**ПРАВИТЕЛЬСТВО САНКТ-ПЕТЕРБУРГА**

**КОММИТЕТ ПО НАУКЕ И ВЫСШЕЙ ШКОЛЕ**

**Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение**

**«Санкт-Петербургский технический колледж управления и коммерции»**

**Отделение «Электроники и машиностроения»**

**ОТЧЕТ**

**Лабораторно-практическая работа№ 13**

**по курсу «Защита информации в автоматизированных системах»**

**«Изучение реестра. Потенциальные места нахождения вируса «Троян»**

**Группа: 9СК-41**

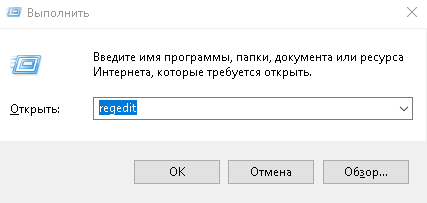
**Студент: Башмаков М.Ю.**

**Санкт-Петербург**

2020

Для выявления возможного заражения компьютера трояном

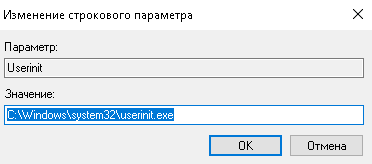
Необходимо проверить его реестр, для начала необходимо проверить одно из возможных мест пройдя по следующему пути:

1. Открыть реестр:
2. Далее необходимо пройти по следующему пути:



1. Затем было бы не плохо открыть свойства Winlogon, и найти строку Userprint



1. Проверить совпадает ли значение ключа со стандартным ( По умолчанию (исходное состояние) 151 этот ключ содержит следующую запись C:\WINDOWS\ system32\userinit.exe) 
2. В случае если значения ключа не совпадает необходимо провести следующие действия:
3. Если в указанном ключе содержатся дополнительные записи, то это могут быть «троянские программы».
4. В этом случае проанализируйте место расположения программы, обратите внимание на время создания файла и сопоставьте с Вашими действиями в это время.
5. Если время создания файла, совпадает со временем Вашей работы в Интернете, то возможно, что в это время Ваш компьютер был заражен «троянским конем».
6. Для удаления этой записи необходимо дважды щелкнуть на названии ключа (или при выделенном ключе выбрать команду изменить из меню Правка программы regedit.exe).
7. В открывшемся окне в поле Значение (рисунок) удалите ссылку на подозрительный файл.
8. Закройте программу regedit.exe.
9. Перейдите в папку с подозрительным файлом и удалите его.
10. Перезагрузите операционную систему и выполните пункты задания 1—4.
11. Если содержимое рассматриваемого ключа не изменилось, то предполагаемый «троянский конь» удален из Вашей системы.
12. Еще одним потенциальным местом записей на запуск «троянских программ» является раздел автозапуска Run.
13. Для этого необходимо в реестре пройти по следующему пути 
14. В данном разделе реестра сохраняются пути всех программ, запускаемых вместе с ОС. В случае если вы обнаружили тут странные и подозрительные программы необходимо провести следующие действия:
15. Если в указанном ключе содержатся дополнительные записи, то это могут быть «троянские программы».
16. В этом случае проанализируйте место расположения программы, обратите внимание на время создания файла и сопоставьте с Вашими действиями в это время.
17. Если время создания файла, совпадает со временем Вашей работы в Интернете, то возможно, что в это время Ваш компьютер был заражен «троянским конем».
18. Для удаления этой записи необходимо дважды щелкнуть на названии ключа (или при выделенном ключе выбрать команду изменить из меню Правка программы regedit.exe).
19. В открывшемся окне в поле Значение (рисунок) удалите ссылку на подозрительный файл.
20. Закройте программу regedit.exe
21. Перейдите в папку с подозрительным файлом и удалите его.
22. Перезагрузите операционную систему и выполните пункты задания 1—4.
23. Если содержимое рассматриваемого ключа не изменилось, то предполагаемый «троянский конь» удален из Вашей системы.

Контрольные вопросы

1)Что такое реестр?

Иерархически построенная база данных параметров и настроек в большинстве операционных систем Microsoft Windows.

2)Поясните особенности «троянских программ».

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.

3)Почему профилактика «троянских программ» связана с системным реестром?

Т.к. троян маскируется под полезное или не очень ПО, а в реестре имеется список всего ПО

4)Какие разделы и ключи являются потенциальными местами записей «троянских программ»?

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

Userinit (REG\_SZ)

Run\... (REG\_SZ)

Т.Е. те проверка которых была описана выше