18 декабря информатика 1 курс технологи.

Практическая работа

Тема работы: Защита информации, антивирусная защита.

Цель работы: Изучить

- основные понятия информационной безопасности;
- классификацию вирусов, способы их распространения, способы борьбы с ними;
- классификацию и назначение антивирусных программ.

Содержание отчёта по практической работе:

- тема и цель работы;
- ответ на задание 1;
- ответы на контрольные вопросы;
- вывод по практической работе.

Вопросы для подготовки к практической работе:

1. Что такое информация?
2. Как вы понимаете термин «защита информации»?
3. Как вы понимаете термин «компьютерный вирус»?
4. С какими антивирусными программами вам приходилось работать?

Теоретическая часть

1. Защита информации

Защита информации – это деятельность, которая направлена на предотвращение утечки защищаемых данных, непреднамеренных и несанкционированных воздействий на защищаемые данные.

Защита информации включает в себя несколько аспектов (рис. 1).

Рисунок 1 – Защита информации

Государственная информационная безопасность представляет собою состояние сохранности всех информационных ресурсов государства, а также защищенность всех законных прав общества и личности в информационной сфере.

В виде стандартной модели информационной безопасности зачастую приводят модель, состоящую из трех различных категорий:

– конфиденциальность – представляет собой состояние информации, при котором допуск к ней осуществляют лишь субъекты, которые имеют такое право;

– целостность – представляет собой избежание несанкционированных изменений информации;

– доступность – представляет собой избежание постоянного или временного сокрытия информации от юзеров, которые получили права доступа.

Антивирусная защита

Официальное появление первого компьютерного вируса датируется 1981 годом, задолго до выхода первой версии Microsoft Windows. Этот вирус, замаскированный под компьютерную игру, атаковал наиболее популярный

компьютер того времени — Apple II. Распростра¬нялся он с черепашьей скоростью (с помощью дискет).

Согласно подсчетам экспертов, объем malware (общепринятое название всех видов вредоносных программ) возрастает более чем на 15 % в год.

Компьютерный вирус — вид вредоносного программного обеспечения, способного внедряться в код других программ, системные области памяти, загрузочные секторы, и распространять свои копии по разнообразным каналам связи.

Основная цель вируса — его распространение. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов — удаление файлов и даже удаление операционной системы, приведение в негодность структур размещения данных, блокирование работы пользователей и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют ресурсы системы.

Ныне существует немало разновидностей вирусов, различающихся по основному способу распространения и функциональности. Если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через локальные и глобальные (Интернет) сети. Растёт и функциональность вирусов, которую они перенимают от других видов программ.

В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы:

– по поражаемым объектам (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);

– файловые вирусы делят по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом;

– по поражаемым операционным системам и платформам (DOS, Windows, Unix, Linux, Android);

– по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы, руткиты);

– по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язык и др.);

– по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.).

–

Антивирусные программы

Антивирусная программа – это специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов и профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Классификация антивирусных средств приведена в таблице 16.

Таблица 1 – Классификации антивирусных программ

Признак классификации	Класс	Описание
1	2	3
По исполнению (средствам блокирования)	Программные	Реализованы только программно.
	Программно-аппаратные	Представляют собой интерфейсные платы, устанавливаемые в каждом отдельном ПК. Обеспечивают защиту от вируса на аппаратном уровне.
По признаку размещения в оперативной памяти	Резидентные	Начинают свою работу при запуске ОС, постоянно находятся в памяти компьютера и осуществляют автоматическую проверку файлов.
	Нерезидентные	Запускаются по требованию пользователя или в соответствии с заданным для них расписанием.
По виду (способу) защиты от вирусов	Программы-детекторы (сканеры)	Находят вирусы в оперативной памяти, на внутренних и/или внешних носителях, выводя сообщение при обнаружении вируса
	Программы-доктора (фаги, полифаги)	Находят заражённые файлы и «лечат» их. Среди докторов существуют полифаги, способные удалять разнообразные виды вирусов.
	Программы-вакцины (иммунизаторы)	Выполняют иммунизацию системы (файлов, каталогов) блокируя действие вирусов.
	Программы-ревизоры	Запоминают исходное состояние программ, каталогов, системных областей диска до момента инфицирования компьютера (обычно на основе подсчёта контрольных сумм), затем сравнивают текущее состояние с первоначальным, выводя найденные изменения на экран. Наиболее надёжны в плане защиты от вирусов.
	Программы-мониторы	Начинают свою работу при запуске ОС, постоянно находятся в памяти компьютера и осуществляют автоматическую проверку файлов по принципу «здесь и сейчас».
	Программы-фильтры (сторожа)	Небольшие резидентные программы, целью которых является обнаружение действий, характерных для вирусов. Обнаруживают вирус на ранней стадии, пока он не начал размножаться.

Продолжение таблицы 1

1	2	3
В соответствии с нормативным правовым актом ФСТЭК России «Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам антивирусной защиты)»	Тип «А»	Средства антивирусной защиты (или их компоненты), предназначенные для централизованного администрирования средствами антивирусной защиты, установленными на компонентах информационных систем (серверах, автоматизированных рабочих местах). Не применяются самостоятельно, предназначены для использования только совместно со средствами антивирусной защиты типов «Б» и/или «В»
	Тип «Б»	Средства антивирусной защиты (или их компоненты), предназначенные для применения на серверах информационных систем
	Тип «В»	Средства антивирусной защиты (или их компоненты), предназначенные для применения на автоматизированных рабочих местах информационных систем
	Тип «Г»	Средства антивирусной защиты (или их компоненты), предназначенные для применения на автономных автоматизированных рабочих местах.

Microsoft Defender

Автономный Microsoft Defender — это мощный автономный инструмент проверки, который можно запустить из доверенной среды без загрузки ОС.

Microsoft Defender (данное название используется начиная с Windows 10 сборки 2004, ранее использовалось название Защитник Windows) — программный продукт компании Microsoft, созданный для того, чтобы удалять, помещать в карантин или предотвращать появление spyware-модулей в операционных системах Microsoft Windows.

Рисунок 2 – Логотип Microsoft Defender

Запустите автономный Microsoft Defender, если:

– Безопасность Windows (в предыдущих версиях Windows — «Центр безопасности Защитника Windows») обнаруживает на вашем компьютере пакеты программ rootkit или сложно удаляемые вредоносные программы и оповещает вас о необходимости запуска автономного Microsoft Defender. При обнаружении таких программ вы увидите сообщение о том, что на устройстве найдено вредоносное программное обеспечение, или сообщение Безопасности Windows о том, что требуется дополнительная очистка.

– Вы подозреваете, что на вашем компьютере могут находиться вредоносные программы, которые ваши средства обеспечения безопасности не могут обнаружить. В этом случае можно запустить проверку компьютера автономным Microsoft Defender, перейдя в раздел «Параметры» меню «Безопасность Windows». Для этого выполните следующие действия.

1. Нажмите кнопку *Пуск* и выберите *Параметры → Обновление и безопасность → Безопасность Windows → Защита от вирусов и угроз*.

Рисунок 1 – Выбор пункта *Параметры*

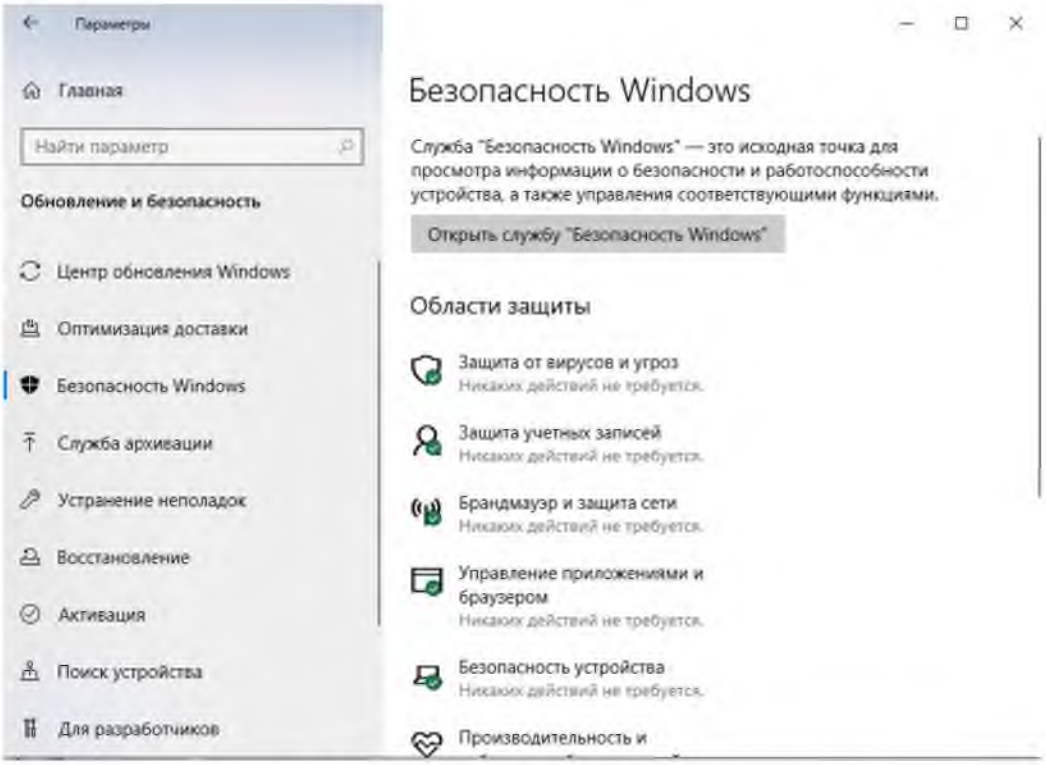

Рисунок 4 – Диалоговое окно *Параметры*

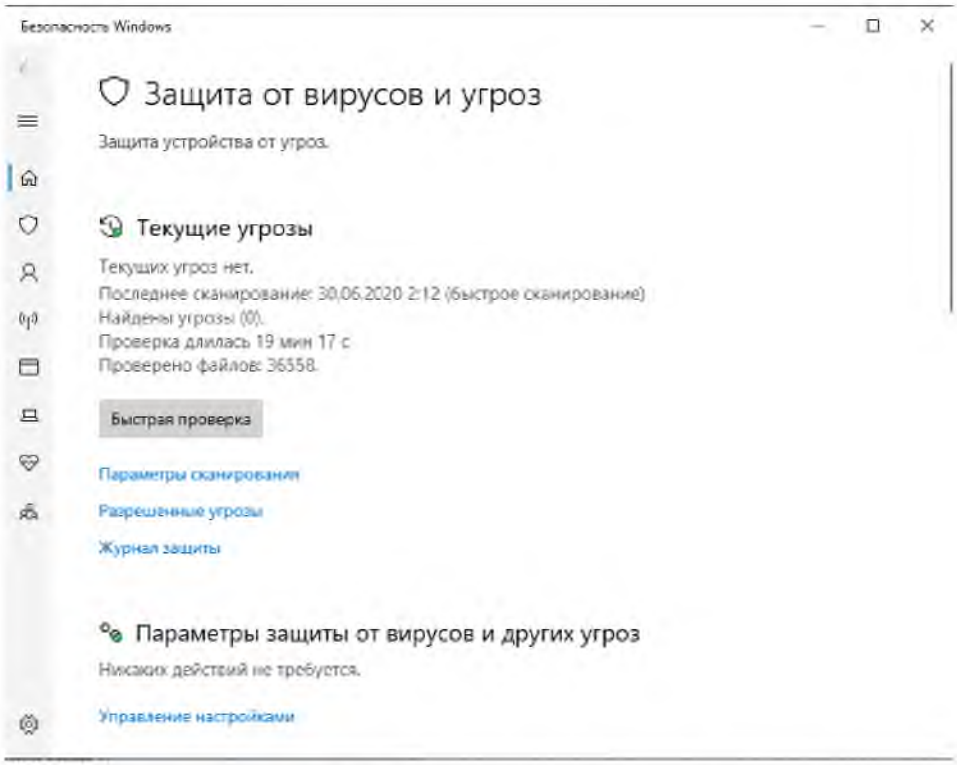

Рисунок 5 – Окно *Защита от вирусов и угроз*

2. На экране «Защита от вирусов и угроз» выполните одно из следующих действий:

- В последней версии Windows 10: В разделе *Текущие угрозы* выберите *Параметры проверки*.
- В предыдущих версиях Windows: В разделе *Журнал угроз* выберите *Запустить новое расширенное сканирование*.

3. Выберите Проверка автономного Microsoft Defender, а затем — Проверить сейчас.

Вам будет предложено выйти из Windows. После этого компьютер должен выполнить перезапуск. Загрузится автономный Microsoft Defender, и он выполнит быструю проверку компьютера в среде восстановления. После завершения проверки (как правило, она занимает около 15 минут) компьютер автоматически выполнит перезапуск.

Замечания

Перед использованием автономного Microsoft Defender сохраните все открытые файлы и закройте все приложения и программы.

Обычно требуются права администратора на компьютере, на котором планируется запустить автономный Microsoft Defender.

При возникновении неустранимой системной ошибки на синем экране во время автономной проверки выполните принудительный перезапуск и попробуйте еще раз запустить проверку автономного Microsoft Defender. Если ошибка с синим экраном возникнет снова, обратитесь в службу поддержки Майкрософт.

Чтобы просмотреть результаты проверки автономного Microsoft Defender:

– Нажмите кнопку *Пуск* и выберите *Параметры → Обновление и безопасность → Безопасность Windows → Защита от вирусов и угроз.*

– На экране «Защита от вирусов и угроз» в Windows 10 в разделе Текущие угрозы выберите *Параметры проверки,* а затем — *Журнал защиты* (в предыдущих версиях Windows он может называться *Журнал угроз*).

Практическая часть

Задание 1.

По поражаемым объектам компьютерные вирусы делятся на:

– файловые вирусы,

– загрузочные вирусы,

– сценарные вирусы,

– макровирусы, вирусы,

– поражающие исходный код.

Найдите определения и примеры вирусов для каждого из этих классов.

Контрольные вопросы:

1. Что такое защита информации?

2. Какие три составляющих информационной безопасности вы знаете?

3. На какие классы делятся компьютерные вирусы по механизму заражения?

4. Чем отличаются резидентные антивирусные программы от нерезидентных?