****

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

Институт Информационных Технологий

Кафедра «Корпоративные информационные системы»

**ОТЧЕТ**

по лабораторной работе № 2

на тему

«Профилактика проникновения «троянских программ» и восстановление зараженных файлов одиночной информационной системы при дистанционном взаимодействии пользователей**»**

по дисциплине

«Информационные системы и технологии»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Выполнил студент группы ИКБО-08-18 | |  | | Валяев Д.А. |
| Принял | к.т.н., доцент | | | Башлыкова А.А. |
| Выполнено | «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 | | г. |  |
| Зачтено | «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2020 | | г. |  |

МОСКВА 2020

**Лабораторная работа № 2.**

Тема**:** **«Профилактика проникновения «троянских программ» и восстановление зараженных файлов одиночной информационной системы при дистанционном взаимодействии пользователей.»**

**Цель работы:** практическое освоение профилактики «троянских программ» и восстановления зараженных файлов одиночной информационной системы.

**Время выполнения:** 4часа

**Раздаточный материал**:дидактический материал

**Перечень и характеристики оборудования, приборов и материалов:**

Тип компьютера: PC

Операционная система: Windows 10 Pro

Пакет обновления: 10.0.18362 Сборка 18362

Internet Explorer: 11.476.18362.0

DirectX: DirectX 12

Тип ЦП: 6х, 3.2 GHz AMD Ryzen 5

Системная память: 16 Гб = 16384 MB

Видеоадаптер: NVIDIA GeForce GTX 1050ti

Монитор: LG W2343

Дисковый накопитель: Western Digital WDC WD10EZEX-08WN4A0 (1 ТБ)

**Теоретические основы**

Для лучше понимания алгоритма выполнения данной лабораторной работы, нужно ознакомиться с некоторыми аспектами, связанными с определениями: 1)информационные ресурсы; 2)макровирусы, 3)троянские программы. Начнем по порядку.

Определение “информационные ресурсы” может трактоваться по-разному, все зависит от сферы деятельности. Информационные ресурсы —  отдельные массивы данных, к которым применяются, определенные методы, обеспечивающие информационную безопасность.

Поговорим про макровирусы. Макровирус — это разновидность компьютерных вирусов разработанных на макроязыках, встроенных в такие прикладные пакеты ПО, как Microsoft Office. Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносятся из одного зараженного файла в другие. Большая часть таких вирусов написана для MS Word.  Наибольшее распространение получили макровирусы для Microsoft Word, Excel и Office 97.

Углубимся в историю. Первый макровирус, получивший название Concept, появился в июле 1995. Впоследствии макровирусы (чаще всего заражающие документы Word) стали основным типом вирусов и оставались таковыми до конца прошлого века, когда Microsoft по умолчанию отключила макросы в Office (версии Office 2000 и выше).

Для существования вирусов в конкретной системе (редакторе) необходимо наличие встроенного в систему макроязыка с возможностями: 1)привязки программы на макроязыке к конкретному файлу; 2)копирования макропрограмм из одного файла в другой; 3)получения управления макропрограммой без вмешательства пользователя (автоматические или стандартные макросы).

Описанным условиям удовлетворяют редакторы MS Word, MS Office 97 и AmiPro, а также электронная таблица MS Excel. Эти системы содержат в себе макроязыки (MS Word — Word Basic, MS Excel и MS Office 97 — Visual Basic), при этом: 1)макропрограммы привязаны к конкретному файлу (AmiPro) или находятся внутри файла (MS Word/Excel/Office 97); 2)макроязык позволяет копировать файлы (AmiPro) или перемещать макропрограммы в служебные файлы системы и редактируемые файлы (MSWord /Excel/Office 97); 3)при работе с файлом при определенных условиях (открытие, закрытие и т. д.) вызываются макропрограммы (если таковые есть), которые определены специальным образом (AmiPro) или имеют стандартные имена (MS Word/Excel/ Office 97).

Давайте разберемся, каков принцип работы макровируса. Макровирусы, поражающие файлы Word, Excel или Office 97, как правило, пользуются одним из трех нижеперечисленных приемов: 1)в вирусе присутствует автомакрос (автофункция); 2)в вирусе переопределен один из стандартных системных макросов (ассоциированный с каким-либо пунктом меню); 3)макрос вируса автоматически вызывается при нажатии на какую-либо клавишу или комбинацию клавиш.

Подробно остановимся на принципе работы макровирусов в Microsoft Word. Большинство известных Word-вирусов (версий 6, 7 и Word 97) при запуске переносят собственный код в область глобальных макросов документа («общие» макросы). При выходе из Word глобальные макросы (включая макросы вируса) автоматически записываются в DOT-файл глобальных макросов (обычно таким файлом является NORMAL.DOT). Таким образом, вирус активизируется в тот момент, когда Word грузит глобальные макросы. Затем вирус переопределяет (или уже содержит в себе) один или несколько стандартных макросов (например, FileOpen, FileSave, FileSaveAs, FilePrint) и перехватывает, таким образом, команды работы с файлами. При вызове этих команд заражается файл, к которому идет обращение. Для этого вирус конвертирует файл в формат Template (что делает невозможными дальнейшие изменения формата файла, то есть конвертирование в какой-либо не-Template формат) и записывает в файл свои макросы, включая Auto-макрос. Другой способ внедрения вируса в систему базируется на так называемых «Add-in» файлах, то есть файлах, являющихся служебными дополнениями к Word. В этом случае NORMAL.DOT не изменяется, а Word при запуске загружает макросы вируса из файла (или файлов), определенного как «Add-in». Этот способ практически полностью повторяет заражение глобальных макросов за тем лишь исключением, что макросы вируса хранятся не в NORMAL.DOT, а в каком-либо другом файле. Возможно также внедрение вируса в файлы, расположенные в каталоге STARTUP. В этом случае Word автоматически подгружает файлы-шаблоны из этого каталога, но такие вирусы пока не встречались.

Бывают также полувирусы, которые не используют перечисленные приемы и размножаются, только если пользователь самостоятельно запускает их на выполнение. Большинство макровирусов содержат все свои функции в виде стандартных макросов MS Word/Excel/Office 97. Существуют, однако, вирусы, использующие приемы скрытия своего кода и хранящие свой код в виде не-макросов. Известны три подобных приема. Все они используют возможность макросов создавать, редактировать и исполнять другие макросы. Как правило, подобные вирусы имеют небольшой (иногда полиморфный) макрос-загрузчик, который вызывает встроенный редактор макросов, создает новый макрос, заполняет его основным кодом вируса, выполняет и затем, как правило, уничтожает, чтобы скрыть следы присутствия вируса. Основной код таких вирусов присутствует либо в теле самого вируса в виде текстовых строк, либо хранится в области переменных документа или в области Auto-text.

Можно очень легко обнаружить макровирус. Характерными признаками присутствия макровирусов являются: 1)невозможность конвертирования зараженного документа Word в другой формат, зараженные файлы имеют формат Template (шаблон), поскольку при заражении Word-вирусы конвертируют файлы из формата Word Document в Template; 2)невозможность записи документа в другой каталог или на другой диск командой «Save As» (только для Word 6); 3)в STARTUP-каталоге присутствуют «чужие» файлы; 4)наличие в Книге (Book) «лишних» и скрытых Листов (Sheets).

В большинстве случаев процедура «лечения» зараженных файлов и дисков сводится к запуску подходящего антивирусного программного обеспечения. Но бывают ситуации, когда обезвреживание вируса приходится осуществлять самостоятельно, т. е. «руками». Данный метод, мы рассмотрим в самой лабораторий работе.

  Лёгкость создания макровирусов поражает воображение, всё находится буквально под рукой: достаточно запустить Word, выбрать меню Сервис – Макрос – Редактор Visual Basic – и запустится программная среда VBA (Visual Basic for Application).

Далее рассмотрим так называемый термин  «троянская программа». Троянская вирусная программа — разновидность [вредоносной программы](https://ru.wikipedia.org/wiki/%D0%92%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0), проникающая в компьютер под видом легитимного программного обеспечения, в отличие от [вирусов](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81) и [червей](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%87%D0%B5%D1%80%D0%B2%D1%8C), которые распространяются самопроизвольно. В данную категорию входят программы, осуществляющие различные неподтверждённые пользователем действия: сбор информации о банковских картах, передача этой информации злоумышленнику, а также использование, удаление или злонамеренное изменение, нарушение работоспособности компьютера, использование ресурсов компьютера в целях майнинга, использование IP для нелегальной торговли.

Свое общее название троянские программы получили за сходство механизма проникновения в компьютер пользователя с описанным в эпизоды [Илиады](https://ru.wikipedia.org/wiki/%D0%98%D0%BB%D0%B8%D0%B0%D0%B4%D0%B0), рассказывающем о «[Троянском коне](https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%BE%D1%8F%D0%BD%D1%81%D0%BA%D0%B8%D0%B9_%D0%BA%D0%BE%D0%BD%D1%8C)» — дарёном деревянном коне, использованном для проникновения в [Трою](https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%BE%D1%8F), что и стало причиной падения Трои. В Коне, подаренном в знак лже-перемирия, прятались воины [Одиссея](https://ru.wikipedia.org/wiki/%D0%9E%D0%B4%D0%B8%D1%81%D1%81%D0%B5%D0%B9), ночью выбравшиеся из Коня и открывшие ворота основным силам объединенной греческой армии. Большая часть троянских программ действуют подобным образом — маскируется под безвредные или полезные программы, чтобы пользователь запустил их на своем компьютере. Считается, что первым этот термин в контексте компьютерной безопасности употребил в своём отчёте «Computer Security Technology Planning Study» [Дэниэл Эдвардс](https://ru.wikipedia.org/w/index.php?title=%D0%94%D1%8D%D0%BD%D0%B8%D1%8D%D0%BB_%D0%AD%D0%B4%D0%B2%D0%B0%D1%80%D0%B4%D1%81&action=edit&redlink=1), сотрудник [АНБ](https://ru.wikipedia.org/wiki/%D0%90%D0%B3%D0%B5%D0%BD%D1%82%D1%81%D1%82%D0%B2%D0%BE_%D0%BD%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B9_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8).

Троянские программы распространяются людьми  — как непосредственно загружаются в компьютерные системы злоумышленниками-инсайдерами, так и побуждают пользователей загружать или запускать их на своих системах. Для достижения последнего троянские программы помещаются злоумышленниками на открытые или индексируемые ресурсы ([файл-серверы](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80) и системы файлообмена), носители информации, присылаются с помощью служб обмена сообщениями (например, [электронной почтой](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D1%87%D1%82%D0%B0)), попадают на компьютер через бреши безопасности или загружаются самим пользователем с адресов, полученных одним из перечисленных способов. Иногда использование троянов является лишь частью спланированной многоступенчатой атаки на определенные компьютеры, сети или ресурсы.

Троянские программы бывают разных типов: 1)удалённый доступ; 2)уничтожение данных; 3)загрузчик; 4)сервер; 5)дезактиватор программ безопасности. Данная классификация, где они разбиваются на категории, основана на том, как трояны внедряются в систему и какой вред наносят данной системе.

Один из довольно простых способов, который поможет выявить троянскую вирусную программу, с помощью, так называемого реестра, будет подробно рассмотрен в лабораторной работе. Помимо прочего есть способ, связанный со специальными программами, которые помогают в борьбе с вредоносной вирусной программой.

**Порядок выполнения работы**

**Задание 1**: восстановить файл, зараженный макровирусом.

Алгоритм выполнения работы. Для восстановления документов Word и Excel достаточно сохранить пораженные файлы в текстовый формат RTF, содержащий практически всю информацию из первоначальных документов и не содержащий макросы.

Для этого выполните следующие действия.

1. В программе WinWord выберите пункты меню «Файл» – «Сохранить как».

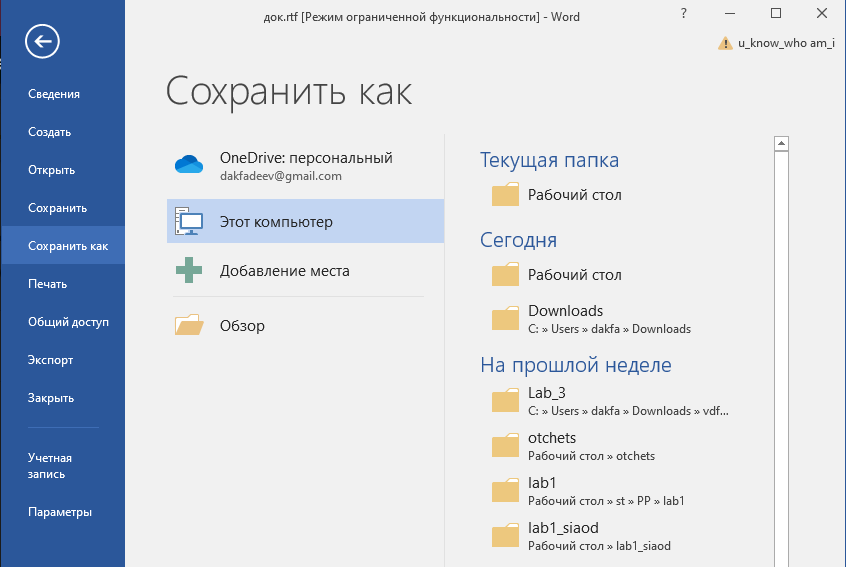


Рис 1. Выбор пункта «Сохранить как»

1. В открывшемся окне в поле «Тип файла» выберите «Текст в формате RTF» (Рис.2).

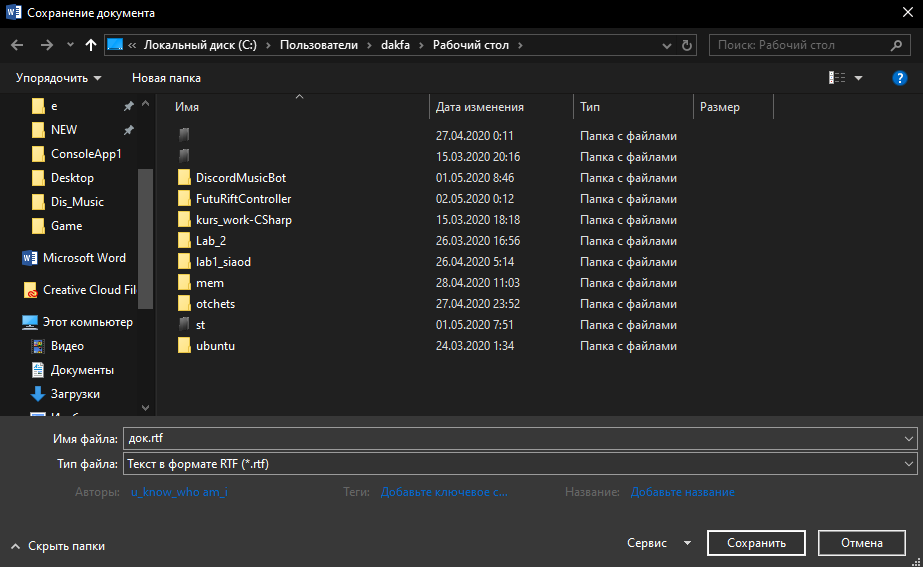


Рис 2. Выбор «Текст в формате RTF»

1. Выберите команду Сохранить, при этом имя файла оставьте прежним.
2. В результате появится новый файл с именем существующего, но с другим расширением.



Рис 3. Два файла с разными расширениями, но одинаковым названием

1. Далее, закройте WinWord и удалите все зараженные Word-документы и файл-шаблон NORMAL.DOT в папке WinWord.

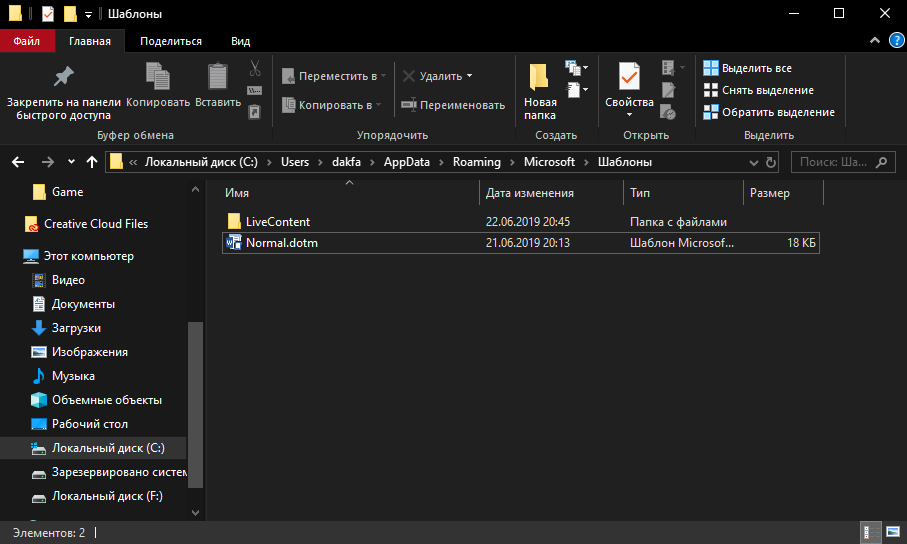


Рис 4. До удаления NORMAL.DOT

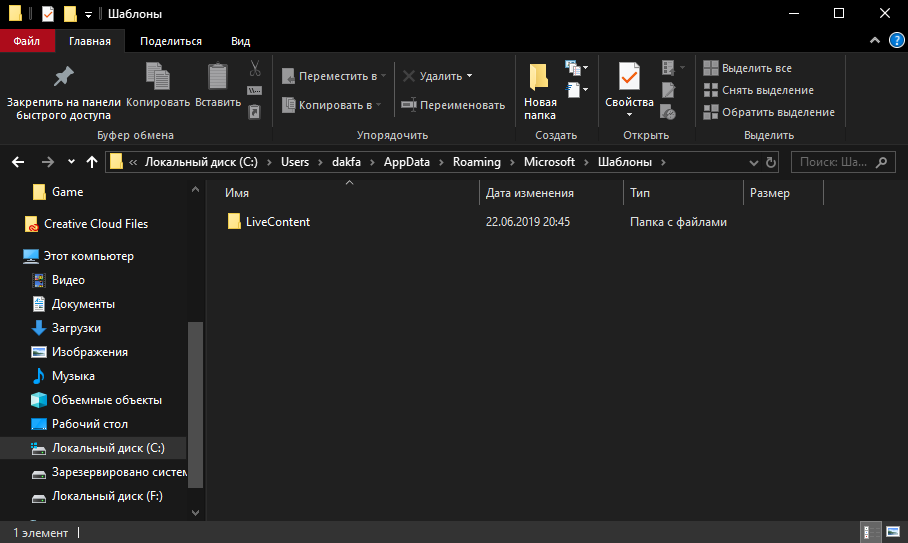
****

Рис 5. После удаления NORMAL.DOT

1. Запустите WinWord и восстановите документы из RTF-файлов в соответствующий формат файла с расширением (.doc).

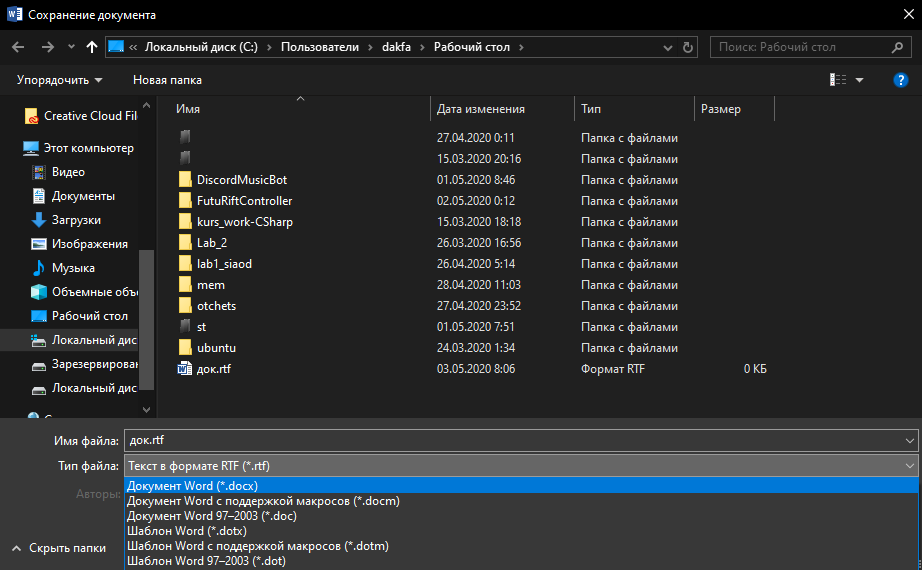


Рис 6. Выбор формата .doc и дальнейшее восстановление

1. В результате этой процедуры вирус будет удален из системы, а практически вся информация останется без изменений.

**Примечание**

* 1. Этот метод рекомендуется использовать, если нет соответствующих антивирусных программ.
  2. При конвертировании файлов происходит потеря невирусных макросов, используемых при работе. Поэтому перед запуском описанной процедуры следует сохранить их исходный текст, а после обезвреживания вируса – восстановить необходимые макросы в первоначальном виде.

1. Для последующей защиты файлов от макровирусов включите защиту от запуска макросов.
2. Для этого, в WinWord выберите последовательно пункты меню : Сервис – Макрос – Безопасность

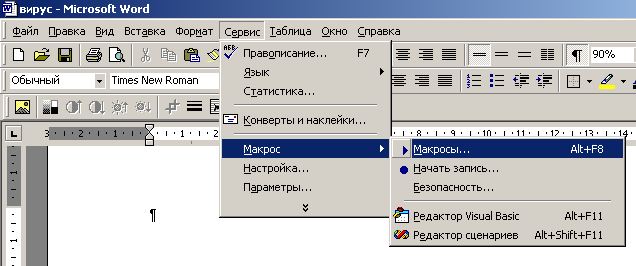


Рис 7. Пример, который вставлен в описание лабораторной работы номер 2.

Так как на данном компьютере установлен Microsoft Word 2016,в ней отсутствует пункт сервис – макрос – безопасность. Поэтому 9 и 10 выполняются по-другому.

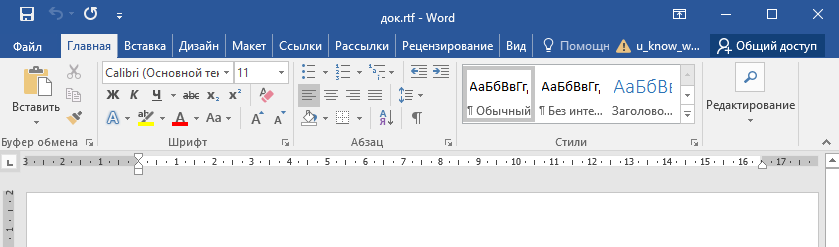


Рис 8. Доказательство, что Microsoft Word 2016 отсутствует сервис – макрос – безопасность

Чтобы выполнить данные пункты, надо зайти в “Файл” - “Параметры” - “Центр управления безопасностью”-“Параметры центра управления безопасностью”. Выбираем “Параметры макросов”

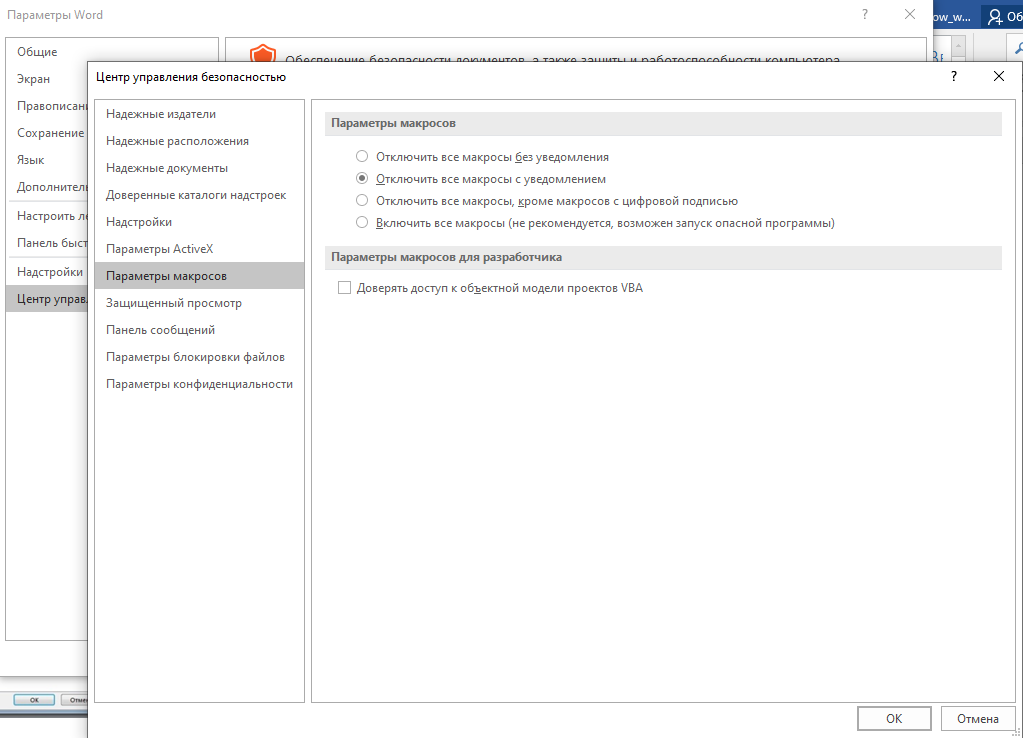


Рис 9. Описание пункт № 9.

1. В открывшемся окне на закладке Уровень безопасности отметьте пункт Высокая (Рис. 13).

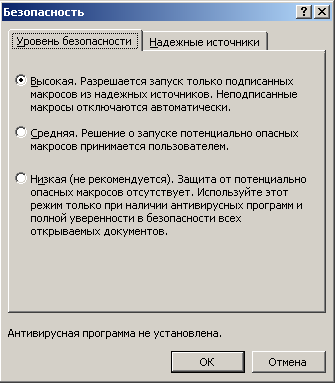


Рис 10. Пример решения пункта №10, который вставлен в описание лабораторной работы №2.

Так как на данном компьютере установлен Microsoft Word 2016, мы делаем вот так:

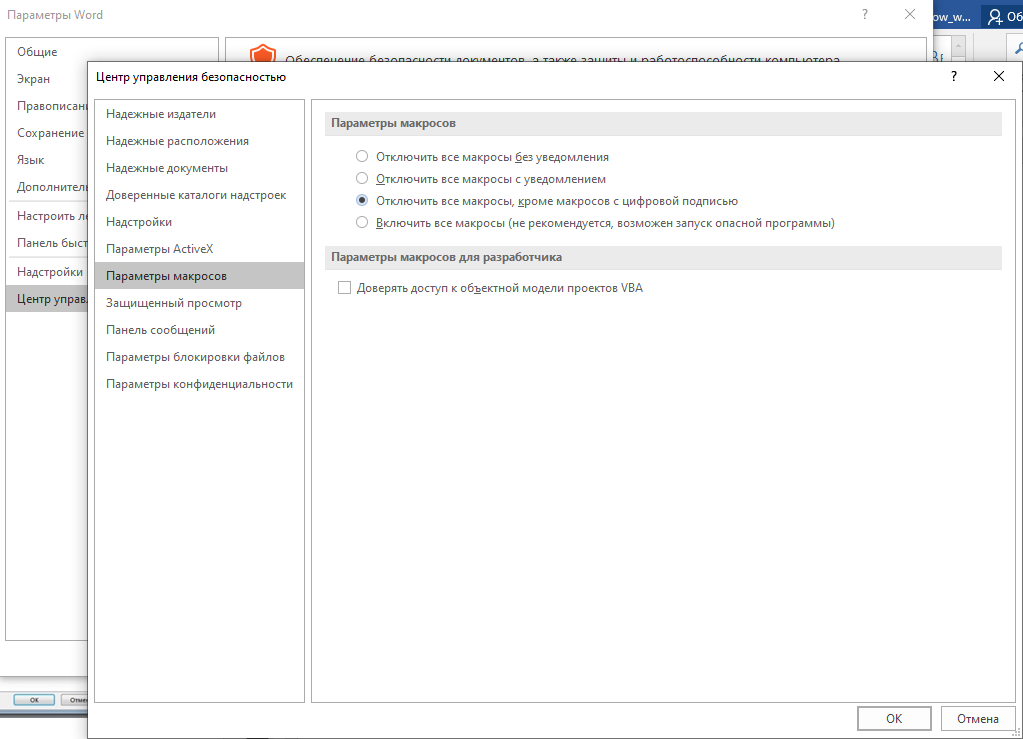


Рис 11. Описание пункт № 9.

Отмечаем третий кружок. Он является в данной версии пунктом “Высокая”.

**Задания для самостоятельной работы каждого студента**

1. Создайте файл virus.doc (содержание – чистый лист) и выполните алгоритм восстановления файла (в предположении его заражения макровирусом). Алгоритм выполнения представлен выше
2. Зафиксируйте этапы работы, используя команду PrintScreen клавиатуры (скопированные таким образом файлы вставьте в новый Word-документ для отчета преподавателю). Данный алгоритм зафиксирован выше.
3. Сравните размеры файлов virus.doc и virus.rtf, используя пункт контекстного меню Свойства (для этого выделить в Проводнике файл, нажмите правую кнопку мыши и выберите пункт Свойства).

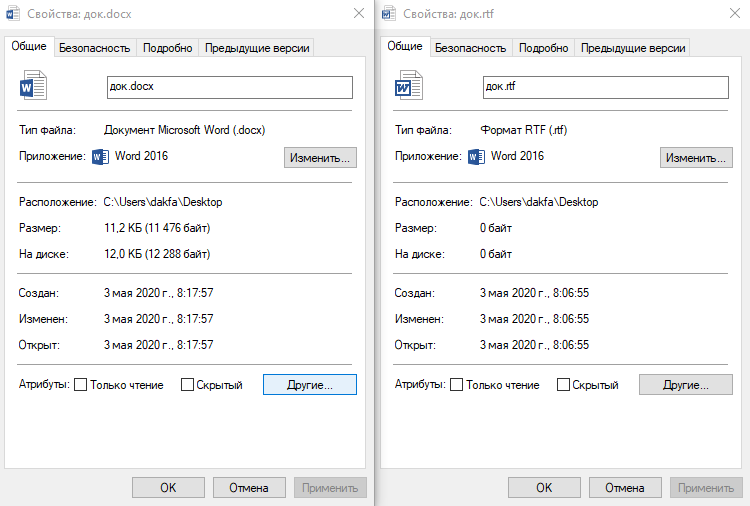


Рис 12. Сравнение размеров файлов virus.doc и virus.rtf

Задание 2: Профилактика проникновения «троянских программ»

В данной задании нужно было ознакомится с краткой теорией и сделать свои скриншоты. В этом задании не нужно было менять теорию.

Краткие теоретические сведения

Реестр операционной системы Windows — это большая база данных, где хранится информация о конфигурации системы. Этой информацией пользуются как операционная система Windows, так и другие программы. В некоторых случаях восстановить работоспособность системы после сбоя можно, загрузив работоспособную версию реестра, но для этого, естественно, необходимо иметь копию реестра. Основным средством для просмотра и редактирования записей реестра служит специализированная утилита «Редактор реестра».

Файл редактора реестра находится в папке Windows. Называется он regedit.exe. После запуска появится окно редактора реестра. Вы увидите список из 5 разделов:

HKEY\_CLASSES\_ROOT.

HKEY\_CURRENT\_USER.

HKEY\_LOCAL\_MACHINE.

HKEY\_USERS.

HKEY\_CURRENT\_CONFIG.

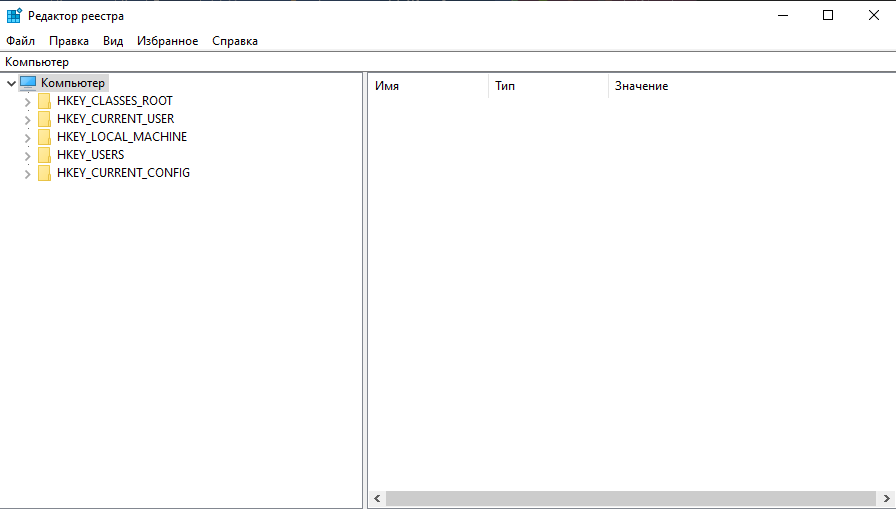


Рис 13. Запуск редактора реестра и изображение 5 разделов

Работа с разделами реестра аналогична работе с папками в Проводнике. Конечным элементом дерева реестра являются ключи или параметры, делящиеся на три типа:

* строковые (напр. «C:\Windows»);
* двоичные (напр. 10 82 A0 8F);
* DWORD – этот тип ключа занимает 4 байта и отображается в шестнадцатеричном и в десятичном виде (например, 0x00000020 (32)).

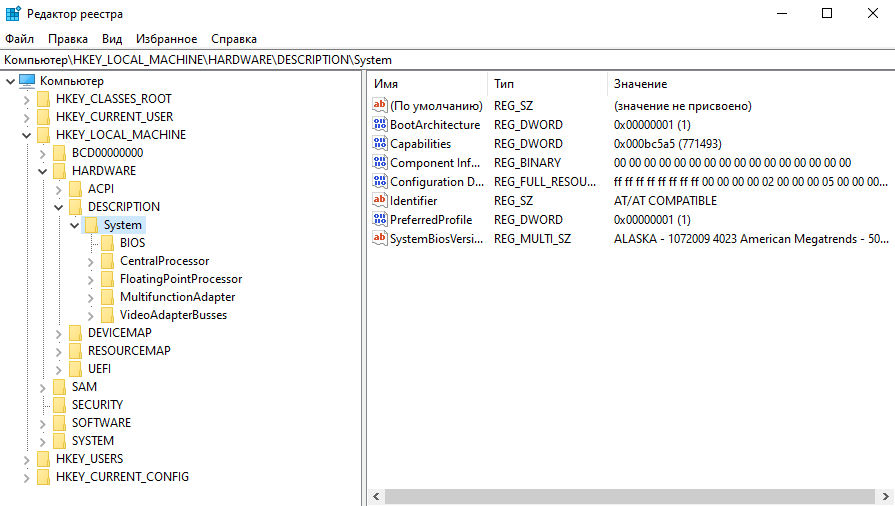
****

Рис 14. Запуск редактора реестра и изображение 5 разделов

В Windows системная информация разбита на так называемые ульи (hive). Это обусловлено принципиальным отличием концепции безопасности этих операционных систем. Имена файлов ульев и пути к каталогам, в которых они хранятся, расположены в разделе HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist.

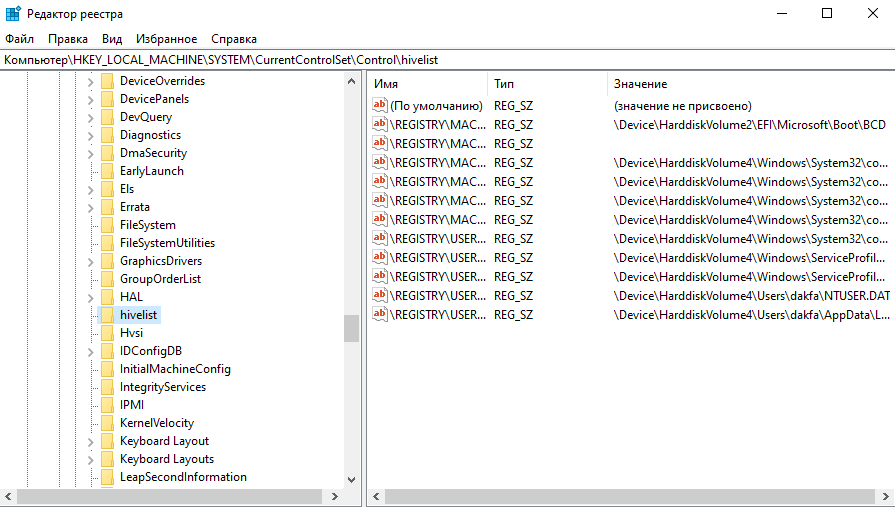


Рис 15.HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist

В таблице 1 даны краткие описания ульев реестра и файлов, в которых хранятся параметры безопасности.

### Таблица 1 Характеристика основных разделов системного реестра

|  |  |
| --- | --- |
| **HKEY\_LOCAL\_MACHINE\SAM** | Содержит информацию SAM (Security Access Manager), хранящуюся в файлах SAM, SAM.LOG, SAM.SAV в папке \%Systemroot%\System32\Config |
| **HKEY\_LOCAL\_MACHINE\SECURITY** | Содержит информацию безопасности в файлах SECURITY, SECURITY.LOG, SECURITY.SAV в папке \%Systemroot%\System32\Config |
| **HKEY\_LOCAL\_MACHINE\SYSTEM** | Содержит информацию об аппаратных профилях этого подраздела. Информация хранится в файлах SYSTEM, SYSTEM.LOG, SYSTEM.SAV в папке \%Systemroot%\System32\Config |
| **HKEY\_CURRENT\_CONFIG** | Содержит информацию о подразделе System этого улья, которая хранится в файлах SYSTEM.SAV и SYSTEM.ALT в папке \%Systemroot%\System32\Config |
| **HKEY\_USERS\.DEFAULT** | Содержит информацию, которая будет использоваться для создания профиля нового пользователя, впервые регистрирующегося в системе. Информация хранится в файлах DEFAULT, DEFAULT.LOG, DEFAULT.SAV в папке \%Systemroot%\System32\Config |
| **HKEY\_CURRENT\_USER** | Содержит информацию о пользователе, зарегистрированном в системе на текущий момент. Эта информация хранится в файлах NTUSER.DAT и NTUSER.DAT.LOG, расположенных в каталоге \%Systemroot%\Profiles\Username, где Username – имя пользователя, зарегистрированного в системе на данный момент |

**Задание 3:** Проверить потенциальные места записей «троянских программ» в системном реестре операционной системы Windows.

Алгоритм выполнения работы

Потенциальными местами записей «троянских программ» в системном реестре являются разделы, описывающие программы, запускаемые автоматически при загрузке операционной системы от имени пользователей и системы.

1. Запустите программу regedit.exe.

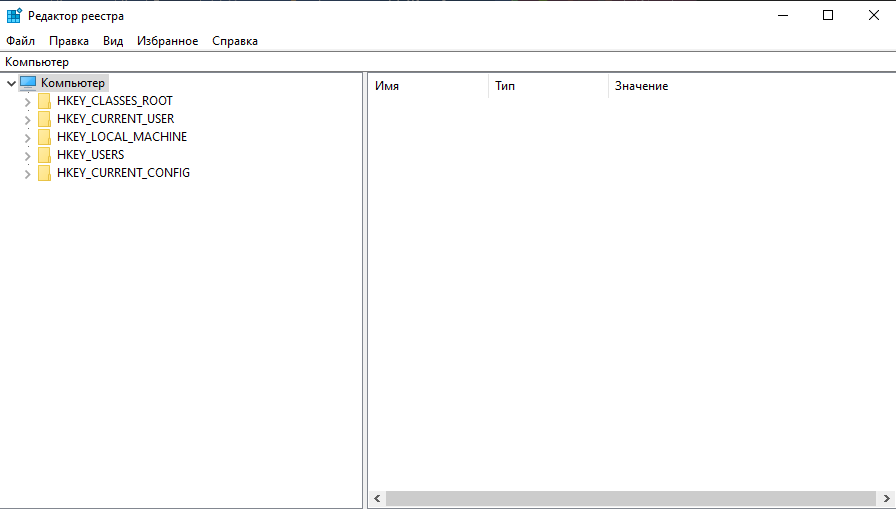


Рис 16. Запуск программ regedit.exe.

1. В открывшемся окне выберите ветвь HKEY\_LOCAL\_MACHINE и далее Software\Microsoft\WindowsNT\CurrentVersion\Winlogon.
2. В правой половине открытого окна программы regedit.exe появится

список ключей.

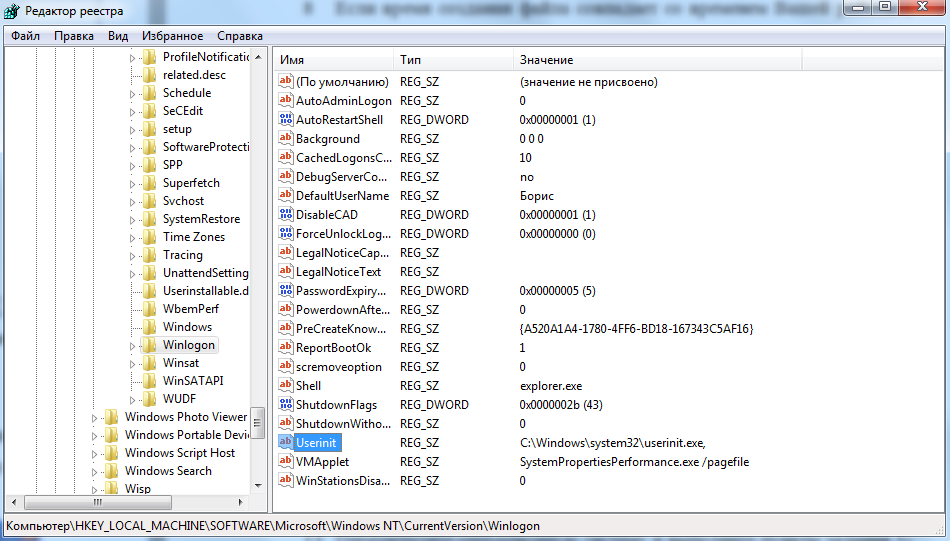


Рис 17. Нахождение ключа Userinit (REG\_SZ)

1. По умолчанию (исходное состояние) – этот ключ содержит следующую запись C:\WINDOWS\system32\userinit.exe.

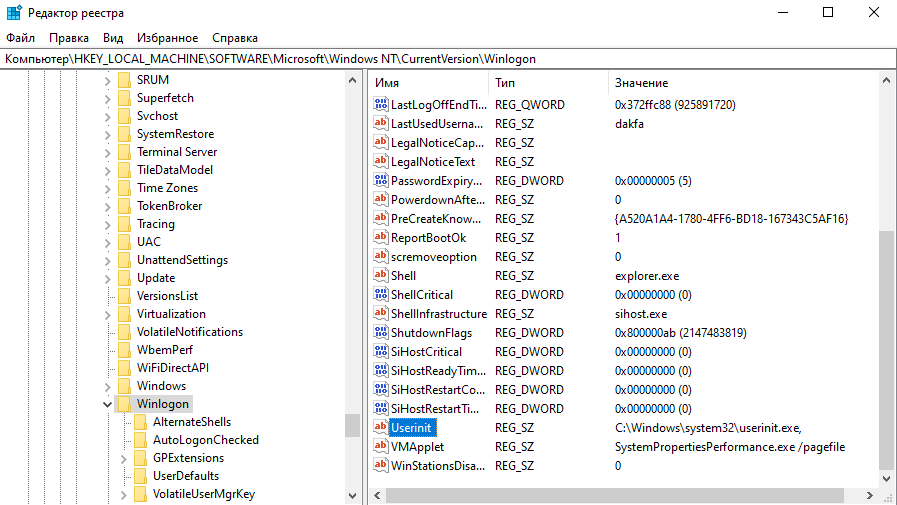


Рис 18. Проверка ключа на значение C:\WINDOWS\system32\userinit.exe

1. Если в указанном ключе содержатся дополнительные записи, то это могут быть троянские программы. Дополнительных записей в ключе нет.

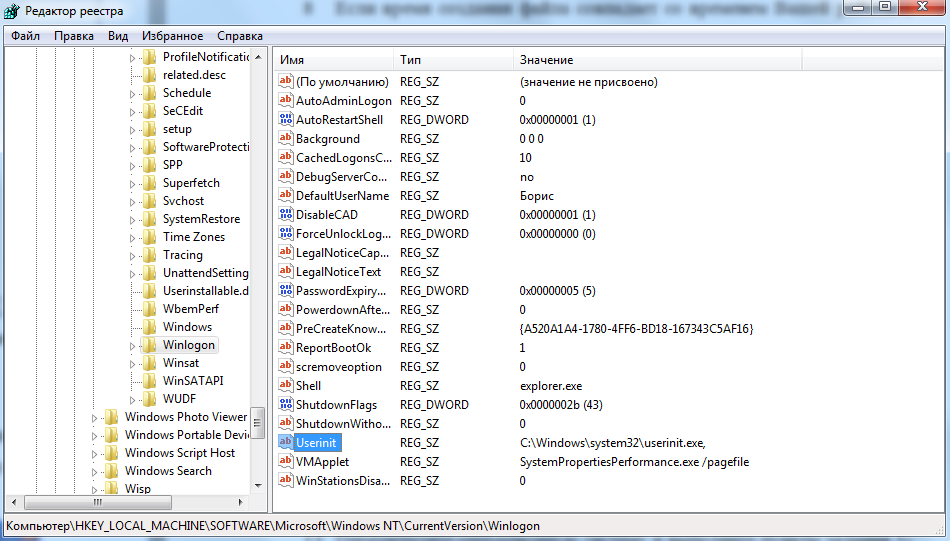


Рис 19. Проверка ключа на дополнительное значение

1. В этом случае проанализируйте место расположения программы, при этом обратите внимание на время создания файла и сопоставьте с Вашими действиями в это время. Дополнительных записей в ключе нет.
2. Если время создания файла совпадает со временем Вашей работы в Интернете, то возможно, что в это время Ваш компьютер был заражен троянским конем. Дополнительных записей в ключе нет.
3. Для удаления этой записи необходимо дважды щелкнуть на названии ключа (или при выделенном ключе выбрать команду Изменить из меню Правка программы regedit.exe). Дополнительных записей в ключе нет.
4. В открывшемся окне в поле Значение удалите ссылку на подозрительный файл. Дополнительных записей в ключе нет.
5. Закройте программу regedit.exe. Дополнительных записей в ключе нет.
6. Перейдите в папку с подозрительным файлом и удалите его. Дополнительных записей в ключе нет.
7. Перезагрузите операционную систему и выполните пункты задания 1-4. Дополнительных записей в ключе нет.
8. Если содержимое, рассматриваемого ключа не изменилось, то предполагаемый «троянский конь» удален из Вашей системы. Дополнительных записей в ключе нет!

С пункта 7-14 Дополнительных записей нет.

Еще одним потенциальным местом записей на запуск «троянских программ» является раздел автозапуска Run.

Для его проверки выполните следующее.

1. Запустите программу regedit.exe.

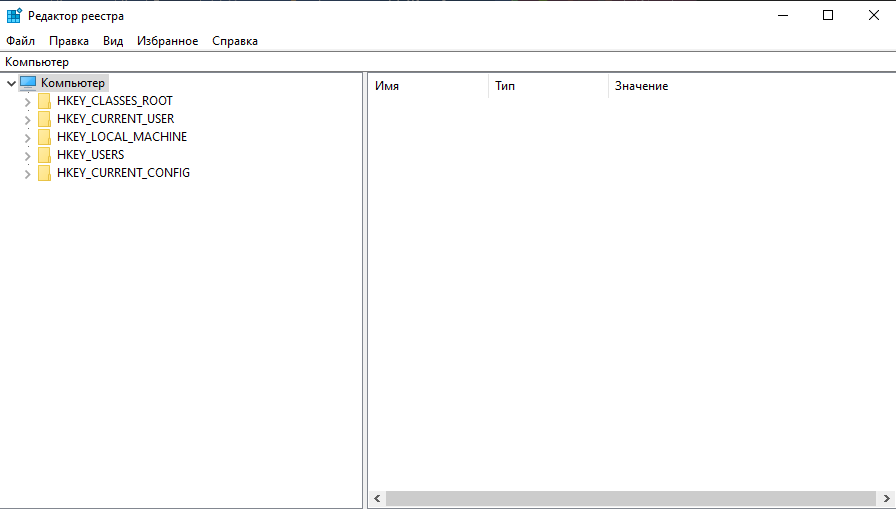


Рис 20. Запуск программы regedit.exe.

1. В открывшемся окне выберите ветвь HKEY\_LOCAL\_MACHINE и далее Software\Microsoft\Windows\CurrentVersion\Run\... (REG\_SZ) (Рис.25).

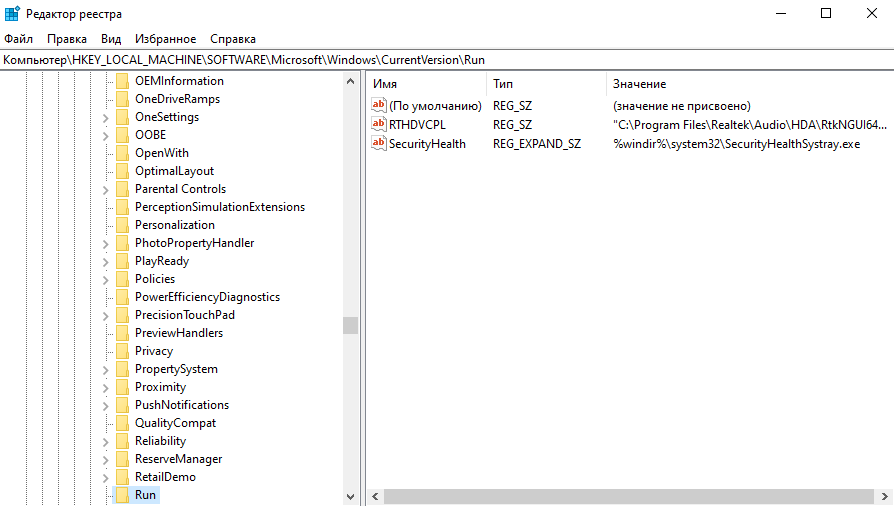


Рис 21. Выбор ветви Run

1. В рассматриваемом примере автоматически запускается резидентный антивирус и его планировщик заданий, а также утилита, относящаяся к программе Nero (запись на CD).
2. Если в указанном разделе есть записи вызывающие подозрения, то выполните пункты 6-14 предыдущего задания. Подозрений никаких нет

**Задания для самостоятельной работы**

1. Проверьте содержимое ключа HKEY\_LOCAL\_MACHINE \Software\Microsoft\Windows\CurrentVersion\Winlogon\System(REG\_SZ). Задание сделано выше.
2. Зафиксируйте этапы работы, используя команду PrintScreen клавиатуры. Данное задание зафиксировано выше.
3. Добавьте итоги в отчет.

**Вывод:**

В ходе выполнения лабораторной работы были рассмотрены основные понятия: макровирус, троянская вирусная программа. Следует заметить, данные понятия различаются. Каждый из данных терминов имеет свои принципы работы, способы распространения, а также способы борьбы с данными вирусами.

Так как информационные технологии развиваются быстрым темпам. Люди должны успевать за темпом, который устанавливает общество. В современном мире почти каждый человек сталкивается с опасностями, связанными с информацией. Каждый пользователь должен понимать что вся информация, хранящаяся допусти на компьютере или на каком-то носителя, всегда может подвергаться хищению или повреждению, с целью использования данной информации в других целях. Поэтому люди должны аккуратно пользоваться интернетом, не скачивать файлы с подозрительных сайтов, ведь данные файлы, могут содержать вирус, который в дальнейшем будет проблематично удалить. Для хоть какой-то защиты, пользователи должны скачивать антивирус, который поможет отсканировать файлы на наличие встроенных вредоносных программ.

В период выполнения работы освоен некоторый перечень знаний необходимый для лучшего понимания темы. В дальнейшем данная информация может помочь людям на протяжении всей жизни, решать проблемы связанные с вирусами, а так же восстановлением поврежденных файлов. Человек, не владеющий данными знаниями, может легко допустить ошибку в решении определенных проблем, связанных с вирусами.

**Ответы на контрольные вопросы**

1. Какие файлы заражают макровирусы?

**Ответ:** Следует из определения. Макровирусы – это потенциально нежелательные утилиты, написанные на микроязыках, которые встроены в графические и текстовые системы обработки. Поэтому наибольшее распространение получили макровирусы для файлов Microsoft Word, Excel и Office 97.

1. Как просмотреть код макровируса?

**Ответ**: В Microsoft Word находим в панели управления “Вид” – “Макросы”. Дальше открывается панель “Макросы”, выбираем макрос. Далее увидим код, тоже самое в любом другом офисном приложении.

1. Как восстановить файл, зараженный макровирусом?

**Ответ:** Для восстановления документов Word и Excel достаточно сохранить пораженные файлы в текстовый формат RTF, содержащий всю информацию из первоначальных документов и не содержащий макросы.

1. Что такое реестр?

**Ответ:** Реестр представляет собой специальную базу данных. В нем имеется информация, касающаяся оборудования, программного обеспечения, а также многое другое. В процессе функционирования системы происходит постоянное обращение к этой информации. Она может изменяться или дополняться, в зависимости от конкретных действий. Подобные мероприятия происходят в автоматическом порядке, пользователю нет необходимости беспокоиться об их выполнении.

1. Поясните особенности «троянских программ».

**Ответ:** Вирус троянский конь – это разновидность шпионского ПО. Основная особенность троянских программ – это замаскированный сбор конфиденциальной информации и передача третьей стороне. К ней относятся реквизиты банковских карт, пароли для платежных систем, паспортные данные и другие сведения. Вирус троян по сети не распространяется, не производит уничтожение данных, не делает фатального сбоя оборудования. Алгоритм этой вирусной утилиты не похож на действия уличного хулигана, который все на своем пути разрушает. Троян – это диверсант, сидящий в засаде, и ждущий своего часа.

1. Почему профилактика «троянских программ» связана с системным реестром?

**Ответ:** Можно легко понять, если на компьютере «троянские программы» или нет. Сделав всего лишь проверку на значение ключа в определенном разделе, если есть какие-то отличия от правильного значения, тогда скорее всего на вашем компьютере присутствуют «троянские программы».

1. Какие разделы и ключи являются потенциальными местами записей «троянских программ»?

**Ответ:** Потенциальными местами для записей «троянских программ» являются разделы, описывающие программы, запускаемые автоматически при загрузке операционной системы от имени пользователей и системы. Одним из ключей является Userinit, который может отличаться от исходного значения. Помимо прочего одним потенциальным местом является раздел автозапуска Run.В этом разделе надо проверить ключи на подозрительность.

1. Какое расширение у файла реестра?

**Ответ:** Файлы реестра по умолчанию имеют расширение .reg(REG\_SZ), которое ассоциировано с приложением Regedit. Если выполнить двойной щелчок мышью, указав на файл с расширением .reg, программа Regedit прочтет этот файл и вставит его содержимое в реестр.

**Ответы на контрольные вопросы по вариантам:**

|  |  |
| --- | --- |
| № варианта | Номера вопросов, на которые нужно привести письменные ответы |
| 3 | 3, 7, 9, 12, 13, 17, 22, 27, 31, 36, 38 |

3. Что такое файл и файловая система? Перечислите типы файлов.

**Ответ:** Файл — это определенное количество информации, имеющее имя и хранящееся в долговременной памяти. Файловая система — это система хранения файлов и организации каталогов. Типы файлов: видеофайлы, текстовые файлы, изображения, аудиофайлы, исполняемые файлы, архивы.

7. Где хранится файл настроек расположения файлов и ярлыков рабочего стола?

**Ответ:** %SystemDrive%Documents and Settings<Username>Ntuser.dat, а все изменения, которые происходят в этом файле, записаны здесь — %SystemDrive%Documents and Settings<Username> ntuser.dat.LOG

9.Укажите путь к общему рабочему столу

**Ответ:** C:\Users\Public\Desktop

1. По каким направлениям строиться работа с графикой в текстовом процессоре Word?

**Ответ:** Работа с графикой в процессоре Word может строиться по трем

направлениям:

1. Вставка объекта, созданного в другом графическом редакторе

(Paint,MsDrawing,Paintbrush)

2) Рисование в самом документе (воспользовавшись инструментами

панели Рисование).

1. Использование готовых рисунков из коллекции Clipart для

оформления текстов.

1. Что такое OLE – технологии?

**Ответ:** OLE (англ. Object Linking and Embedding) — технология связывания и внедрения объектов в другие документы и объекты, разработанные корпорацией Майкрософт. OLE позволяет передавать часть работы от одной программы редактирования к другой и возвращать результаты назад. Например, установленная на персональном компьютере издательская система может послать некий текст на обработку в текстовый редактор, либо некоторое изображение в редактор изображений с помощью OLE-технологии.

17. Как сменить обои рабочего стола в Windows 7.

**Ответ:**

1)Кликните правой кнопкой мышки в любом свободном месте рабочего стола для вызова контекстного меню.

2) Выберите пункт «Персонализация»

3) В окне настроек персонализации щелкните внизу по ссылке «Фон рабочего стола»

4) В открывшемся окне выберите одно или несколько изображений и нажмите кнопку «Сохранить изменения»

22. Как добавить в область «Закреплено» новую папку

**Ответ:**

Для добавления папки в данную область, необходимо перетащить папку на панель задач и при появлении надписи «Закрепить в Проводнике» отпустить ее.

27. Как определить тип процессора и объем памяти Вашего компьютера?

**Ответ:** Для определения типа процессора и объема оперативной памяти необходимо на нажать правой кнопкой мыши по вкладке «Мой компьютер», находящейся в меню «Пуск» или на рабочем столе и выбрать пункт «Свойства»

31. Вы перетащили значок файла левой кнопкой мыши из одной папки в другую в пределах диска C:\ . Какое действие произошло?

**Ответ:** При перетаскивании файла из одного места в другое на одном физическом диске (из C:\docs в C:\files) Windows перемещает объект.

36. Корзина в Windows используется для?

**Ответ:** Корзина — элемент графического интерфейса пользователя, предназначенный для удаления и, часто, временного хранения удалённых объектов (в некоторых реализациях — только файлов и каталогов). Корзина позволяет восстановить недавно удалённый объект в случае ошибочного удаления.

1. Стандартная в ОС Windows программа Paint???

**Ответ:** Paint — Простой растровый графический редактор, стандартная программа, входящая в состав всех версий Windows. Paint также часто упоминается как MS Paint или Microsoft Paint. Позволяет создавать рисунки, картинки и т.д. или редактировать изображения. Кроме того, его можно использовать для сохранения графических файлов в различных форматах.

**Список источников**

Интернет ресурсы

1. Понятие, принцип работы, обнаружение макровируса. Чума компьютерного века. [Электронный ресурс] Режим доступа: [https://www.sites.google.com/site/gimnazia35/home/komputernye-virusy/kak-rabotaut-virusy/makrovirusy](https://www.sites.google.com/site/gimnazia35/home/komputernye-virusy/kak-rabotaut-virusy/makrovirusy%20) (дата обращения 15.04.2020г.)
2. История макровируса. Kaspersky. [Электронный ресурс] Режим доступа: <https://www.kaspersky.ru/resource-center/definitions/macro-virus> (дата обращения 15.04.2020г.)
3. Принцип работы макровируса и процедуры лечения зараженных файлов. КомпьютерМастер. [Электронный ресурс] Режим доступа: [https://computermaster.ru/articles/virmacro.html](https://computermaster.ru/articles/virmacro.html%20) (дата обращения 15.04.2020г.)
4. Троянская вирусная программа. Wikipedia. [Электронный ресурс] Режим доступа: [https://ru.wikipedia.org/wiki/Троянская\_программа](https://ru.wikipedia.org/wiki/Троянская_программа%20) (дата обращения 15.04.2020г.)