Задание

1. Прежде чем приступить к выполнению практического задания, внимательно ознакомьтесь с теоретическими сведениями.
2. Выполнить 4 задания и ответить на Контрольные вопросы.
3. Готовую работу скинуть либо в социальной сети «Вконтакте» в личном сообщении (https://vk.com/id35792775), либо скинуть на электронную почту guv@apt29.ru
   Срок выполнения: до 22.05.20 до 12:00

Практическая работа № 30.

Тема: **«Антивирусная защита ПК»**

Цель: ознакомиться с теоретическими аспектами защиты информации от вредоносных программ: разновидностями вирусов, способами заражения и методы борьбы. Ознакомиться с различными видами программных средств защиты от вирусов. Проверка настроек антивирусов, сканирование файлов, папок и дисков, обновления антивирусной базы Получить навыки работы с антивирусным пакетом **Антивирус Касперского**.

Оснащение: ПК, антивирусная программа, программа восстановления файлов.

Ход работы:

Теоретические сведения

Компьютерный вирус - это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять различные нежелательные действия на компьютере. Программа, внутри которой находится вирус, называется "зараженной". Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и "заражает" другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или FAT-таблицу, "засоряет" оперативную память и т.д.). Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а при выполнении определенных условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает также, как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной.

Компьютерный вирус может испортить, то есть изменить ненадлежащим образом, любой файл на имеющихся в компьютере дисках. Но некоторые виды файлов вирус может "заразить". Это означает, что вирус может "внедриться" в эти файлы, т.е. изменить их так, что они будут содержать вирус, который при некоторых обстоятельствах может начать свою работу.

Методы защиты от компьютерных вирусов

Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.

Для защиты от вирусов можно использовать:

• общие средства защиты информации, которые полезны также и как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;

• профилактические меры, позволяющие уменьшить вероятность заражения вирусом;

• специализированные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств:

• копирование информации - создание копий файлов и системных областей дисков;

• разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

Задание 1

Подготовить доклад на тему: «Общие сведения и особенности работы антивирусной программы [***Название антивирусной программы***]».

Задание 2

Изучить антивирусный пакет ***Антивирус Касперского***. Подготовить отчет по лабораторной работе.

Порядок выполнения

1). Сканирование папок на наличие вирусов:

– Двойным щелчком на значке антивируса на панели индикации открыть главное окно программы;

– Изучить содержимое окна: обратить внимание на дату последнего обновления антивирусной базы и дату последней полной проверки компьютера;

– В своей личной папке создать папку **Подозрительные файлы** и создать там 2 файла: ***Текстовый файл*** и ***Документ Microsoft Word***. Имена файлов ввести согласно своему варианту по **Вариантам задания к работе**;

– Выбрав пункт в главном окне программы пункт **Проверка – Быстрая проверка** и добавить в окно заданий папку **Подозрительные файлы**.

– Выполнить проверку папки. По завершению сканирования, используя кнопку «**Отчеты**» - **«Сохранить как…»**, сохранить отчет с результатами проверки в папке **Подозрительные файлы**. Имя файла-отчета – **Scan_Log**.

2). Обновление антивирусной базы:

– Нажмите на пункт **Обновление** и, используя кнопку **Обновить**, осуществите обновление базы известных вирусов.

– По завершению обновления, используя кнопку «**Отчеты**» - **«Сохранить как…»**,, сохранить отчет об обновлении в папке **Подозрительные файлы**. Имя файла-

отчета – **Upd_Log.**

– Закройте окно **Антивируса Касперского**.

Задание 3

Изучить антивирусный пакет **Avast!**

Порядок выполнения;

1. Найдите иконку антивируса Avast! В системном трее, правой кнопкой мышки вызовите меню и выберите «Открыть интерфейс пользователя Avast!»

2. Перейдите на вкладку «Сканировать компьютер». Вам будет представлены 4 вида сканирования: Экспресс, Полное, Сканирование носителей и возможность выбрать папку для сканирования вручную.

3. Выберите «Сканирование съемных носителей» и нажмите кнопку «Пуск» в окне антивируса – будут автоматически проверены все подключенные к компьютеру съемные носители (диски, флэшки, дискеты).

4. По завершении сканирования выберите четвертый вид сканирования и вручную укажите любую папку на вашем съемном носителе и проверьте еѐ.

5. Во вкладке «Экраны в реальном времени», в подменю «Экран файловой системы» нажав кнопку «Расширенные настройки» вы можете разрешить/запретить антивирусу следующие действия:

6. Сканировать программы при выполнении (например, программа excel.exe будет сканироваться при каждом выполнении Microsoft Excel)

7. Сканировать сценарии при выполнении (например, файл JS (JavaScript) будет сканироваться при каждом его выполнении). Сканировать библиотеки (DLL) при загрузке (при выполнении программы будут сканироваться еѐ вспомогательные файлы – библиотеки DLL и т.д.)

8. Во вкладке «Экраны в реальном времени», в подменю «Веб-экран» нажав кнопку «Расширенные настройки» вы можете разрешить/запретить антивирусу следующие действия:

9. Включить веб-сканирование

10. Использовать интеллектуальное сканирование потока

11. Во вкладке «Обслуживание» в подменю «Обновить» есть возможность ручного запуска обновлений для «Модуля сканирования и определения вирусов» и непосредственно для программы. (По умолчанию модуль обновляется автоматически, а обновление программы запрашивает разрешения пользователя).

12. По завершению сканирования, используя кнопку «**Отчеты**» - **«Сохранить как…»**, сохранить отчет с результатами проверки.

Задание 4

Изучить антивирусный пакет **Dr. Web CureIt**

1. При запуске этого портативного антивируса вам будет предложено запустить его в режиме усиленной защиты – он необходим в случае, если вредоносные программы блокируют работу операционной системы. Нажмите «Отмена».

2. Далее появится предупреждение, т.к. использование антивируса бесплатно доступно только для лечения домашних компьютеров. Нажмите «Нет».

3. Нажмите «Пуск» и будет автоматически запущены быстрая проверка компьютера.

В этом режиме проверяются:

• Оперативная память
• Загрузочные секторы всех дисков
• Объекты автозапуска
• Корневой каталог загрузочного диска
• Корневой каталог диска установки Windows
• Системный каталог Windows
• Папка Мои Документы
• Временный каталог системы
• Временный каталог пользователя

4. По окончании быстрой проверки выбрать в меню пункт «Выборочно» и указать путь к съемному носителю – выполнить его проверку.

5. По завершению сканирования, используя кнопку «**Отчеты**» - **«Сохранить как…»**, сохранить отчет с результатами проверки

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1). Что называется компьютерным вирусом?
2). Какая программа называется "зараженной"?
3). Что происходит, когда зараженная программа начинает работу?
4). Как может маскироваться вирус?
5). Каковы признаки заражения вирусом?
6). Каковы последствия заражения компьютерным вирусом?
7). По каким признакам классифицируются компьютерные вирусы?
8). Как классифицируются вирусы по среде обитания?
9). Какие типы компьютерных вирусов выделяются по способу воздействия?
10). Что могут заразить вирусы?
11). Как маскируются "невидимые" вирусы?
12). Каковы особенности самомодифицирующихся вирусов?
13). Какие методы защиты от компьютерных вирусов можно использовать?
14). В каких случаях применяют специализированные программы защиты от компьютерных вирусов?
15). На какие виды можно подразделить программы защиты от компьютерных вирусов?
16). Как действуют программы-детекторы?
17). Что называется сигнатурой?
18). Всегда ли детектор распознает зараженную программу?
19). Каков принцип действия программ-ревизоров, программ-фильтров, программ-вакцин?
20). Как выглядит многоуровневая защита от компьютерных вирусов с помощью антивирусных программ?
21). Перечислите меры защиты информации от компьютерных вирусов.
22). Каковы современные технологии антивирусной защиты?
23). Каковы возможности антивируса Касперского для защиты файловых серверов? почтовых серверов?

24). Какие модули входят в состав антивируса Касперского для защиты файловых систем?

25). Каково назначение этих модулей?

26). Какие элементы электронного письма подвергаются проверке на наличие вирусов?

27). Как обезвреживаются антивирусом Касперского, обнаруженные подозрительные или инфицированные объекты?

28). Как обновляется база вирусных сигнатур?