**Министерство образования и науки Российской Федерации**

**«Национальный исследовательский университет «МИЭТ»**

**Кафедра «Информационная безопасность»**

**ДИСЦИПЛИНА**

**«Технологии защиты информации   
от несанкционированного доступа»**

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ**

**по проведению лабораторной работы № 01**

«**Выявление угроз несанкционированного доступа**

**к конфиденциальной информации**»

**Москва, 2021**

**1 Практическая часть**

## 1.1 Контроль уязвимости ОС в процессе инициализации

1 Загрузить операционную систему и попробовать войти в операционную систему методом перебора паролей.

-> 3.Password and Registry Tools -> Active@ Password Changer.

5 Выбрать путь диск с установленной Windows

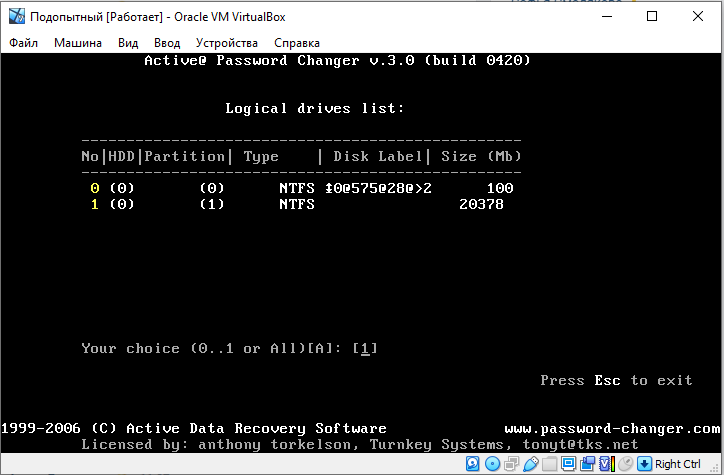


Рисунок 1 – Программа Active@ Password Changer

6 После автоматического поиска файла с паролями выбрать пользователя с паролем.

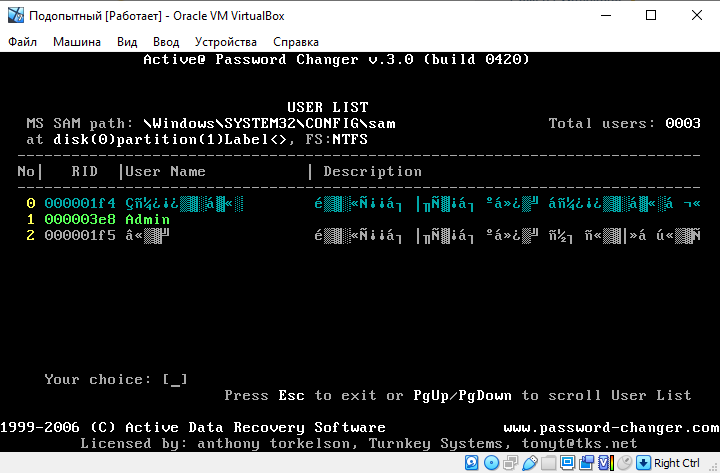


Рисунок 2 – Меню выбора пользователя

7 Выбрать соответствующий пункт, позволяющий стереть пароль.

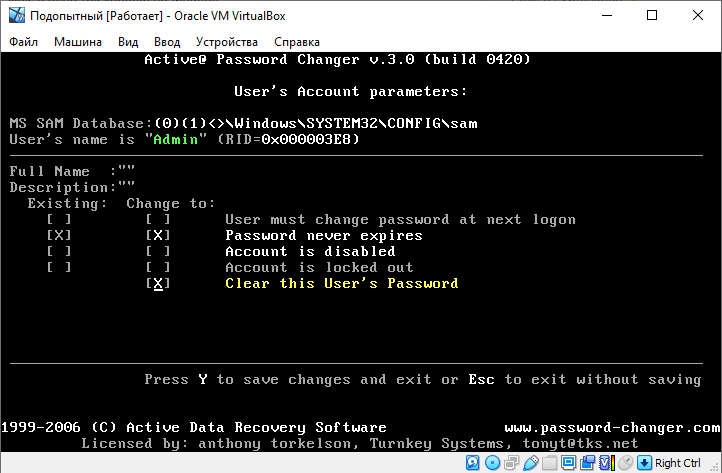


Рисунок 3 – Операции с паролем пользователя

8 Перезагрузить ОС.

9 Сделать выводы.

**Вывод:** Пароль был успешно сброшен. Именно из-за простоты сброса паролей в винде без дополнительной защиты и необходимо ставить пароль на биос и/или дополнительные средства доверенной загрузки

## 1.2 Контроль запуска программ

*Автозагрузка в меню Пуск*

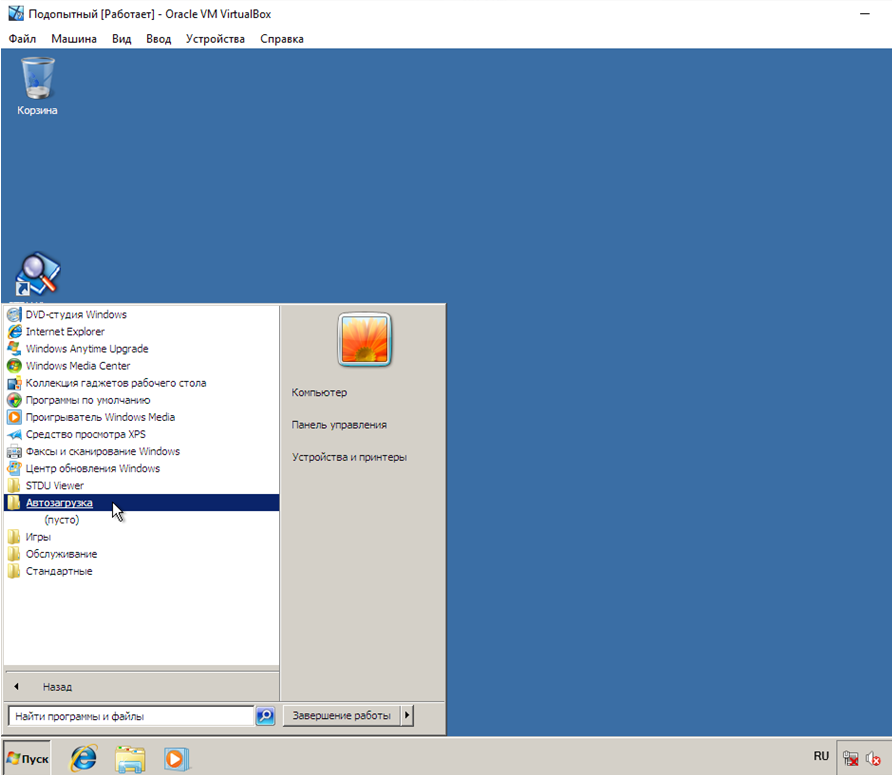


Рисунок 4 – Автозагрузка в меню Пуск

*Системный реестр Windows*

1 Вызвать системную утилиту regedit.exe.

2 Просмотреть ветки автозапуска

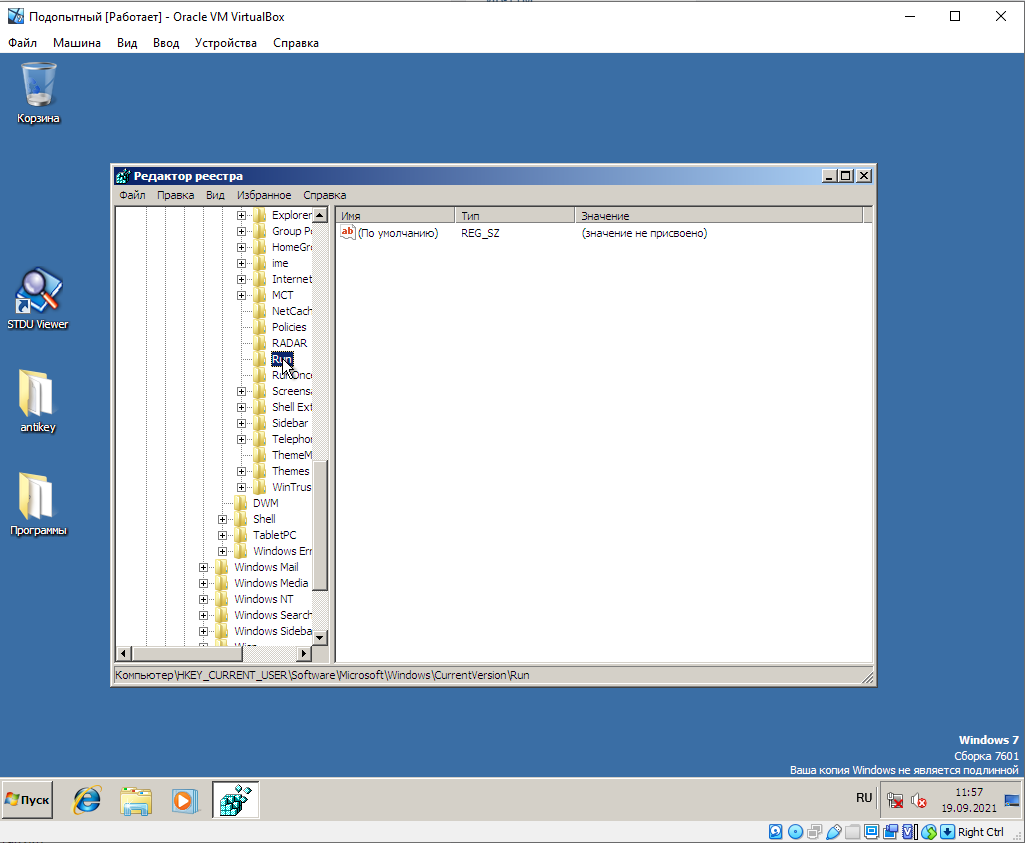


Рисунок 5 – ветка ключейHKCU\Software\Microsoft  
\Windows\CurrentVersion\Run

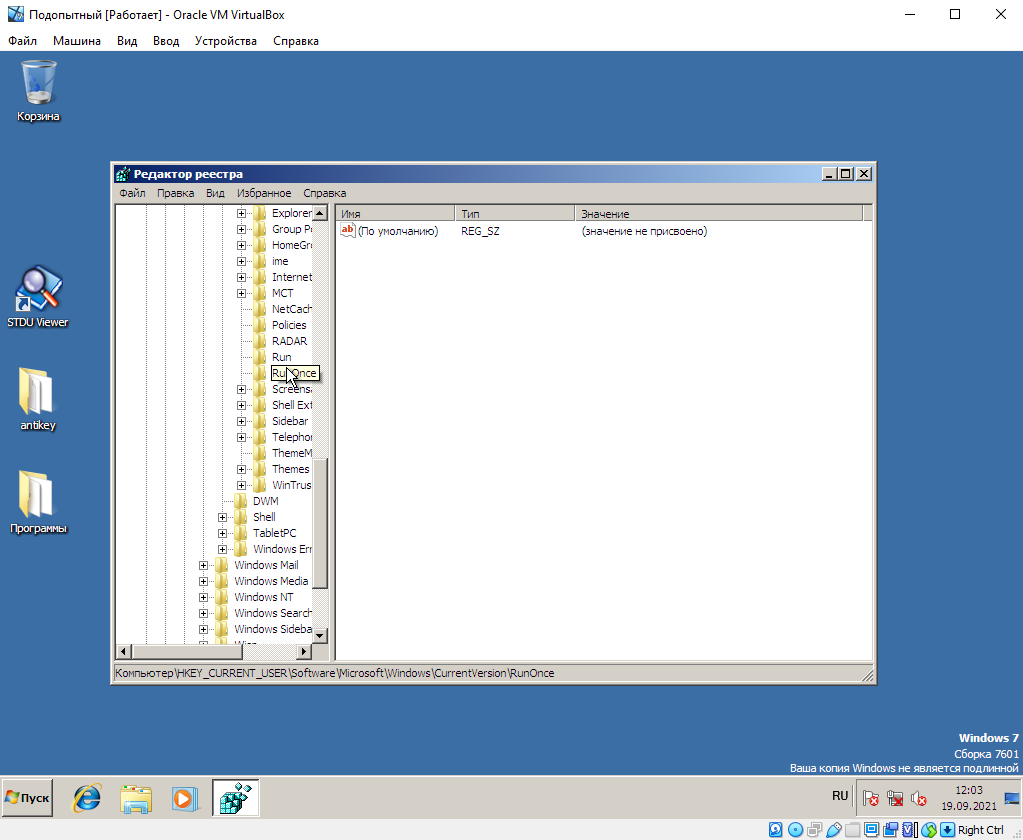


Рисунок 6 – ветка ключейHKCU\Software\Microsoft  
\Windows\CurrentVersion\RunOnce

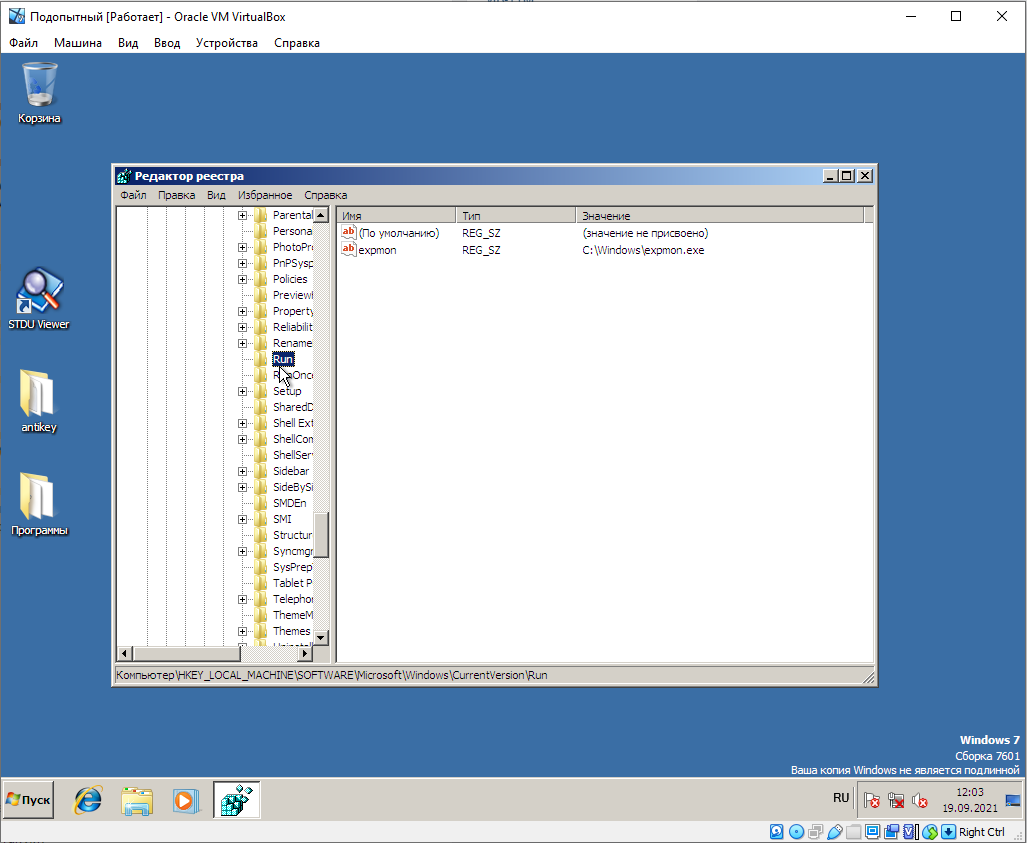


Рисунок 7 – ветка ключейHKLM\Software\Microsoft  
\Windows\CurrentVersion\Run

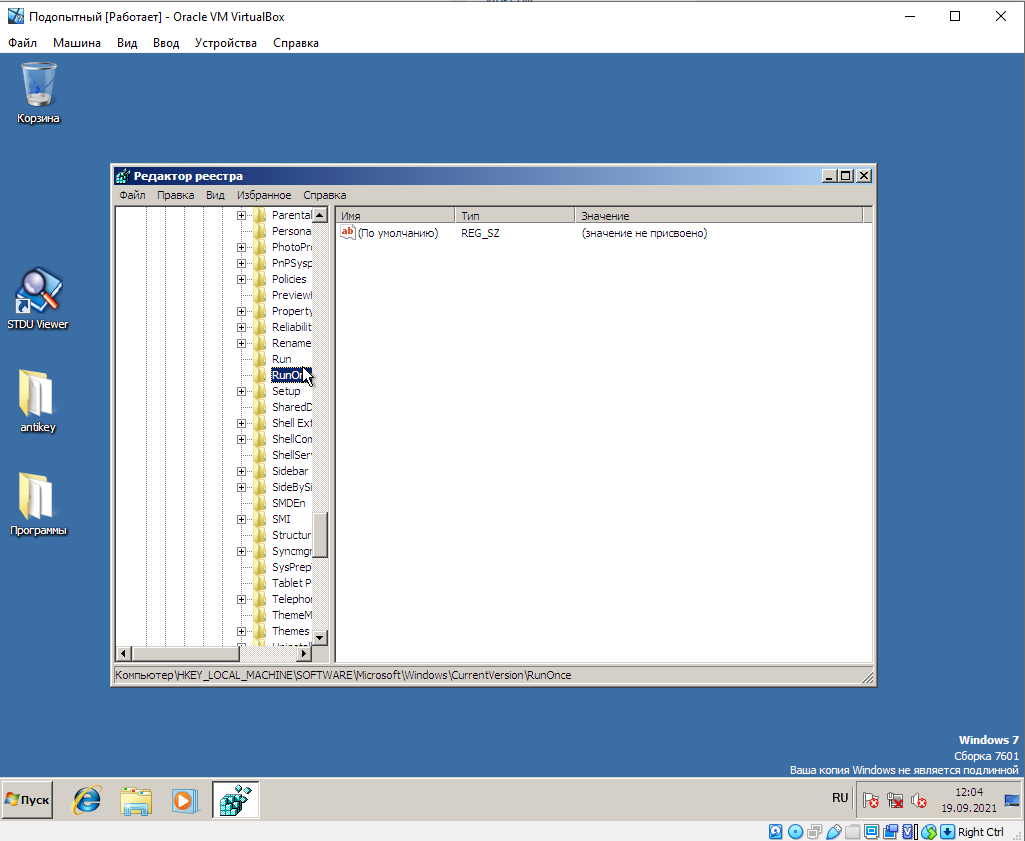


Рисунок 8 – ветка ключейHKLM\Software\Microsoft  
\Windows\CurrentVersion\RunOnce

**Отсутствует в предоставленной системе**

Рисунок 9 – ветка ключейHKLM\Software\Microsoft  
\Windows\CurrentVersion\RunOnceEx

*Конфигурационные файлы win.ini и system.ini*

1 Открыть системные файлы Windows - system.ini и win.ini

2 Просмотреть список программ запуска в файле win.ini

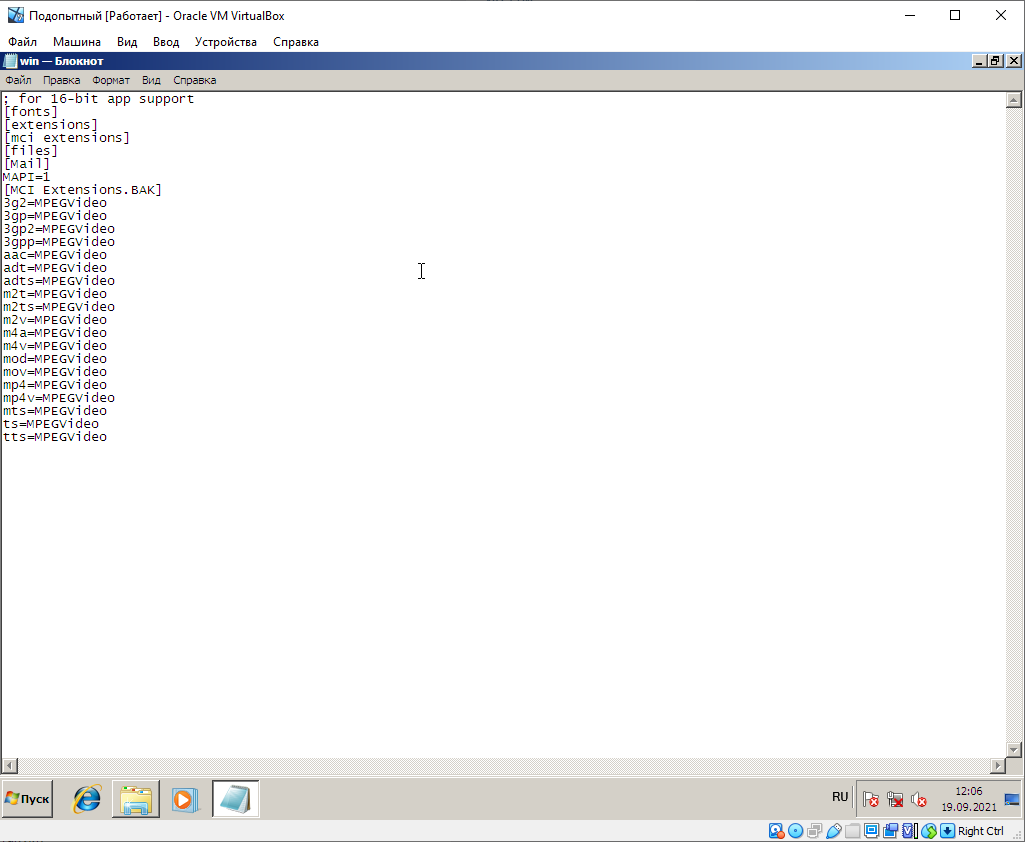


Рисунок 10 – Файл win.ini

3 Просмотреть список программ запуска в файле system.ini

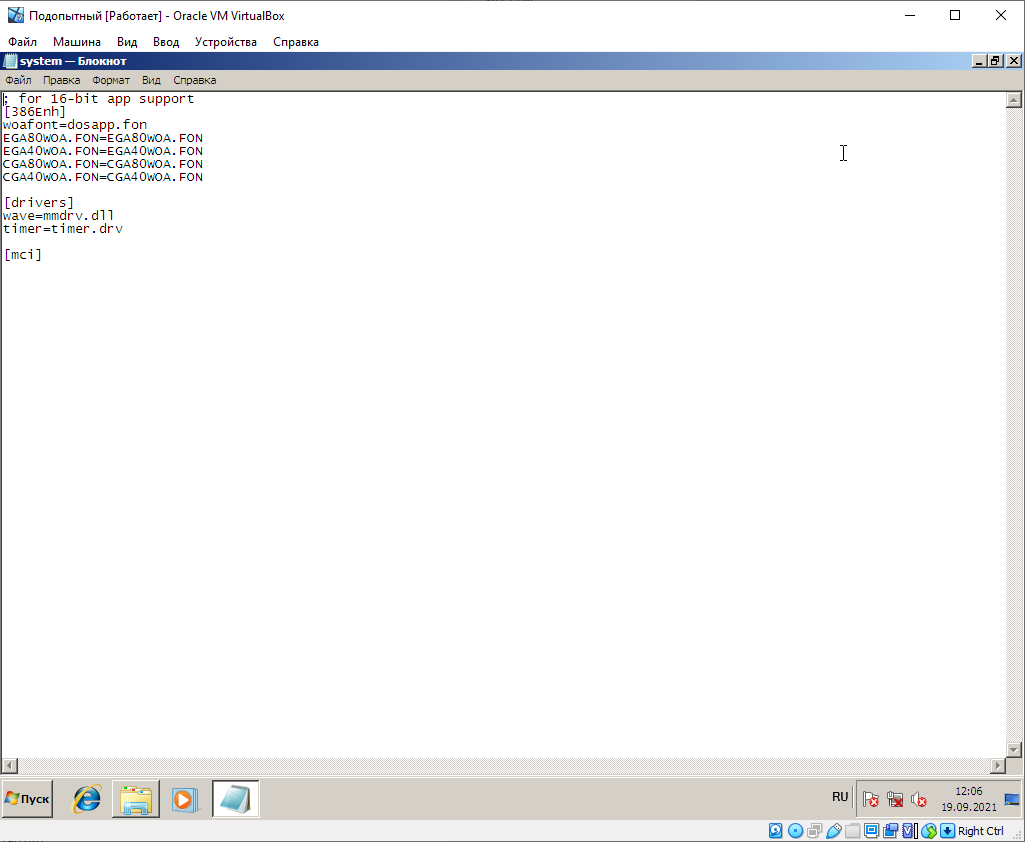


Рисунок 11– Файл system.ini

4 Открыть утилиту msconfig и просмотреть загружаемое содержимое

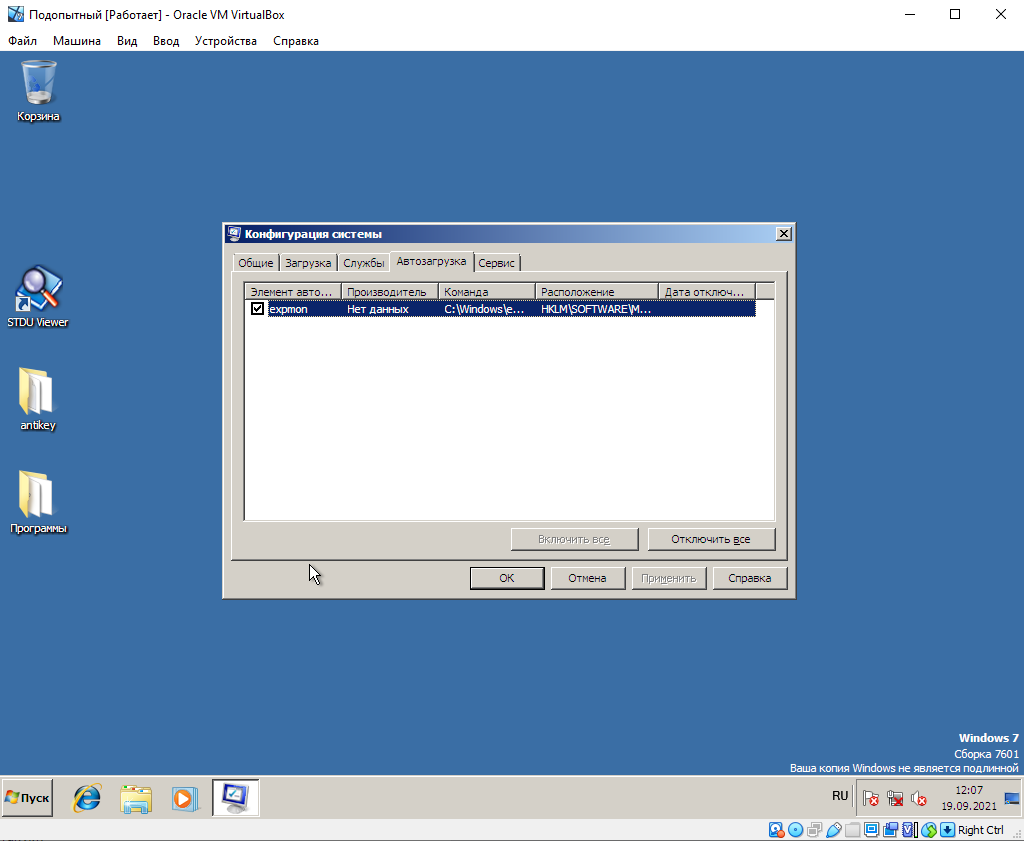


Рисунок 12 Окно программы msconfig

5 Сделать анализ всех запускаемых процессов и составить таблицу

|  |  |  |
| --- | --- | --- |
| **Имя** | **Местонахождение** | **Описание** |
| REGEDIT.exe | | |
| expmon | C:\Windows\expmon.exe | В соответствии с интернетом, либо это модуль защитника мейл ру, либо кейлоггер. Вобщем в обоих случая вирус XD |
| Файлы win.ini и system.ini | | |
| … |  | Только шрифты, драйверы и кодеки |
| MSCONFIG.exe | | |
| … |  | **То же самое, что и в реестре** |

## 1.3 Контроль подозрительных процессов в памяти

1 Вызвать диспетчер задач путем нажатия комбинации клавиш Ctrl + Shift + Esc или вызвать контекстное меню в системной панели (внизу экрана) и выбрать пункт Диспетчер задач->Процессы.

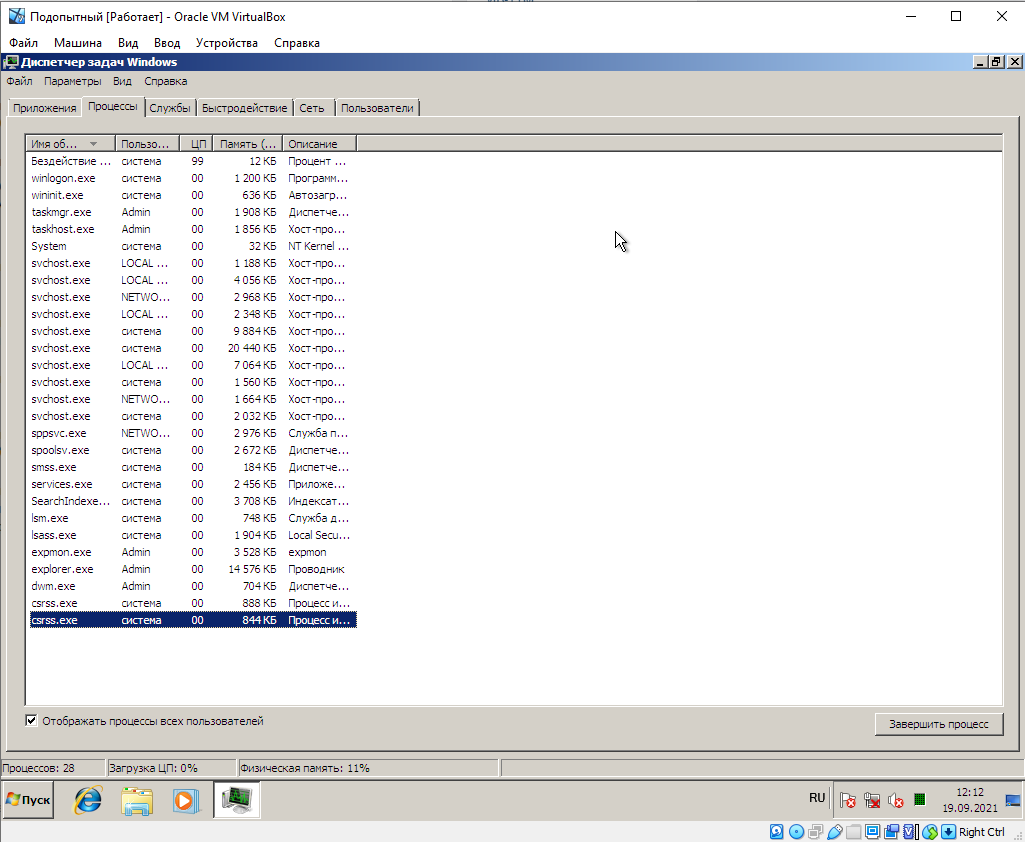


Рисунок 13 Диспетчер задач в Windows

2 Запустить программу Process Explorer с рабочего стола.

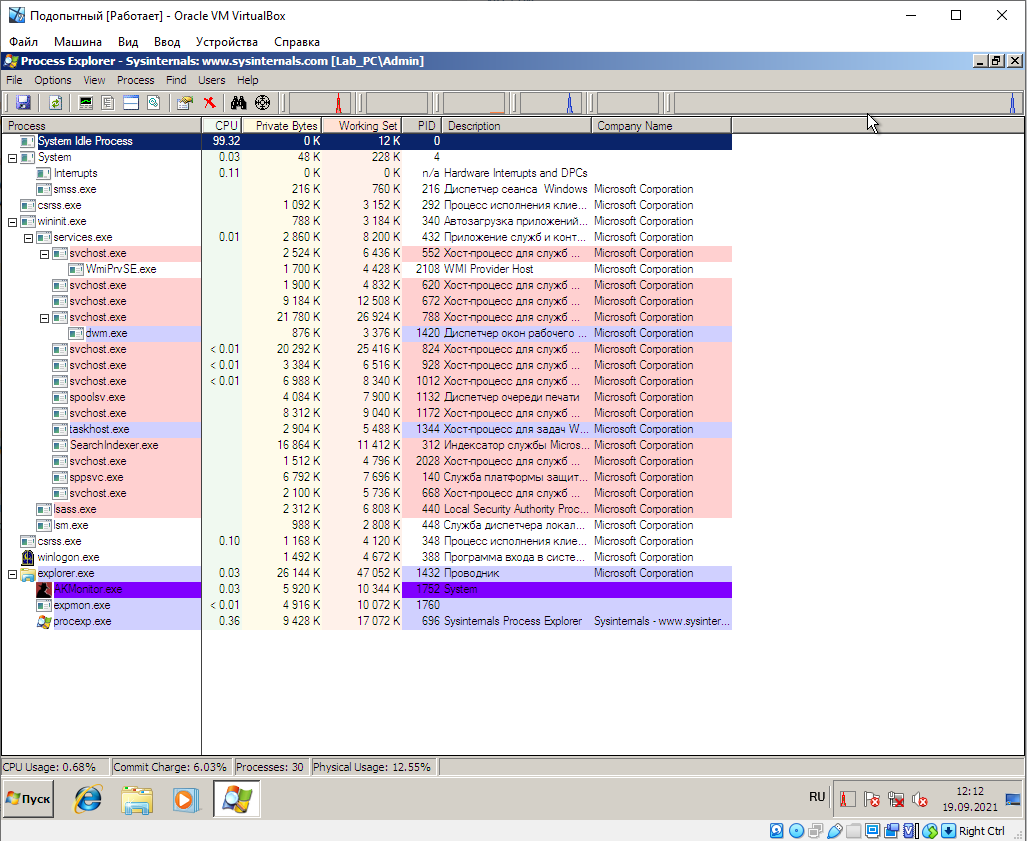


Рисунок 14 Программа Process Explorer

3 Запустить программу Autoruns с рабочего стола

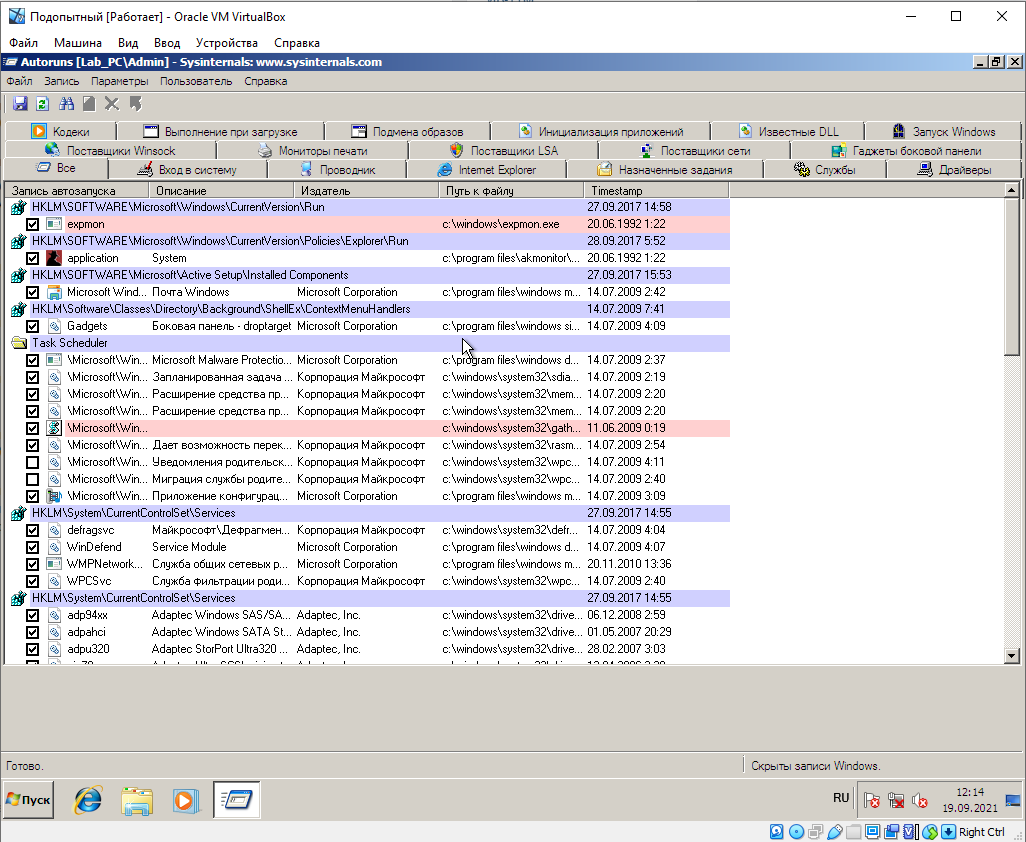


Рисунок 15 Программа Autoruns

4 Провести анализ подозрительных и выше не описанных процессов (2.2 Контроль запуска программ) в трех программах и найти расхождения

|  |  |  |  |
| --- | --- | --- | --- |
| Процесс/программа | Диспетчер задач | Process Explorer | Autoruns |
| AKmonitor | - | + | + |
| GatherNetworkInfo | - | - | + |

## 1.4 Контроль сетевой активности

1 Определить при помощи команды netstat –n какие порты открыты на компьютере.

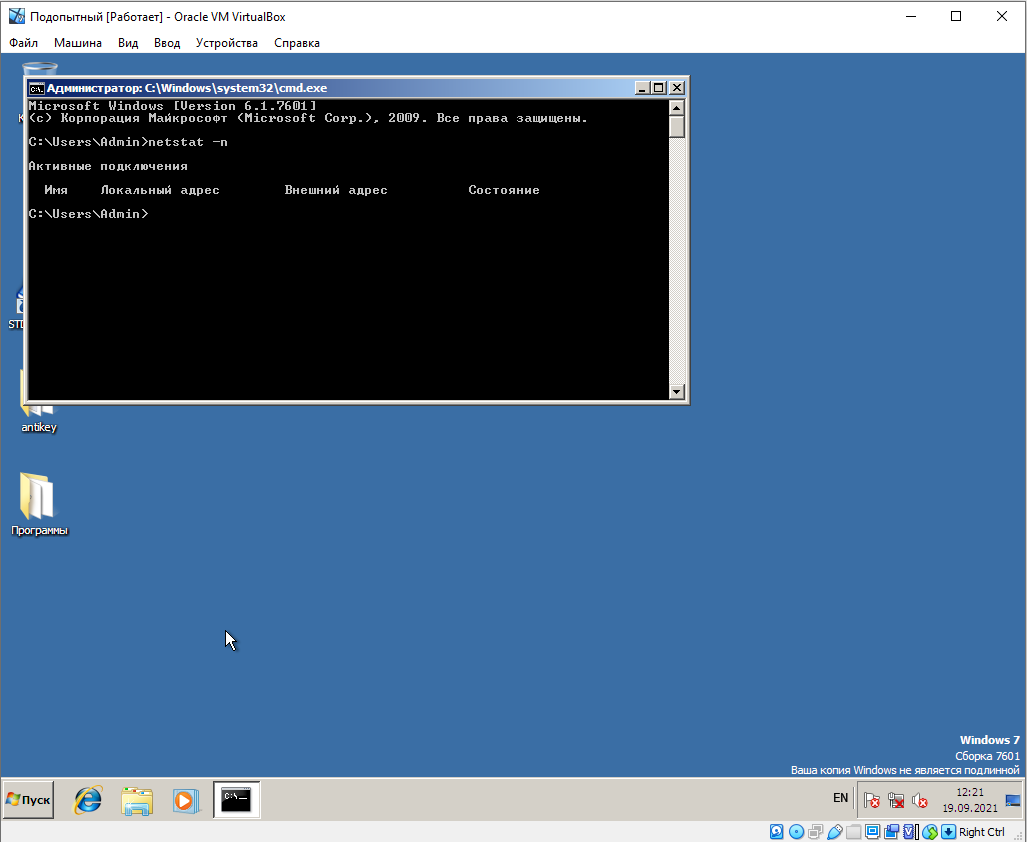


Рисунок 16 Команда netstat -n

2 Определить установленные соединения и открытые порты

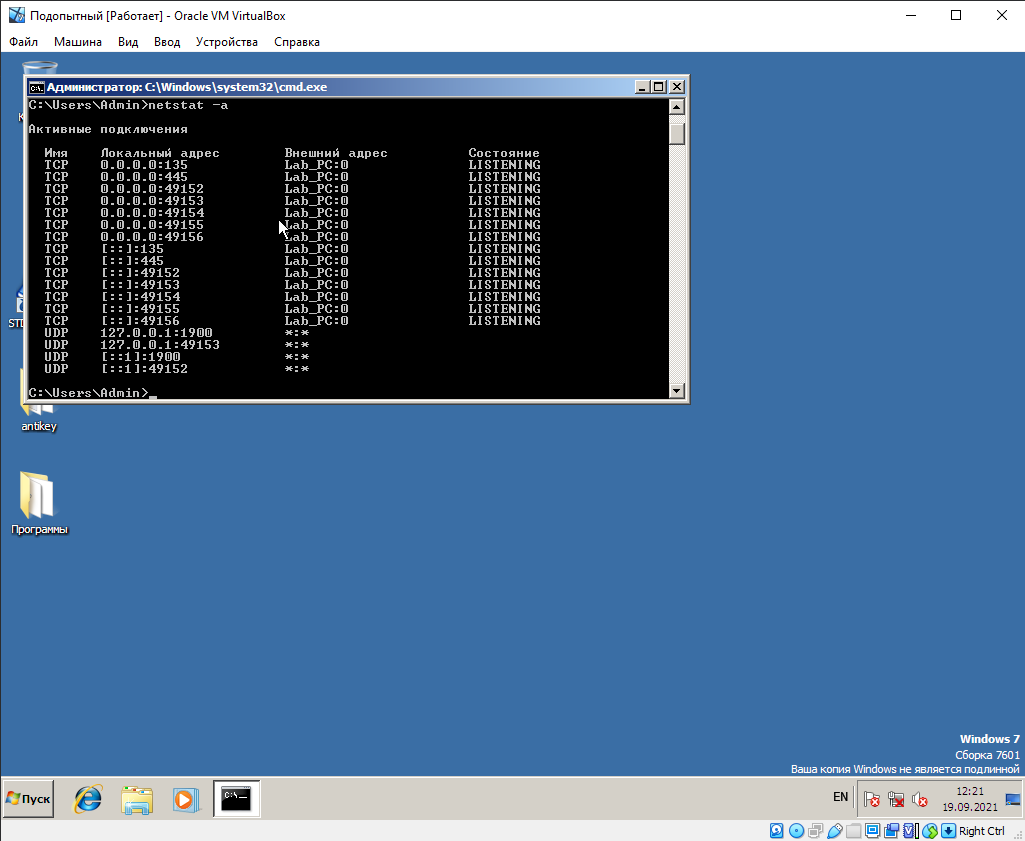


Рисунок 17 Команда netstat -a

3 Запустить стороннюю утилитами tcpview.exe.

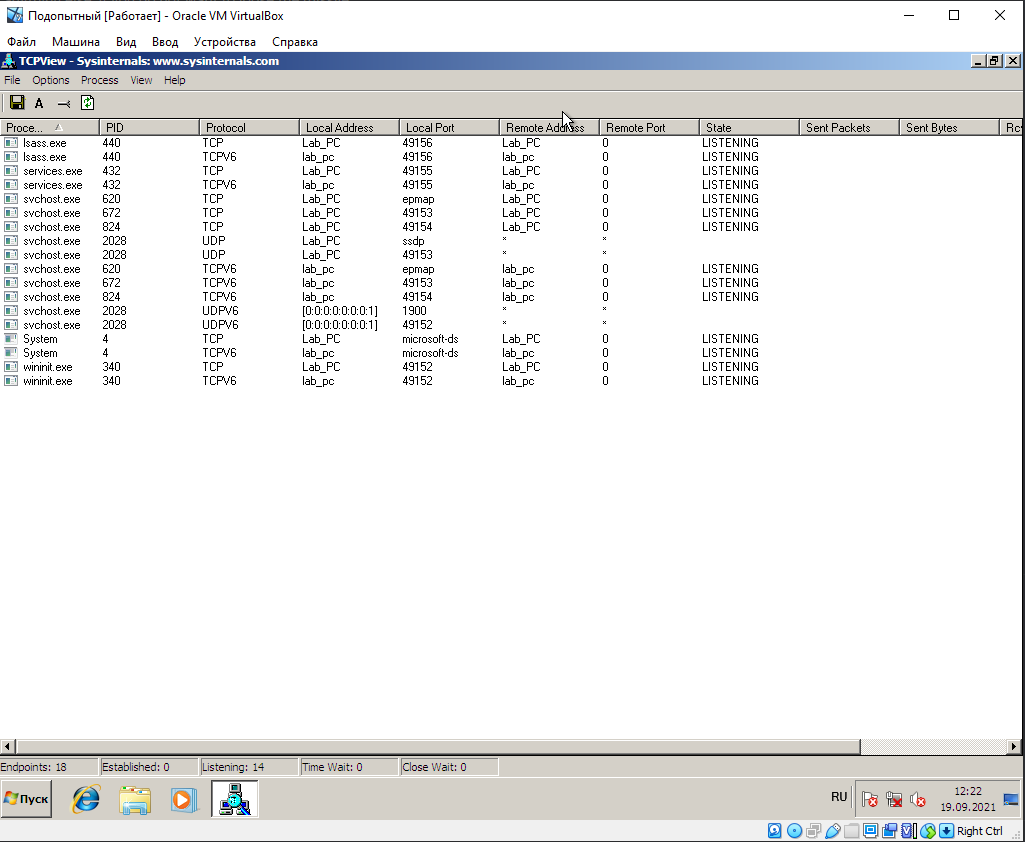


Рисунок 18 Утилита tcpview.exe

4 Подключить виртуальную машину к интернету и проверьте что изменилось.

5 Провести анализ открытых портов и процессов (до и после подключения к интернету). Сделать выводы  
**Вывод:** после включения интернета количество открытых портов удвоилось, появились новые процессы в TCPView. А вот процессы в остальных программах вроде бы не изменились.

## 1.5 Контроль использования программных закладок

1 Осуществить вход в программу кейлоггер \_\_\_\_\_\_\_\_\_\_ путем нажатия комбинации клавиш Ctrl+Alt+Shift+A и ввода пароля

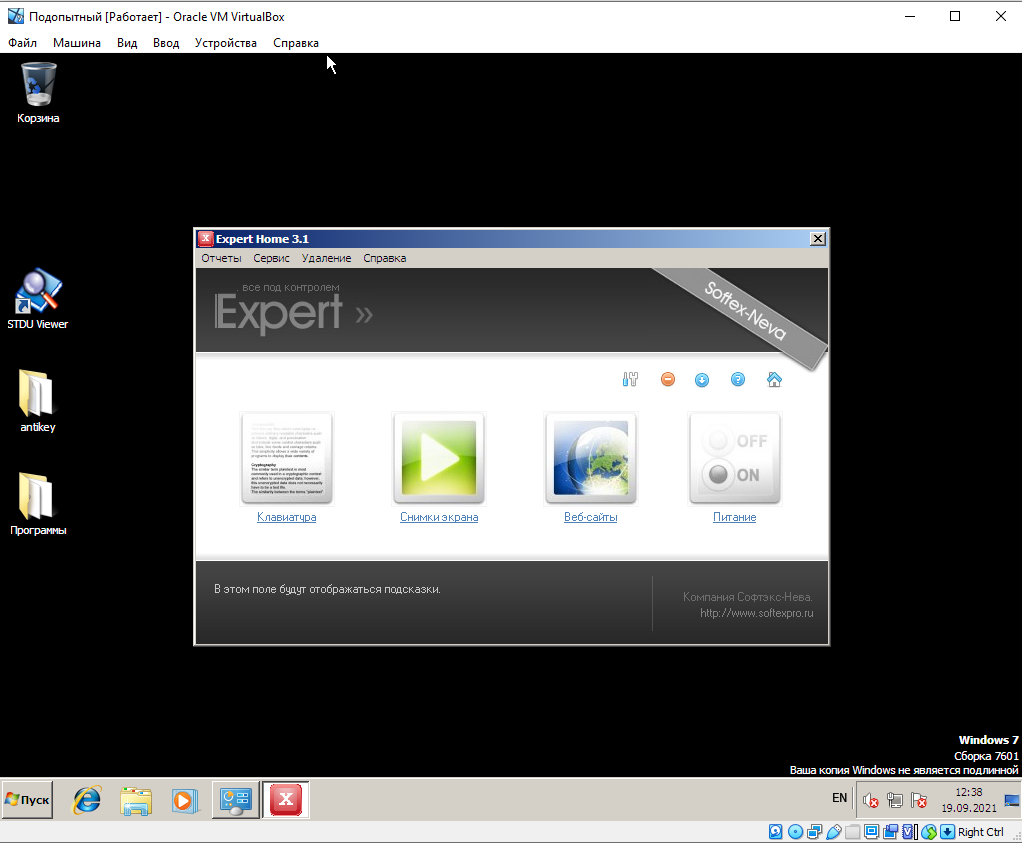


Рисунок 19 Кейлоггер Expmon

2 Действия, осуществляемые кейлоггером (перечислить):

- Регистрирование нажатий клавиш  
 - Создание снимков экрана

- Лог посещенных веб-сайтов  
 -Лог питания компьютера

3 Установить программу d:\Antikey\ak10.3.3.exe

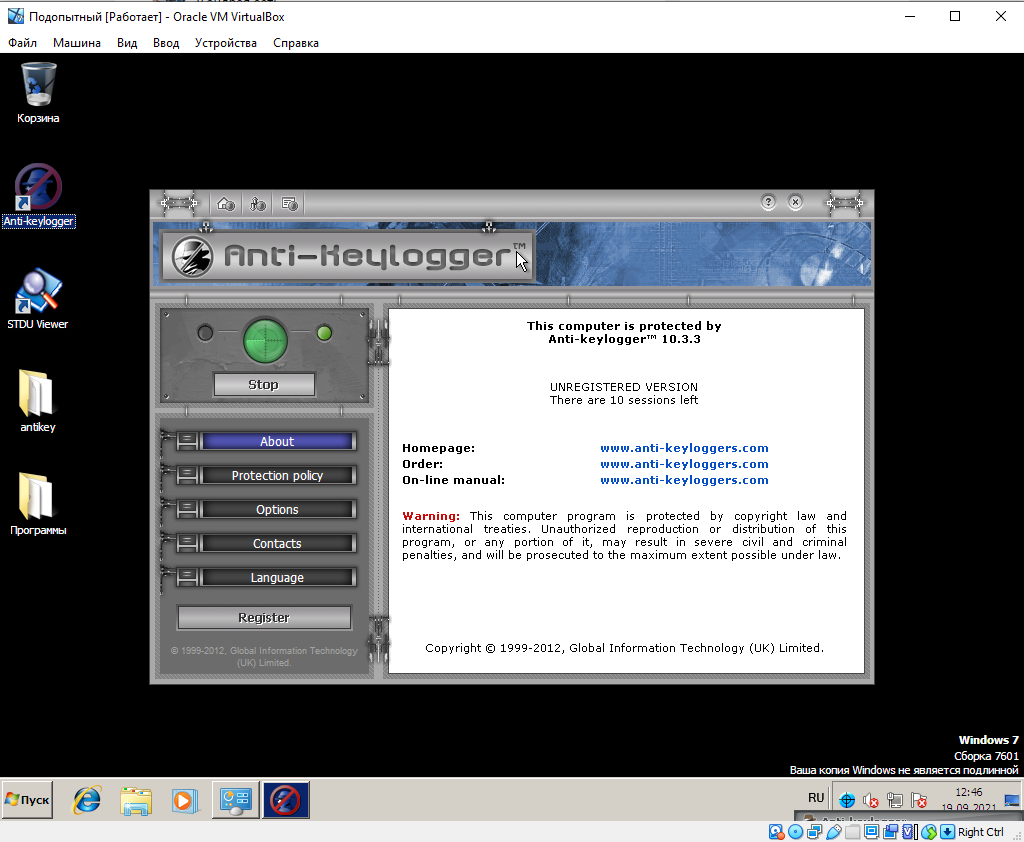


Рисунок 20 Программа Anti-keylogger

4 Запустить сканирование и просмотреть какие библиотеки обнаружены как потенциально опасные (Политика защиты)

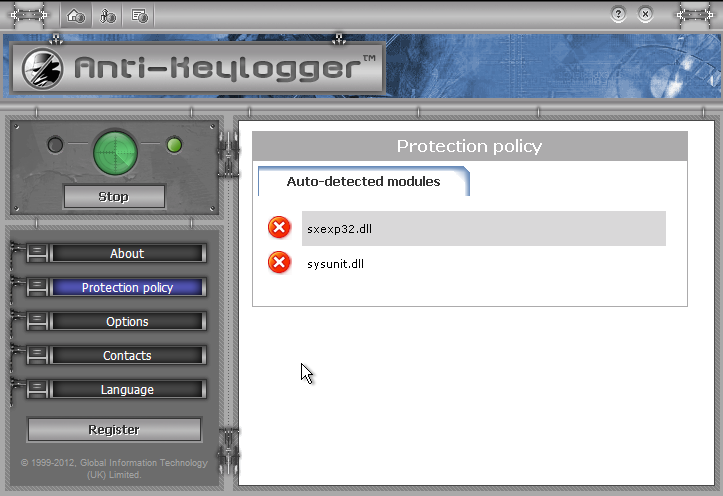


Рисунок 21 Потенциально опасные библиотеки,  
обнаруженные программой Anti-keylogger

5 Ввести произвольный текста с включенной программой Anti-keylogger и просмотреть последние записи, которые зафиксировались в кейлогере.

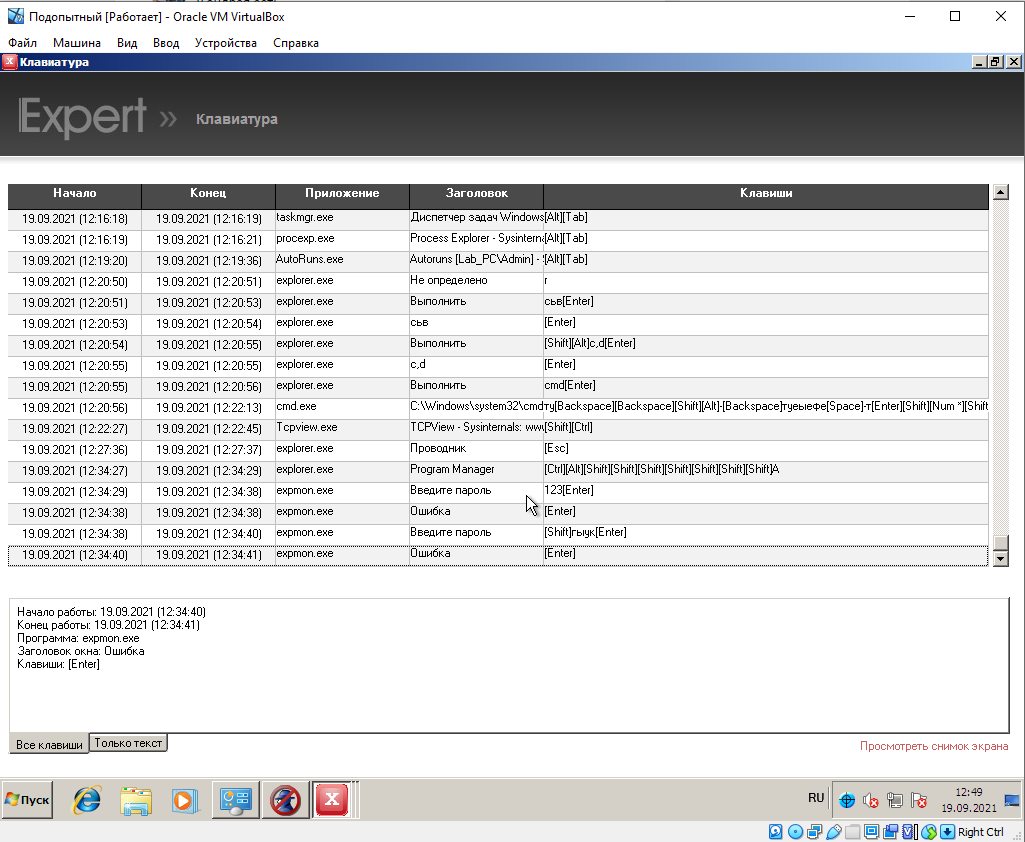


Рисунок 22 Последние записи, зафиксированные в кейлогере

6 Сделать выводы

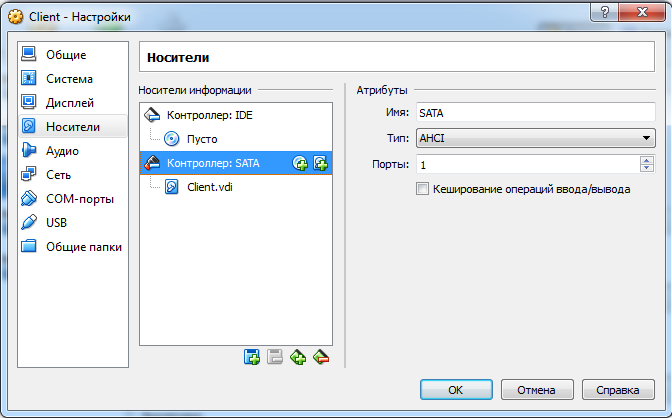
**Вывод:** после включения антикейлоггера кейлоггер не смог зарегистрировать нажатия клавиш (логично вообщем-то).

## 1.6 Контроль уязвимости ОС, позволяющая использовать удаленную информацию

1 Подключите к виртуальной машине образ жесткого диска с заданиями ЛР1.vdi (D:\Лаб.работы\ЛР1):

- выключить виртуальную машину;

- меню->настройка->носители->контроллер SATA->Добавить жесткий диск->Выбрать существующий диск



2 Запустить программу Back2Life с рабочего стола.

Рисунок 23 Программа восстановления данных Back2Life

3 Восстановить файл, находящийся на диске «E:\» в папке, соответствующей номеру студента.

Рисунок 24 Удаленный файл

4 Сделать выводы по структуре файла (восстановился/не восстановился, текстовый документ/неизвестный формат)

5 Скопировать скрипт Visual Basic Clear\_Free\_Space на «E:\» и запустить на выполнение

6 Выявить какой процесс занят выполнением данного скрипта (Диспетчером задач Windows или программами: Process Explorer, Autoruns)

Рисунок 25 Процесс скрипта Clear\_Free\_Space

7 После завершения процесса выполнить шаги 2-4.

Рисунок 26 Структура диска «E:\» в программе Back2Life

Рисунок 27 Восстановленный файл

8 Сделать выводы

**Вывод**: данный диск (ЛР1.vdi) отсутствует в папках на яндекс диске, выполнить задание невозможно.

## 1.7 Стеганографический метод скрытия информацию

1 Запустить программу OpenPuff с рабочего стола

2 Для скрытия файла нажмите кнопку «Hide»

3 Ввести пароль A (Cryptography), если необходимо – Enabled B, C

4 Добавить файл в который мы будем «скрывать» (3)

5 Выбрать сам файл, который необходимо скрыть (2)

6 Нажать кнопку «Hide» для выполнения действий по вскрытию

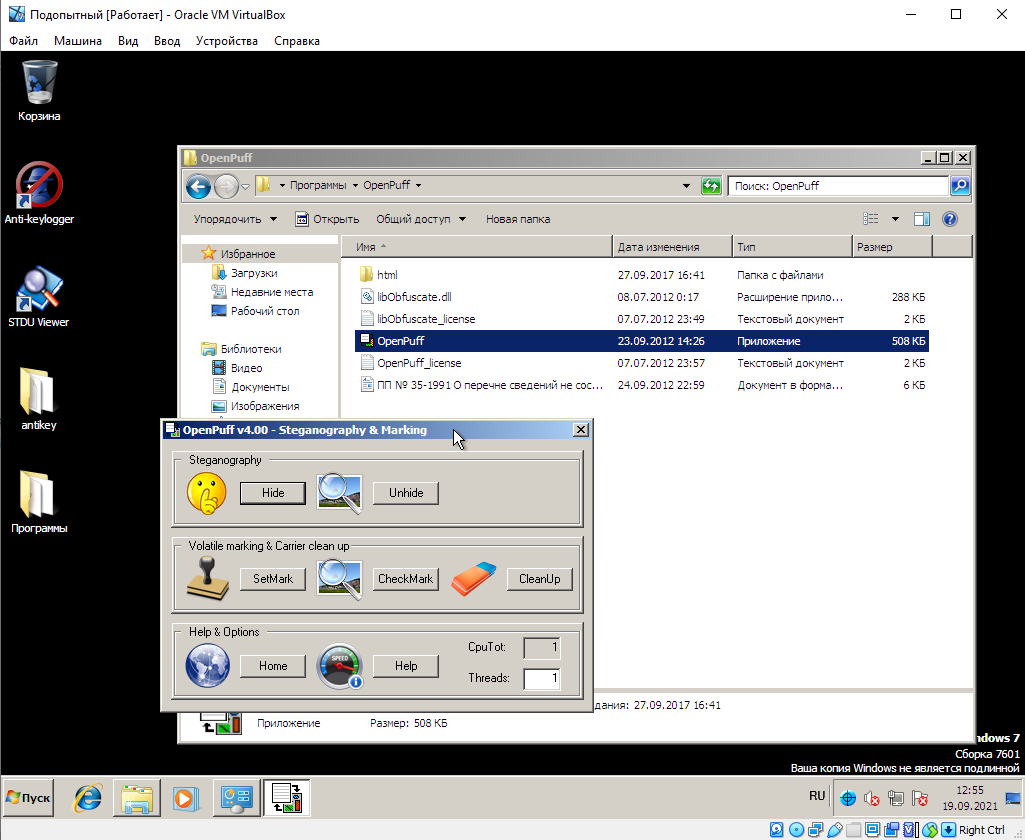


Рисунок 24 Главное окно программы OpenPuff

7 Сделать выводы о стеганографическом методе скрытия информации.

**Вывод:** стеганография – очень мощный инструмент, так как скрывается сам факт наличия посторонней информации. По-сути единственным способом выявления стеганографии является сканирование всех файлов на предмет посторонней информации, для чего требуется знать как минимум структуру, а желательно и содержимое оригинальных файлов, что может быть невыполнимо, например, на проприетарных файлах баз данных различных приложений.

**2 Контрольные вопросы**

3.1 Перечислите источники угроз.

* Нарушитель
* Носитель вредоносной программы
* Аппаратная закладка

3.2 Перечислите персонал, который можно отнести к внутренним нарушителям.

* Обслуживающий персонал (например, уборщик)
* Сотрудники, имеющие доступ в помещение, но не к информации и т.д.

3.3 Перечислите угрозы несанкционированного доступа.

* Угрозы доступа (проникновения) в операционную среду с использованием штатного программного обеспечения (средств операционной системы или прикладных программ общего применения)
* Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств за счет преднамеренных изменений служебных данных, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.
* Угрозы внедрения вредоносных программ (программно-математического воздействия)
* Угрозы использования нетрадиционных информационных каналов

3.4 Какие деструктивные действия применимы к информации?

* уничтожение информации в секторах дискет и винчестера;
* исключение возможности загрузки операционной системы (компьютер «зависает»);
* искажение кода загрузчика;
* форматирование дискет или логических дисков винчестера;
* закрытие доступа к COM- и LPT-портам;
* замена символов при печати текстов;
* подергивания экрана;
* изменение метки диска или дискеты;
* создание псевдосбойных кластеров;
* создание звуковых и(или) визуальных эффектов (например, падение букв на экране);
* порча файлов данных;
* перезагрузка компьютера;
* вывод на экран разнообразных сообщений;
* отключение периферийных устройств (например, клавиатуры);
* изменение палитры экрана;
* заполнение экрана посторонними символами или изображениями;
* погашение экрана и перевод в режим ожидания ввода с клавиатуры; шифрование секторов винчестера;
* выборочное уничтожение символов, выводимых на экран при наборе с клавиатуры;
* уменьшение объема оперативной памяти;
* вызов печати содержимого экрана;
* блокирование записи на диск;
* уничтожение таблицы разбиения (Disk Partition Table), после этого компьютер можно загрузить только с флоппи-диска;
* блокирование запуска исполняемых файлов;
* блокирование доступа к винчестеру.

3.5 Классифицируйте угрозы безопасности по уровню эталонной модели взаимодействия открытых систем.

* На физическом уровне
* На канальном уровне
* На сетевом уровне
* На транспортном уровне
* На сеансовом уровне
* На представительном уровне
* На прикладном уровне

3.6 Перечислите основные виды вредоносных программ.

* программные закладки;
* классические программные (компьютерные) вирусы;
* вредоносные программы, распространяющиеся по сети (сетевые черви);
* другие вредоносные программы, предназначенные для осуществления НСД.

3.7 Какие уязвимости отдельных протоколов стека протоколов TCP/IP существуют?

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование протокола** | **Уровень стека протоколов** | **Наименование (характеристика) уязвимости** | **Содержание нарушения безопасности информации** |
| FTP (File Transfer Protocol) – протокол передачи файлов по сети | Прикладной, представи-тельный, сеансовый | 1. Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде)  2. Доступ по умолчанию  3. Наличие двух открытых портов | Возможность перехвата данных учетной  записи (имен зарегистрированных пользователей, паролей).  Получение удаленного доступа к хостам |
| telnet – протокол управления удаленным терминалом | Прикладной, представи-тельный, сеансовый | Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде) | Возможность перехвата данных учетной  записи пользователя.  Получение удаленного доступа к хостам |
| UDP – протокол передачи данных без установления соединения | Транспорт-ный | Отсутствие механизма предотвращения перегрузок буфера | Возможность реализации  UDР-шторма.  В результате обмена пакетами происходит существенное снижение производительности сервера |
| ARP – протокол преобразования IP-адреса в физический адрес | Сетевой | Аутентификация на базе открытого текста (информация пересылается в незашифрованном виде) | Возможность перехвата трафика пользователя злоумышленником |
| RIP – протокол маршрутной информации | Транспорт-ный | Отсутствие аутентификации управляющих сообщений об изменении маршрута | Возможность перенаправления трафика через хост злоумышленника |
| TCP – протокол управления передачей | Транспорт-ный | Отсутствие механизма проверки корректности заполнения служебных заголовков пакета | Существенное снижение скорости обмена и даже полный разрыв произвольных соединений по протоколу TCP |
| DNS – протокол установления соответствия мнемонических имен и сетевых адресов | Прикладной, представи-тельный, сеансовый | Отсутствие средств проверки аутентификации полученных данных от источника | Фальсификация ответа  DNS-сервера |
| IGMP – протокол передачи сообщений о маршрутизации | Сетевой | Отсутствие аутентификации сообщений об изменении параметров маршрута | Зависание систем  Win 9x/NT/2000 |
| SMTP – протокол обеспечения сервиса доставки сообщений по электронной почте | Прикладной, представи-тельный, сеансовый | Отсутствие поддержки аутентификации заголовков сообщений | Возможность подделывания сообщений электронной почты, а также адреса отправителя сообщения |
| SNMP – протокол управления маршрутизаторами в сетях | Прикладной, представи-тельный, сеансовый | Отсутствие поддержки аутентификации заголовков сообщений | Возможность переполнения пропускной способности сети |

3.8 Какие методы используются при формирования нетрадиционных каналов?

* компьютерной стеганографии;
* основанные на манипуляции различных характеристик ИС, которые можно получать санкционировано

3.9 Какие методы стеганографического преобразования по типу контейнера существуют?

Методы, использующие:

* аудиоконтейнеры
* текстовые контейнеры
* графические контейнеры

3.10 В каких случаях возможно восстановление файлов?

Если в сектора, в которых находились удаленные файлы, не было записано новой информации.

3.11 Перечислите основные виды программно-аппаратных закладок.

* Автономные
* Конструктивно-встроенные

3.12 Каким средством возможно обнаружить аппаратную закладку?

Аппаратную закладку можно выявить проверкой на рентгене и последующем изучении снимка. Так же возможно обнаружить ее по побочных признакам работы, таким как радиоизлучение.