Иван Андреевич Трещев

Анализ защищенности распределенных информационных систем

Для студентов технических специальностей

Иван Трещев

Анализ защищенности распределенных информационных систем. Для студентов технических специальностей

«Издательские решения»

Трещев И. А.

Анализ защищенности распределенных информационных систем. Для студентов технических специальностей / И. А. Трещев — «Издательские решения»,

ISBN 978-5-44-939419-4

В книге описаны основные подходы к анализу защищенности распределенных информационных систем. В качестве средств для автоматизированного анализа защищенности использованы сертифицированные по требованиям Федеральной службы по техническому и экспортному контролю Сканер ВС и XSpider.

ISBN 978-5-44-939419-4

Содержание

Анализ защищенности распределенных информационных систем Для студентов технических специальностей

Иван Андреевич Трещев

Обнаружить все «дыры» невозможно. Один из законов Мерфи.

Ряд идей изложенных в пособии Антон Александрович Воробьев
Тестирование и анализ Алексей Владимирович Проваторов

ISBN 978-5-4493-9419-4
Создано в интеллектуальной издательской системе Ridero

Введение

Требования законодательства Российской Федерации, Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности, Министерства обороны Российской Федерации и других ведомств однозначно определяют необходимость проведения мероприятий по анализу защищенности и наличия уязвимостей в информационных системах. Любая современная ИТ система обязательно включает некоторую базу данных и почти всегда является территориально распределенной, что влекёт необходимость анализа не только на наличие несанкционированного доступа к информации на локальных автоматизированных местах, но и проведение мероприятий по антивирусному контролю, межсетевому экранированию, обнаружению и предотвращению вторжений. Отдельно оговоримся, что при передаче любой информации подлежащей защите за пределы локальной вычислительной сети предприятия единственным способом обеспечения защищенности информации – конфиденциальности, целостности, доступности является криптографическая защита.

В данной книге не рассмотрены вопросы криптографической защиты информации, поскольку любые практически-ориентированные методики являются информацией ограниченного распространения и в соответствии с административным регламентом и находятся в ведении ФСБ России.

Анализ защищенности и выявление уязвимостей в информационных системах является действием постоянным, т.е. любой специалист по защите информации на объекте информатизации должен систематически проводить необходимые мероприятия. Защищенность информационной системы будет тем выше, чем более строго соблюдаются инструкции, регламенты, соглашения, политики и другие нормативные документы разработанные в организации по защите информации. Соблюдение требований законодательства по защите информации в данном случае является необходимым, достаточным и обязательным требованием по обеспечению информационной безопасности.

Корпорации Microsoft, Apple и другие систематически выпускают обновления системы безопасности для своих операционных систем и тем самым демонстрируют, что любая операционная система, как продукт информационных технологий, подвержена атакам злоумышленников и требует постоянной доработки и сопровождения со стороны создателей.

Уязвимости zero-day появляются систематически и обеспечить состояние защищенности на объекте представляется возможным только если своевременно и в полном объеме устанавливать соответствующие обновления. Хотя автор хотел бы отметить, в случае установки обновлений нет никаких гарантий, что некоторые программные закладки или же недекларированные возможности не внедряются производителем.

Далее в работе под потенциальным злоумышленником понимается не только аутсайдер для предприятия (некая личность не имеющая к нему отношения), но и инсайдер (другими словами сотрудник предприятия). Книга не является сборником практических рецептов по «взлому» информационных систем, а носит лишь информационный характер.

Проводить мониторинг уязвимостей в каждой информационной системе необходимо с точки зрения обеспечения своевременной реакции на инциденты информационной безопасности.

получение административных привелегий в Windows 7

Часто при анализе защищенности информационных систем мы сталкиваемся с проблемой, точнее непониманием со стороны руководства предприятия информационную систему которого необходимо проанализировать. Всегда возникает вопрос – зачем нам это? В качестве ответа на данный вопрос можно предложить продемонстрировать на что способен потенциальный злоумышленник. Цель данной главы привести один из возможных вариантов демонстрации. Конечно предложенная здесь методика вполне вероятно может и не сработать (настроена система обновлений операционной системы, отключена система восстановления при загрузке операционной системы, отключен механизм залипания клавиш), но в 90% случаев она работает. Она не требует никаких дополнительных механизмов, навыков, средств.

Для начала нужно выполнить перезагрузку компьютера используя кнопку reset или же отключив и включив питание то есть выполнить hard reset при работающей операционной системе, чтобы появился экран с выбором вариантами загрузки ОС Windows как на Рис. 1.

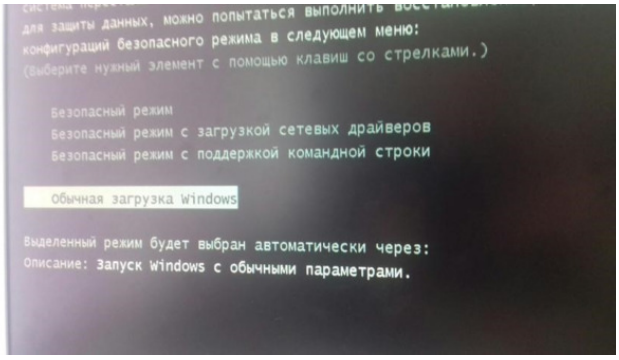

Рис. 1. – Варианты загрузки ОС, означающие, что компьютер был некорректно перезагружен.

После чего запускаем средство восстановления при запуске, как показано на Рис. 2.

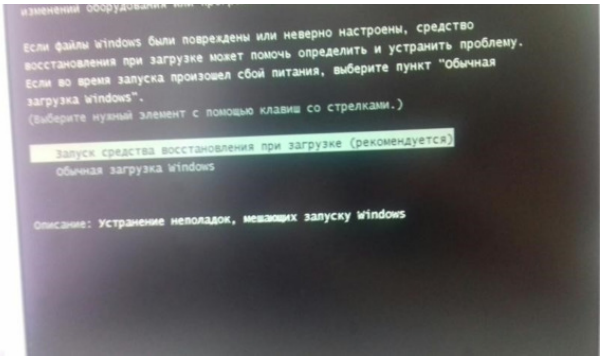

Рис. 2. – Выбор запуска средства восстановления.

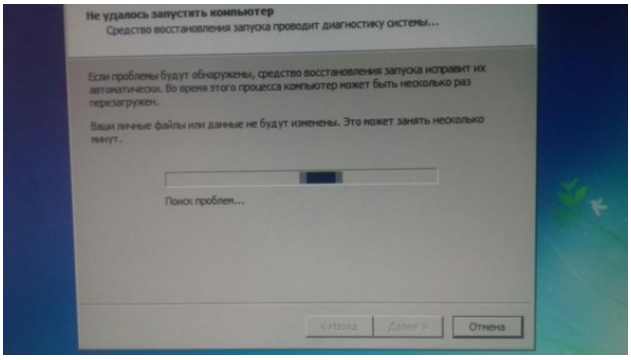

Рис. 3. – Окно средства восстановления.

После этого на окне восстановления системы жмём отмену, как показано на Рис. 4.

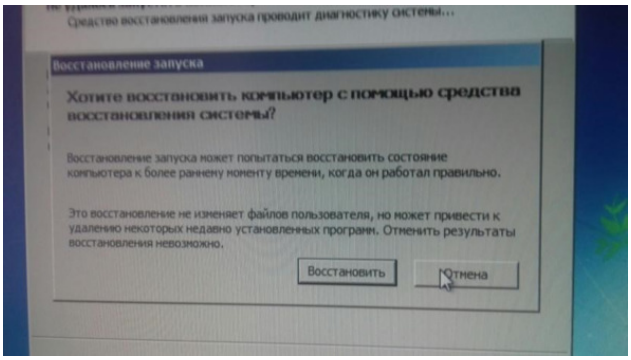

Рис. 4. – Дополнительное окно, на котором нужно нажать отмена.

На новом окне «Показать подробности проблемы», см. Рис. 5.

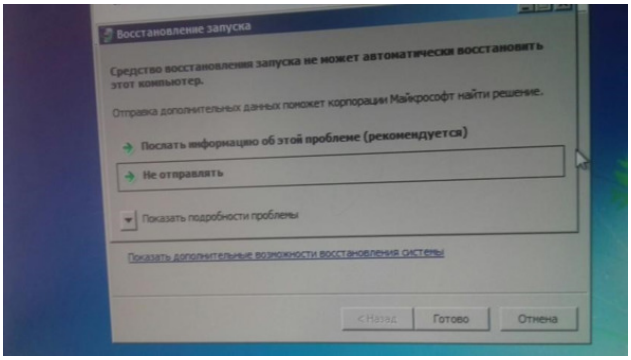

Рис. 5. – Окно выбора отправки дополнительных данных

Таким образом мы планируем использовать недокументированную возможность (недекларированную) запуска блокнота и обозревателя файлов. Запустив приложение без запуска операционной системы мы получим возможность манипулировать файловой системой без надзора со стороны операционной системы.

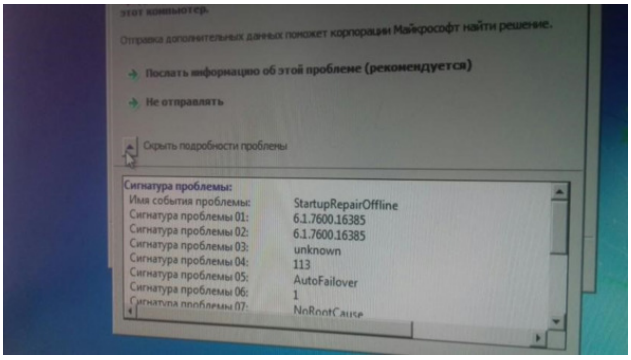

Рис. 6. – Развёрнутое окно выбора отправки дополнительных данных

Затем находим «X:\windows\system32\ru-RU\erofflps. txt». И жмём на него, как показано на Рис. 7.

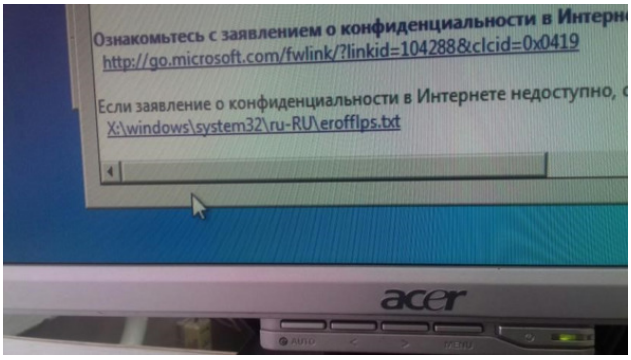

Рис. 7. – X:\windows\system32\ru-RU \erofflps. txt.

Появился блокнот, который представлен на Рис. 8.

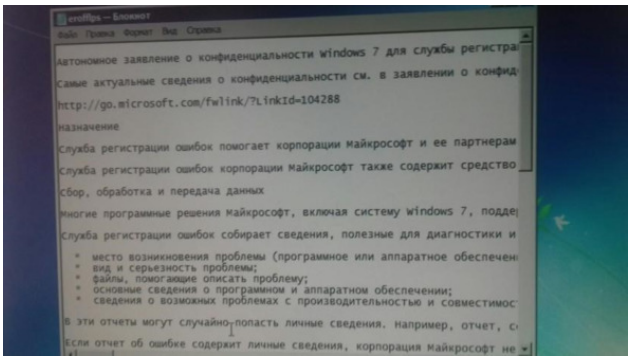

Рис. 8 Появившийся блокнот

Жмём «Файл» – «Открыть…», как показано на Рис. 9.

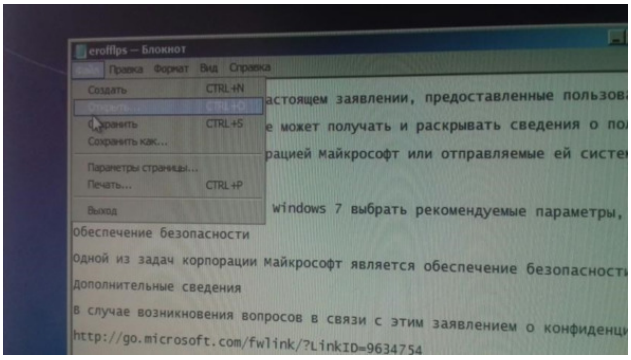

Рис. 9. – «Файл» – «Открыть…».

Появился проводник, который можно увидеть на Рис. 10

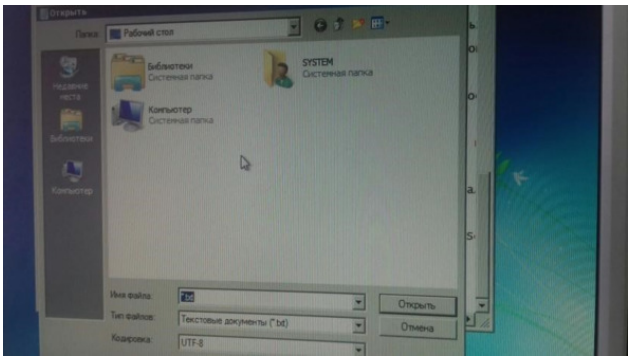

Рис. 10. – Открывшийся проводник.

Открываем «Мой компьютер», как показано на Рис. 11.

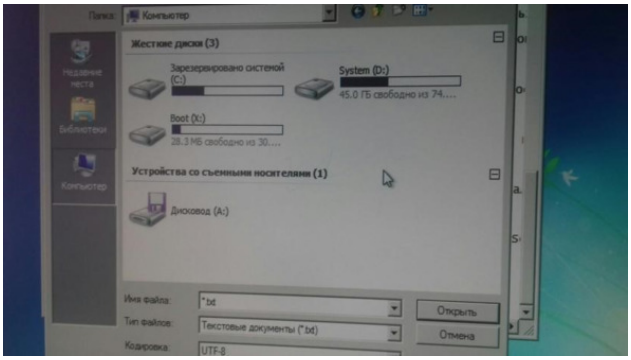

Рис. 11. – Проводник «Моего компьютера».

Открываем диск С, как показано на Рис 12.

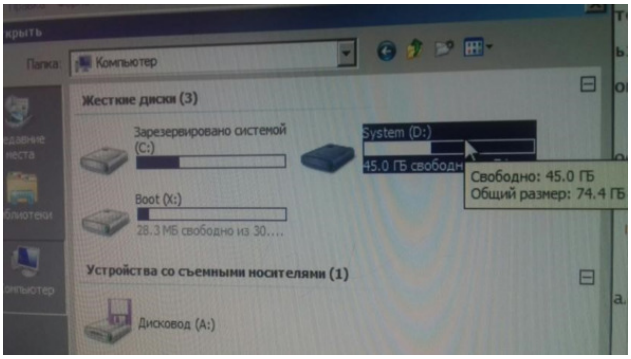

Рис. 12. – Выбор диска C в проводнике «Моего компьютера».

Находим папку Windows, которую можно увидеть на Рис. 13.

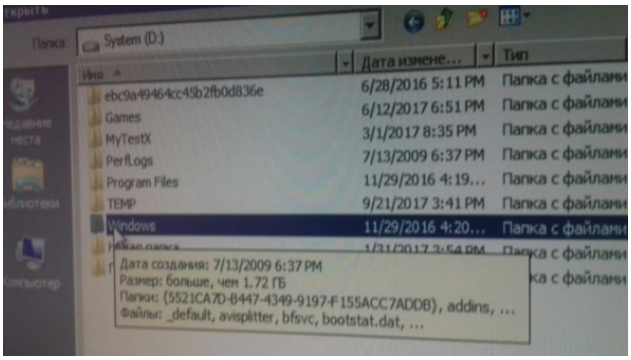

Рис. 13. – Выбор папки Windows.

Открываем её. В ней находим папку System32, которую можно увидеть на Рис. 14.

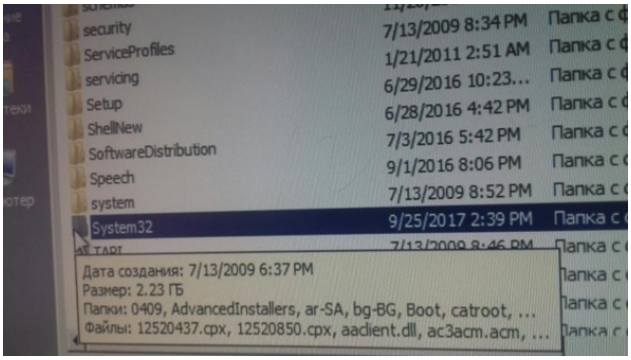

Рис. 14. – Выбор папки System32.

Выбираем тип файлов «Все файлы», как показано на Рис. 15.

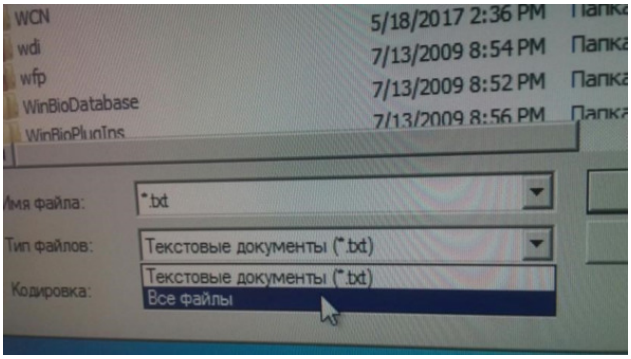

Рис. 15. – Выбор типа файлов «Все файлы».

Находим файл sethc, который представлен на Рис. 16.

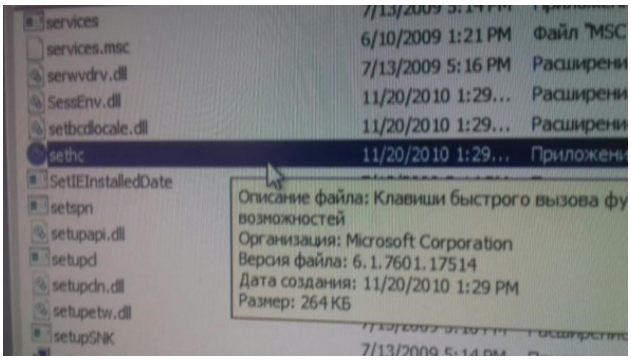

Рис. 16. – Выбор файла sethc.

Переименовываем его в sethc1, как показано на Рис. 17.

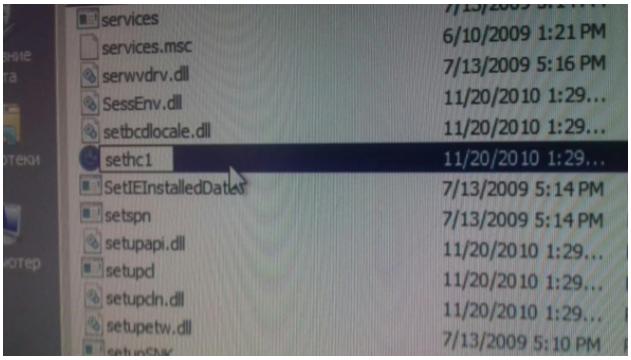

Рис. 17. – Переименованный файл sethc в sethc1.

Находим файл cmd, который представлен на Рис. 18.

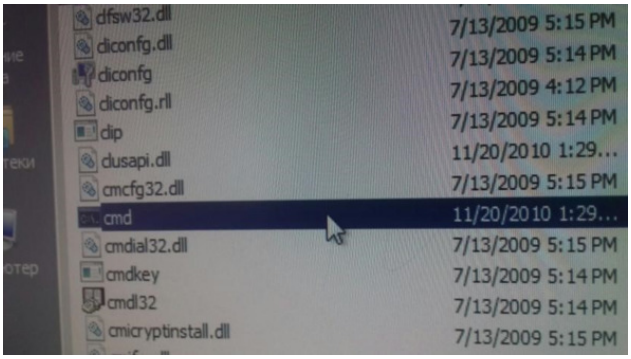

Рис. 18. – Выбор файла cmd.

Копируем его, как показано на Рис. 19.

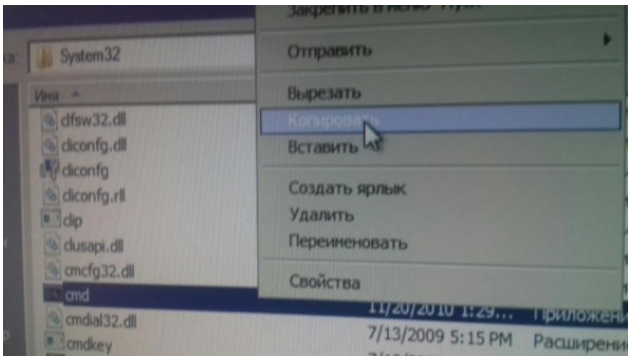

Рис. 19. – Выбор копирования файла cmd.

Вставляем, как показано на Рис. 20.

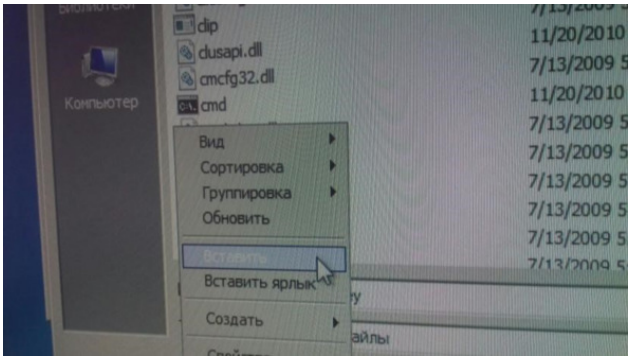

Рис. 20. – Вставка файла cmd.

Переименовываем его в sthc, как показано на Рис 21 и Рис. 22.

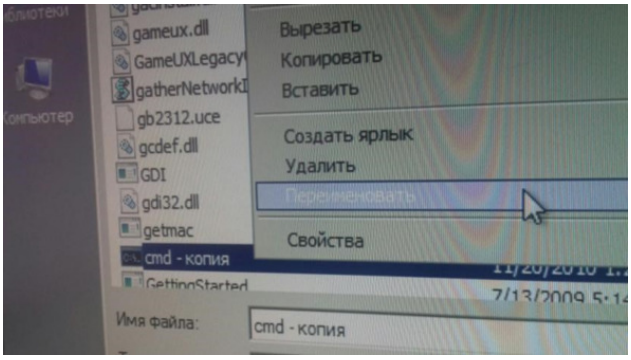

Рис. 21. – Выбор переименования файла cmd в sethc.

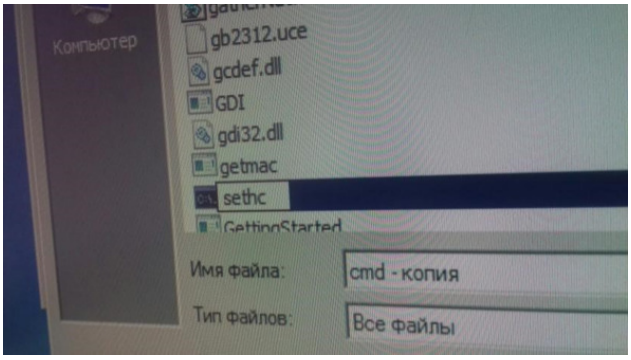

Рис. 22. – Файл cmd, переименованный в sethc.

Запускаем компьютер, экран загрузки ОС Windows представлен на Рис. 23.

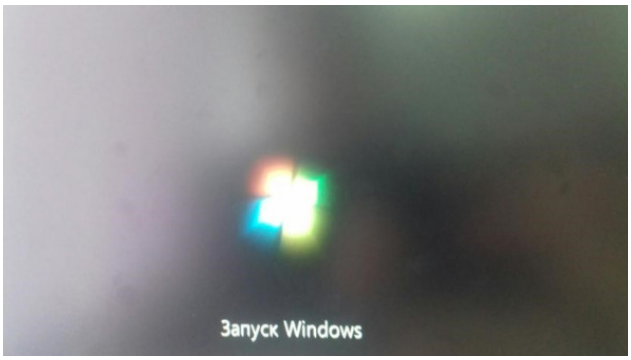

Рис. 23. – Запуск Windows.

Нажимаем много раз Shift что бы вызвать залипание клавиш, отметим что в данном случае программа залипания клавиш запускается с самыми высокими локальными привелегиями, но появится Командная строка, которая представлена на Рис. 24.

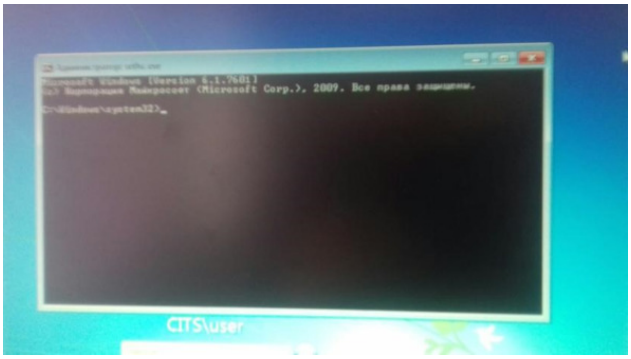

Рис. 24. – командная строка, выпавшая в результате вызывания залипания клавиш.

Пишем команду net user admin 123456Qq /add, как показано на Рис. 25.

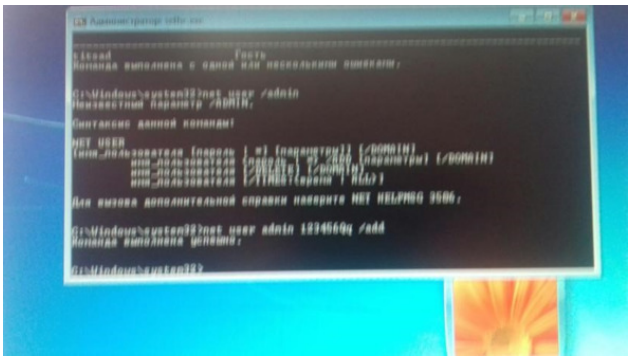

Рис. 25. – команда net user admin 123456Qq /add, написанная в командной строке.

Проверяем правильно ли всё сделано было, как показано на Рис. 26.

Конец ознакомительного фрагмента.