовное законодательство Российской Федерации понимает программы, специально созданные для нарушения нормального функционирования компьютерных программ.

Под нормальным функционированием понимается выполнение определенных в документации на программу операций.

В Российской Федерации отношения производителей и распространителей вирусов с обществом регулируются статьей 273 Уголовного кодекса, гласящей следующее: «Создание программ для ЭВМ или внесение изменений в yже существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации или копированию информации, нарушению рабов ЭВМ, систем ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами наказывается лишением свободы на срок до 3-х лет со штрафом от 200 до 500 минимальных размеров оплаты труда…».

Аналогичные законы приняты и в других странах. Компьютерные вирусы – это целая группа компьютерных программ, способных размножаться путем самокопирования и внедряться в код других приложений. Кроме этого они способны по различным каналам рассылать свои копии. Внедряясь в код программ вирусы, приводят к ошибкам и нарушению работы компьютера, а также к уничтожению файлов.

Несмотря на значительные усилия по созданию противовирусного программного обеспечения, полной гарантии безопасности и защиты от попадания вредоносных программ на стационарное или мобильное устройство не существует.

Поэтому, наряду с использованием самых современных антивирусов нужно научиться придерживаться некоторых установок:

 не устанавливать и не запускать на компьютере незнакомые приложения из источников, не имеющих серьезной репутации;

 не открывать подозрительные сайты, а при входе на популярные сервисы в интернете обращать внимание на написание доменного имени в адресной строке;

 регулярно обновлять программы, обеспечивающие безопасность работы системы.

***ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ И ФОРМА ОТЧЕТНОСТИ:***

Задание 1. Понятие и виды антивирусных программ.

**Антивирусом** называют специализированную программу, в функции которой входит обнаружение и удаление вредоносных приложений на компьютере. Кроме этого антивирусы выполняют функцию восстановления зараженных файлов.

Виды антивирусных программ:

1. Фильтры - Программа-фильтр располагается в резидентном режиме в оперативной памяти компьютера и переносит данные, принимаемые вирусами для размножения и нанесения вреда, а также информирует пользователя об этом сообщении. Пользователь вправе отказаться от выполнения данной операции или согласиться с ней, если будет выполняться данная операция.
2. Детекторы - Детекторы позволяют обнаруживать файлы, заражённые одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске, специфическая для данного вируса комбинация байтов. При её обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения заражённых файлов
3. Ревизоры - Программы-ревизоры имеют две стадии работы:

Сначала они запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска). Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю. К распространенным программам-ревизорам относится антивирус Касперского.

1. Программы-доктора - Программы-доктора (фаги) не только находят заражённые вирусами файлы, но и «лечат» их, то есть удаляют из файла тело программы вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов. Среди фагов выделяют полифаги, то есть программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Учитывая, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление их версий

Задание 2. Организация антивирусной защиты.

1. Выбор подходящей антивирусной программы: Исследуйте рынок антивирусного программного обеспечения и выберите программу, которая лучше всего соответствует вашим потребностям. Убедитесь, что она обладает надежной защитой и регулярно обновляется с помощью новых сигнатур вирусов.
2. Установка и регулярное обновление антивирусного программного обеспечения: Установите выбранную антивирусную программу на все компьютеры и устройства в сети. Важно убедиться, что антивирусное программное обеспечение обновляется регулярно, чтобы иметь актуальные сигнатуры и защиту от новых угроз.
3. Запланированное сканирование системы: Настройте регулярное запланированное сканирование системы для поиска и удаления вредоносного программного обеспечения. Это поможет обнаружить и устранить потенциальные угрозы, прежде чем они причинят вред вашей системе.
4. Общение и обучение пользователей: Проводите обучающие сессии и информируйте пользователей о базовых принципах безопасности компьютера, таких как неоткрытие подозрительных вложений, неустановка ненадежного программного обеспечения и регулярное обновление паролей. Это поможет снизить риск внесения вредоносного программного обеспечения из-за непреднамеренных действий пользователей.
5. Создание политики безопасности: Разработайте и реализуйте политику безопасности, которая определяет правила и процедуры для обеспечения антивирусной защиты. Включите в нее требования к использованию антивирусного программного обеспечения, частоте обновлений и сканирований системы, а также процедуры реагирования на обнаружение вредоносного кода.
6. Резервное копирование данных: В случае атаки вредоносного программного обеспечения может потребоваться восстановление данных. Регулярно создавайте резервные копии важных данных и храните их в отдельном и надежном месте.

Задание 3. Примеры и возможности бесплатных антивирусных программ. Оформить в виде таблицы.

|  |  |
| --- | --- |
| Антивирусная программа | Основные возможности |
| Avast Free Antivirus | - Защита от вирусов, шпионского ПО и рекламных программ Онлайн-защита Развернутый анализ в режиме реального времени |
| AVG AntiVirus Free | - Антивирусная защита Защита в реальном времени Сканирование по требованию |
| Avira Free Security | - Базовая антивирусная защита Веб-защита Безопасное браузерное прослушивание |
| Bitdefender Antivirus Free Edition | - Проверка и удаление вредоносных программ Минимальное влияние на системные ресурсы |
| Kaspersky Security Cloud – Free | - Антивирусная защита Защита в реальном времени Онлайн-безопасность |

Задание 4. Примеры и возможности платных антивирусных программ. Оформить в виде таблицы.

|  |  |
| --- | --- |
| Антивирусная программа | Основные возможности |
| Norton Antivirus | - Защита от вирусов и других угроз Wi-Fi-защита Защита конфиденциальности и идентичности |
| McAfee Total Protection | - Многоуровневая защита от вирусов, шпионского ПО и рекламных программ Парольный менеджер Защита конфиденциальных данных |
| Kaspersky Internet Security | - Антивирусная защита Защита от сетевых атак Защита конфиденциальных данных |
| ESET Smart Security Premium | - Защита от вирусов и других угроз Брандмауэр Защита банковских транзакций |
| Trend Micro Maximum Security | - Улучшенная антивирусная защита Защита в режиме реального времени Защита от рандомного шифрования |

Задание 5. Скачать и установить антивирусную программу Avast. Описать пошаговый процесс установки в виде таблицы.

|  |  |
| --- | --- |
| Для установки Avast, перейдите в папку, в которую производилась загрузка установочного файла и запустите инсталляцию, нажав на нем два раза лев. кн. мыши. |  |
| Возникнет окно-предупреждение от Контроля учетных записей Windows «Разрешить этому приложению вносить изменения на вашем устройстве?», так как вы знаете, что это вы начали установку данной программы и в нем написано, что это проверенный издатель AVAST Software s.r.o., то необходимо согласиться с установкой.  Нажмите «Да». |  |
| В следующем окне вы можете настроить устанавливаемые компоненты и дополнительные приложения. В данном случае, нам не нужно устанавливать браузер Google Chrome, поэтому мы снимаем галочку в чекбоксе.  Нажмите «Настройка». |  |
| В этом окне вы можете настроить компоненты программы, которые желаете использовать. С ненужных просто уберите галочку. Например, вы можете отказаться от установки браузерного расширения SafePrice или компонента для обновления программ.  Нажмите «Установить». |  |
| После того как вы нажали кнопку «Установить», возле трея появится маленькое окошко, на котором будет отображаться этап установки антивируса Avast Free Antivirus. Не выключайте компьютер! |  |
| После завершения загрузки и установки всех необходимых компонентов, появится информационное окно «Вы защищены».  Нажмите «Продолжить». |  |
| Далее вам предложат поделиться определенными данными с компанией Аваст и их партнерами. Вы можете согласиться на это, либо отказаться. Дальше мы покажем, как и где в настройках потом можно изменить свое решение, а пока согласимся.  Нажмите «Соглашаюсь». |  |

Задание 6. Проверить компьютер на наличие вирусов с помощью антивирусной программы Avast. Удалить программу Avast.

|  |  |
| --- | --- |
| Откройте программу и Нажмите «Начать первое сканирование». |  |
| Следующее информационное окно будет отображать в процентах ход сканирования.  Вы можете нажать «Остановить сканирование». |  |
| Если вирусы и уязвимости найдутся, вам предложат их удалить, в таком случае, разумно будет с этим согласиться. На последнем этапе Аваст предложит вам решить некоторые сложные проблемы вашей системы, то есть попросту начнут вам продавать свою полную платную версию Avast Premium Security. Бесплатной версии для базовой защиты достаточно, поэтому вы можете проигнорировать советы антивируса.  Нажмите «Пропустить». |  |
| Последующее окно сообщит, что сканирование завершено и компьютер в безопасности.  Нажмите «Готово». |  |

Удаление антивируса Avast

|  |  |
| --- | --- |
| Как и почти любой другой антивирус Avast Free Antivirus может быть удален двумя способами: с помощью удаления в «Панель управления» — «Программы и компоненты» (как любую другую программу в Windows) или с помощью специальной утилиты на официальном сайте. |  |

Задание 7. Программа «Защитник Windows». Назначение, возможности, скрины.

Windows Defender (Защитник Windows) – программный продукт компании Microsoft, предназначенный для предотвращения появлений, помещения на карантин или удаления шпионских вредоносных модулей в операционных системах Microsoft Windows. Свою эволюцию “Защитник” прошел от Windows XP до Windows 10, приобретая и улучшая свои функции безопасности.

Возможности:

1. **Защита в реальном времени.** Помогает обнаруживать вредоносные программы и предотвращать их установку или запуск на компьютере. Защита состоит из:
   1. Отслеживания списка программ, автоматически запускающихся при старте ОС.
   2. Отслеживания установок Windows, что связаны с безопасностью системы.
   3. Слежки за компонентами и безопасностью, что связаны с Internet Explorer.
   4. Отслеживания взаимодействующих с ОС и с запущенными программами служб и драйверов.
   5. Наблюдения за обновлением компонентов Windows.
   6. Мониторинг автозапуска программ и всех действий, которые они выполняют.
   7. Наблюдения за инструментами и файлами, с помощью которых осуществляется регистрация и автозапуск ПО.
2. **Облачная защита.** Позволяет отправлять данные о потенциальных угрозах безопасности в корпорацию Microsoft в режиме реального времени. Перед отправкой, запрашивает разрешение пользователя.
3. **Автоматическая отправка образцов.** Отправка данных отправляется автоматически, без уведомления пользователя.
4. **Исключения.** Пользователь может самостоятельно указать файл, который хочет исключить из проверки и обработки антивирусом.
5. **Расширенные уведомления.** Защитник отправляет автоматические уведомления, чтобы пользователь автоматически получал уведомления о работоспособности ПК. Если функция будет отключена, антивирус будет уведомлять только о критических уведомлениях.
6. **Автономный Защитник.** Функция помогает устранить из зараженного компьютера “особо тяжкие” вредоносные программы. После включения функции ПК перезагрузится, а поиск и устранение займет около 15 минут.

Скрины:









