Министерство науки и высшего образования РФ

ФГБОУ ВО «Томский государственный университет
систем управления и радиоэлектроники»
Кафедра комплексной информационной безопасности
электронно-вычислительных систем (КИБЭВС)

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебно-методическое пособие
для студентов направлений подготовки
10.00.00 Информационная безопасность

Томск, 2022

УДК 004.056
ББК 32.973.26-018.2
К 64

Авторы:
А.А. Конев, А.Ю. Якимук, А.К. Новохрестов, И.А. Рахманенко

Конев Антон Александрович
К 64 Технологии обеспечения информационной безопасности: учебно-методическое пособие. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2022. – 351 с.

Настоящее учебно-методическое пособие содержит описания лабораторных и самостоятельных работ по дисциплине «Технологии обеспечения информационной безопасности» для направлений подготовки, входящих в укрупненную группу специальностей и направлений 10.00.00 Информационная безопасность.

УДК 004.056
ББК 32.973.26-018.2

СОДЕРЖАНИЕ

Лабораторная работа № 1
Администрирование учетных записей пользователей в операционной системе Windows

1. Цель работы

Целью работы является освоение средств администрирования учётных записей пользователей и групп пользователей в ОС Windows 8, изучение основных параметров, определяющих взаимодействие пользователей с операционной системой, консолью управления и групповой политикой.

2. Краткие теоретические сведения

В операционной системе Windows 10 существует 2 группы пользователей:

– локальные учетные записи;

– учетные записи Microsoft.

Первая группа называется локальной, по причине того, что аутентификация происходит на локальном компьютере. Все учетные данные необходимые для этого (имя пользователя, пароль и параметры учетной записи) хранятся в нем.

В случае работы с учетной записью Microsoft — аутентификация пользователей происходит на сервере сети, то есть удаленно. Преимущество данного способа в том, что любой сотрудник предприятия может зайти в сеть с любого компьютера, а не только с закрепленного за ним. Сервер хранит все параметры пользователя, а также при необходимости и документы, с которыми он работает. Однако второй тип пользователей имеет свой недостаток – при отсутствии интернет-соединения или коммутируемом (не устанавливаемом автоматически) соединении аутентификация будет невозможна.

Локальные учетные записи бывают трех видов:

– учетная запись администратора, создаваемая при установке системы и используемая при изменении параметров системы;

– учетная запись пользователя, позволяющая использовать установленные администратором из внешних источников программы и изменять параметры персонализации;

– гостевая учетная запись.

Консоль управления Microsoft Management Console (MMC) – это компонент операционных систем семейства Windows NT, предоставляющий администраторам графический интерфейс для настройки системных приложений и прикладных программ.

Оснастка – компонент для MMC, включающий набор параметров какого-либо модуля операционной системы (файловой системы, управления пользователями и т.д.) или прикладного приложения.

Набор параметров для прикладных программ может быть добавлен в оснастку при помощи административных шаблонов – особым образом структурированных файлов с расширением *.adm.

Групповая политика – это набор правил или настроек, в соответствии с которыми производится настройка рабочей среды Windows.

3. Ход работы

3.1. Управление учётными записями локальных пользователей

Рассмотрите механизм работы с учетными записями пользователей, предлагаемых Windows 10. Для этого через меню «Пуск» перейдите к параметрам системы (рис. 1).

Рис. 1. Параметры Windows

Перейдите в раздел «Учётные записи». В данном разделе будет представлена информация о том, под какой учетной записью был осуществлен вход, представлены функции по изменению параметров входа, представлены учетные записи на данном компьютере (если таковые имеются) и предложено создать новых пользователей (рис. 2).

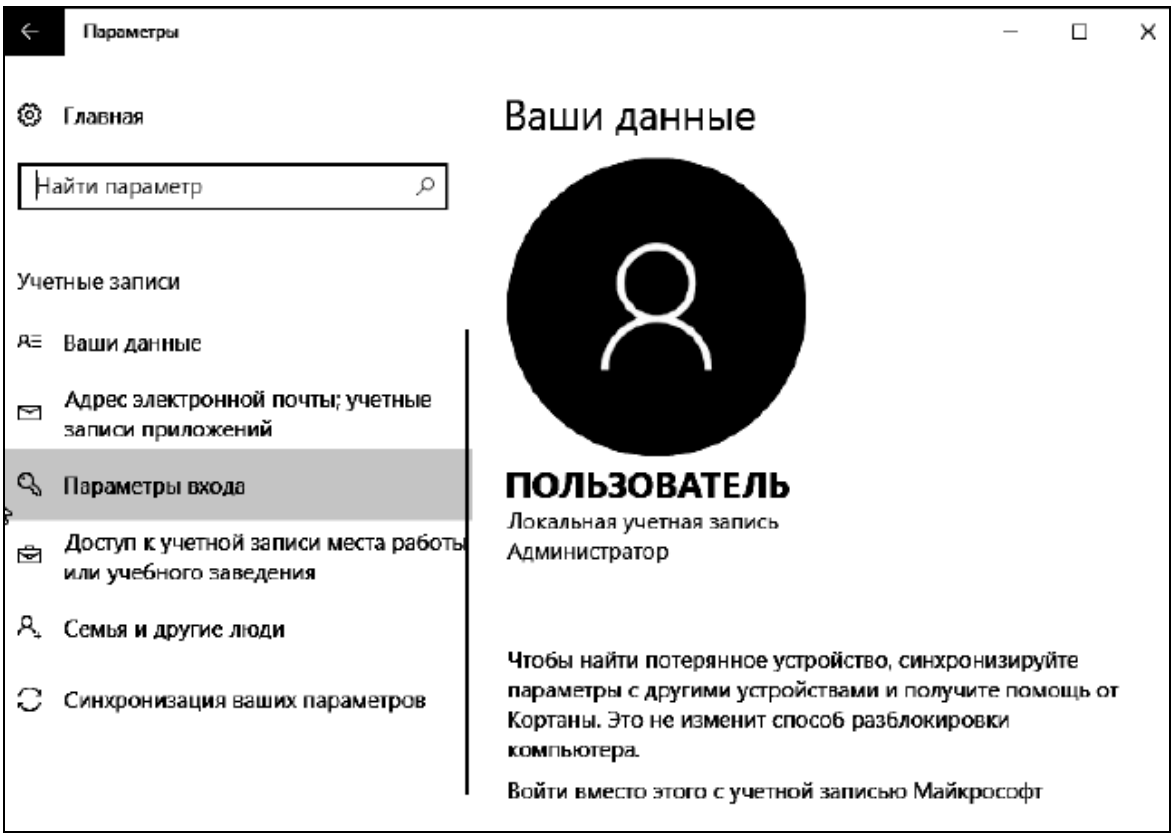


Рис. 2. Вкладка управления пользователями

Перейдите во вкладку «Семья и другие люди», нажмите на «Добавить нового пользователя для этого компьютера». В результате поступит предложение ввести электронный адрес или номер телефона для авторизации. Чтобы добавить локального пользователя нажмите на «У меня нет данных для данного человека» (рис. 3).

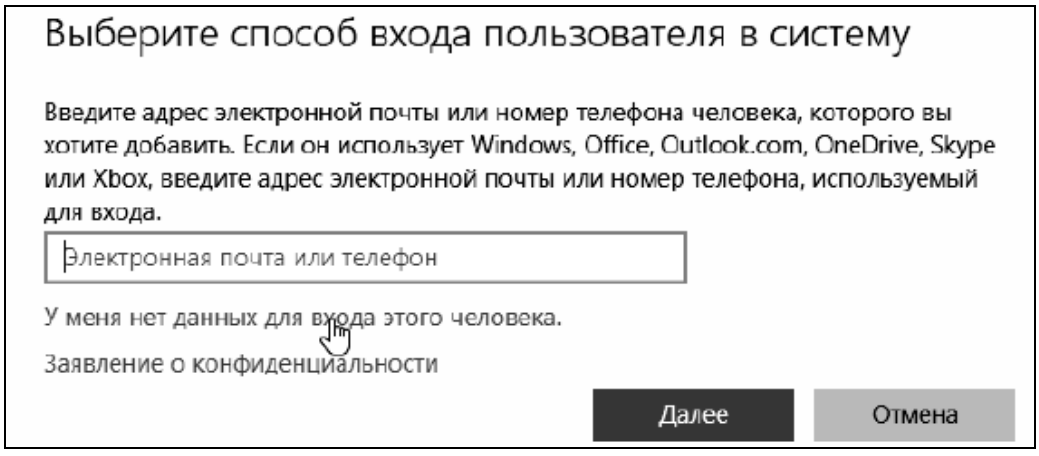


Рис. 3. Выбор способа входа в систему

Потом кликните по надписи: «Добавить пользователя без учётной записи» (рис. 4).

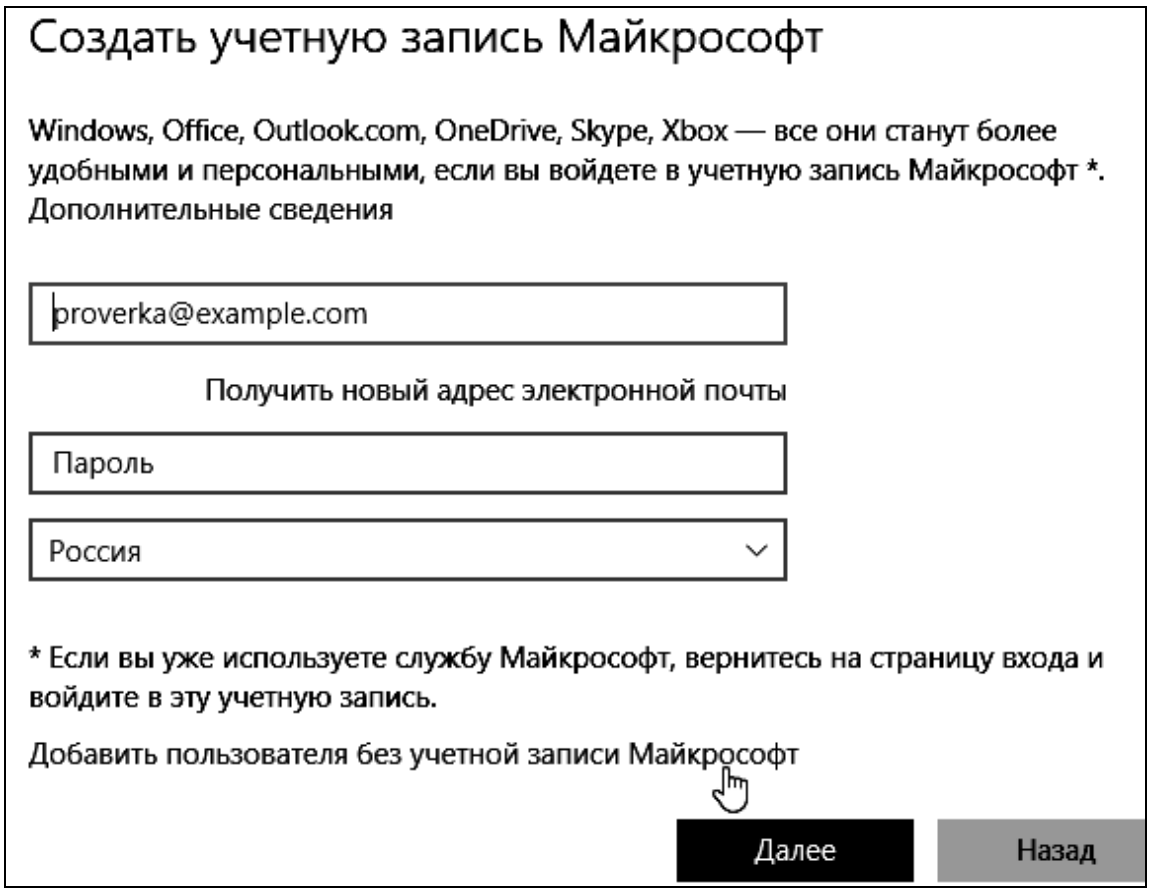


Рис. 4. Добавление локального пользователя

После этого потребуется задать имя пользователя и пароль для него, а также подсказку для пароля. После завершения создания пользователя – соответствующая запись появится в перечне учетных записей на данном компьютере.

Запустите Microsoft Management Console (mmc) – компонент Windows, позволяющий администрировать систему. Откройте меню «Пуск – Выполнить – mmc». Для добавления необходимого набора оснасток в меню консоли выберите «Файл – Добавить или удалить оснастку». В результате будет предложен перечень, из которого пользователь может выбрать одну или несколько оснасток.

Нажмите «Файл» и перейдите в пункт «Параметры». Здесь можно выбрать режим работы пользователя с этой консолью: авторский режим, предоставляющий пользователю полный доступ ко всем функциям MMC, и пользовательский режим.

Существует три вида пользовательского режима:

– полный доступ (full access) даёт пользователю доступ ко всем командам MMC, но не позволяет добавлять или удалять оснастки, или изменять свойства консоли;

– ограниченный доступ, много окон (Limited Access Multiple Windows) позволяет пользователю осуществлять доступ только к областям дерева консоли, которые отображались при сохранении консоли, а также открывать новые окна;

– ограниченный доступ, одно окно (Limited Access Single Window) работает так же, как многооконный ограниченный доступ с той разницей, что пользователь не может открывать новые окна.

Сохраните консоль в авторском и пользовательских режимах (рис. 5). Выявите отличия работы консоли в различных режимах.

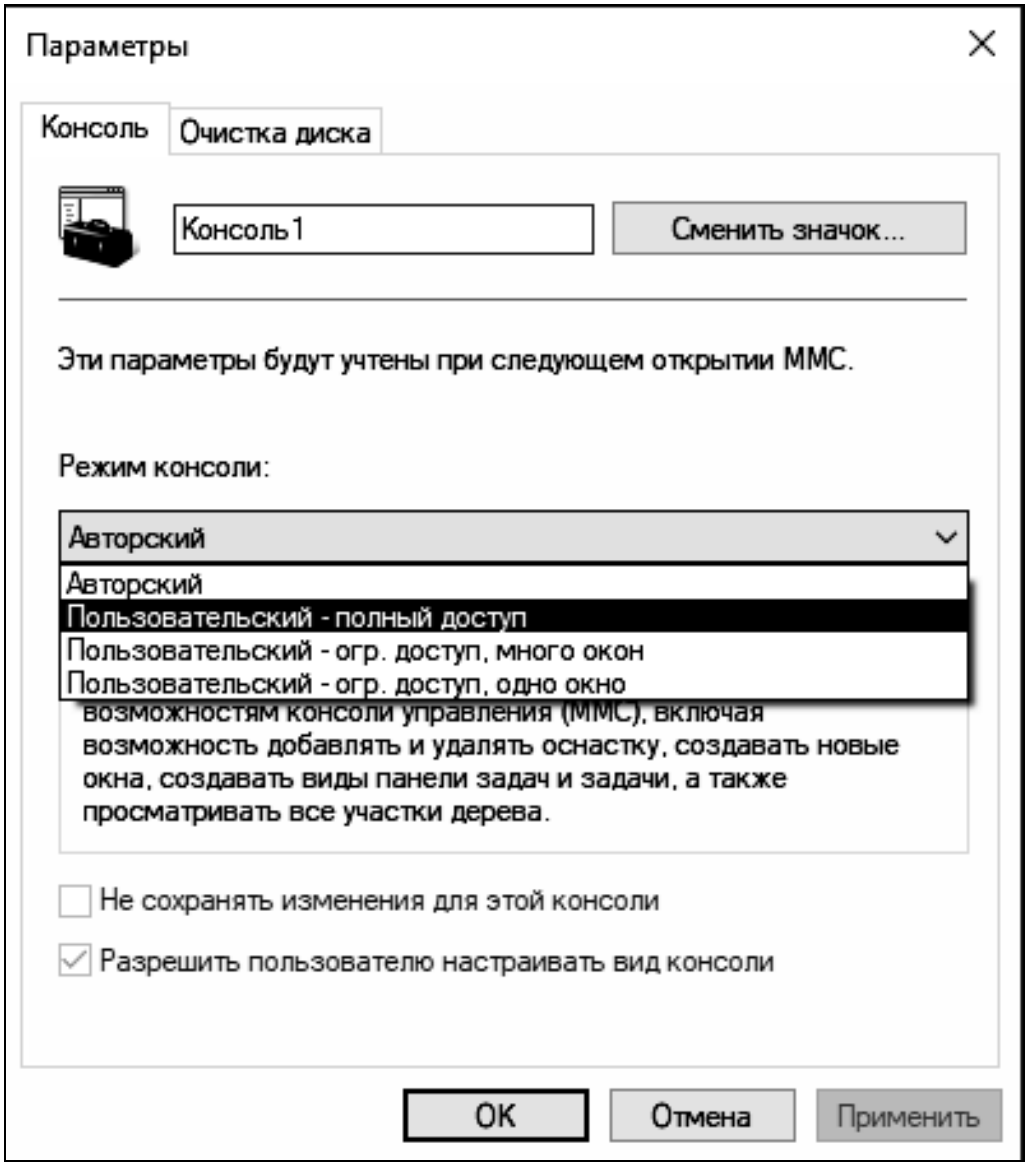


Рис. 5. Параметры режима консоли

Через пункт «Добавить или удалить оснастку» добавьте «Локальные пользователи и группы» (рис. 6).

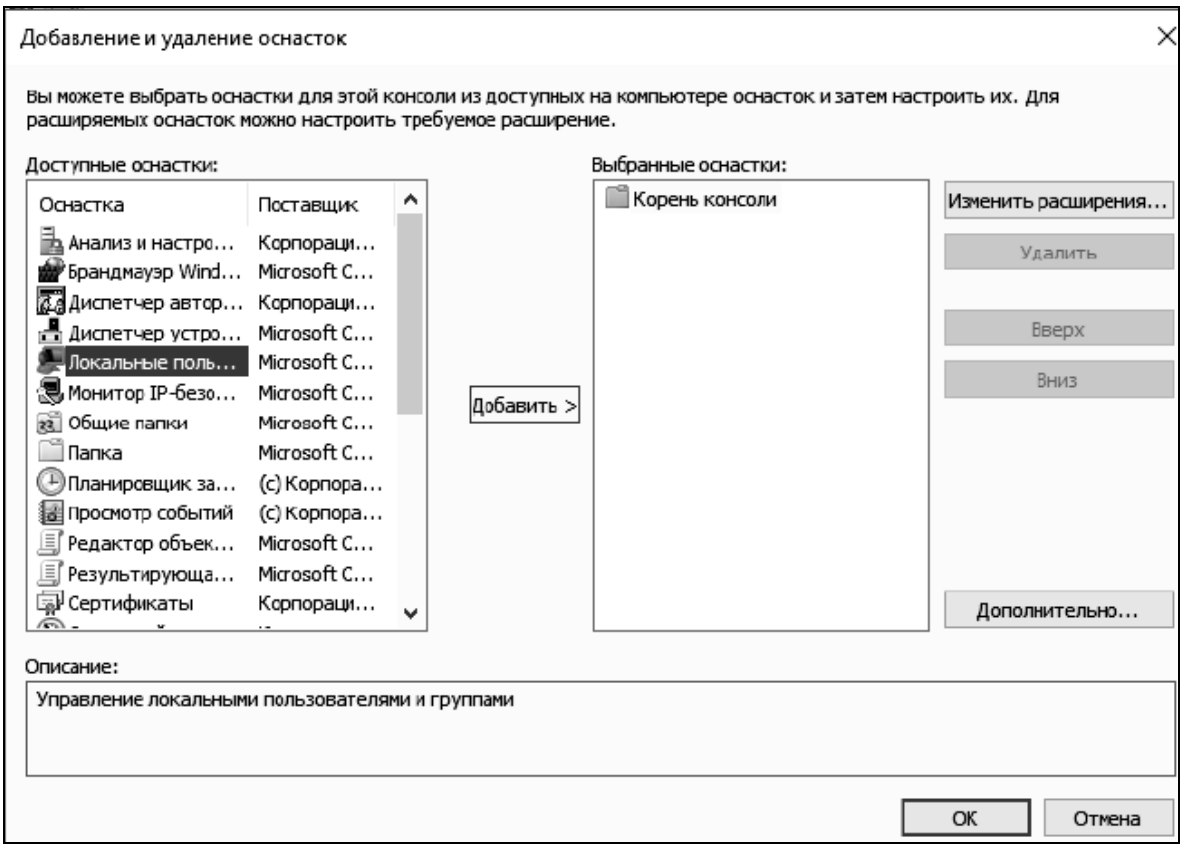


Рис. 6. Добавление оснастки

Через данную оснастку также возможно добавить нового пользователя (рис. 7).

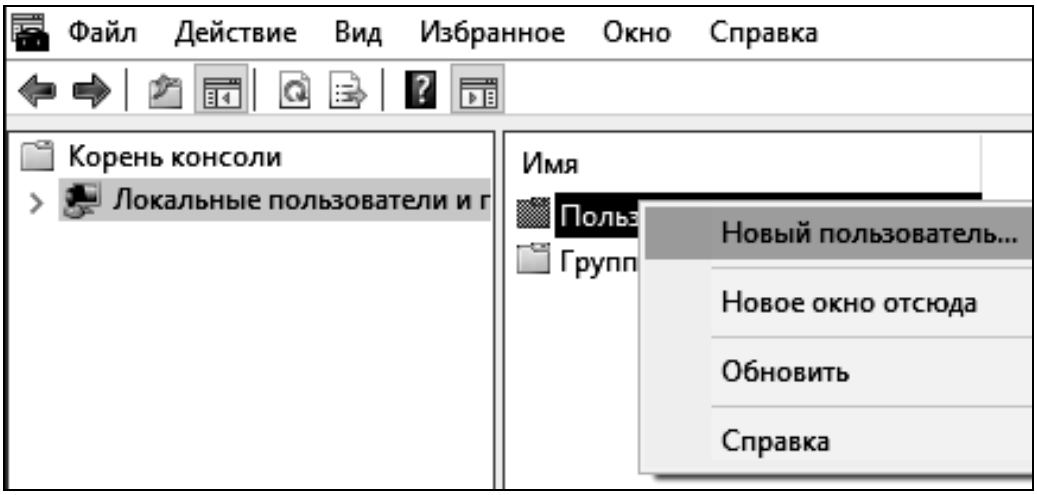


Рис. 7. Добавление пользователя через оснастку

В появившемся окне (рис. 8) введите имя учётной записи, а также пароль и его подтверждение. Если администратор устанавливает пользователю временный пароль, то для обязательной смены пароля необходимо включить параметр «Потребовать смену пароля при следующем входе в систему». Сразу после успешной аутентификации пользователь

получает запрос на смену пароля, в ответ на который он должен задать новый пароль. Этот подход необходимо использовать в тех случаях, когда администратор системы не должен знать пароли пользователей.

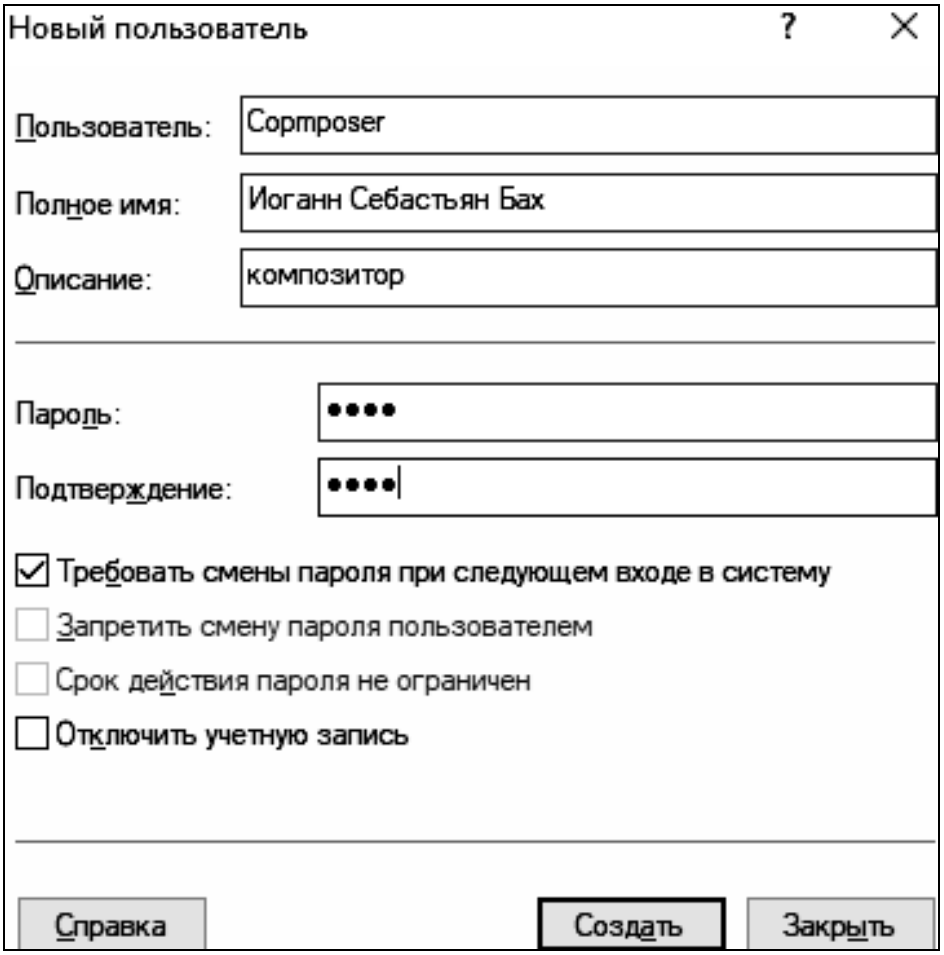


Рис. 8. Настройка параметров учётной записи при её создании

Если пользователь забыл свой пароль, то член группы «Администраторы» может сбросить его старый пароль при помощи функции «Задать пароль», доступной в контекстном меню учётной записи этого пользователя (рис. 8). Смените пароль у созданной учётной записи.

В данный момент времени учетная запись «Администратор» является заблокированной (рис. 10). Разблокируйте её, выбрав соответствующий пункт в свойствах учетной записи. Посмотрите какие еще параметры можно настроить через свойства.

Войдите в систему под созданной учётной записью. При первом входе пользователю будет выдано сообщение о необходимости ввести пароль (рис. 11) и окно смены пароля (рис. 12). Смените пароль созданной учётной записи. Здесь подтверждение действий осуществляется клавишей «Enter».

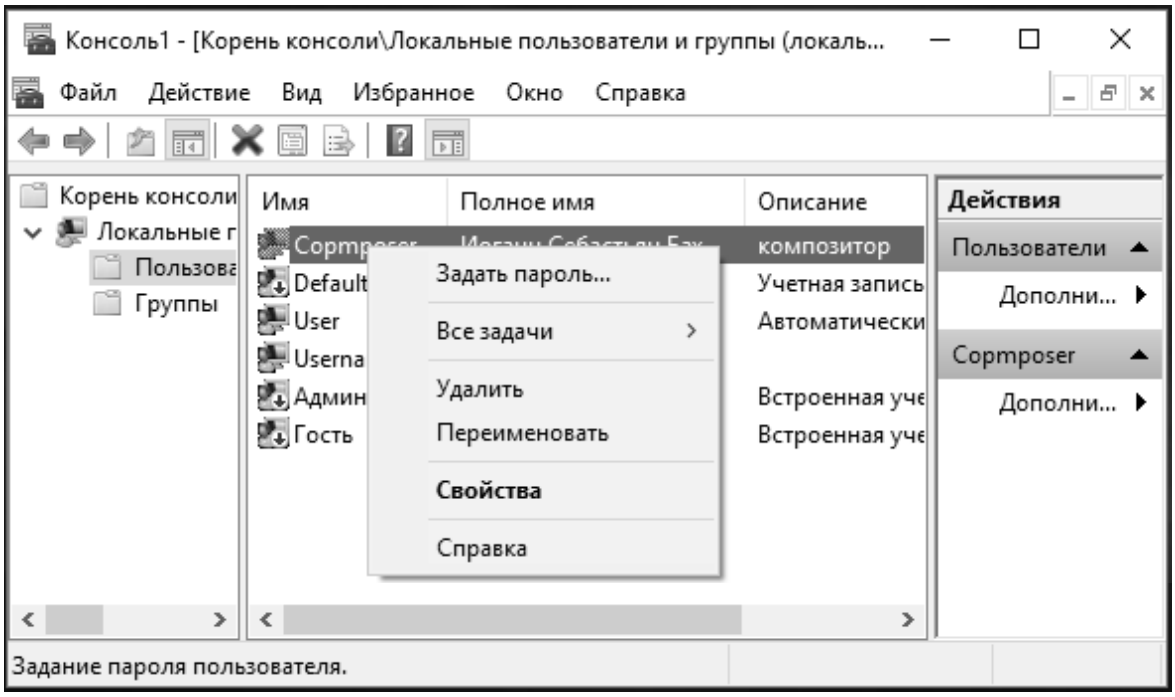


Рис. 9. Задание пароля пользователя администратором

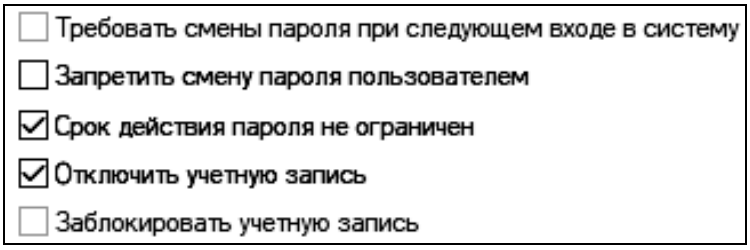


Рис. 10. Изменение свойств администратора

Рис. 11. Сообщение пользователю о необходимости смены пароля

Рис. 12. Окно «Смена пароля»

Для применения к пользователю набора прав и ограничений можно включить его учётную запись в группу пользователей с соответствующим набором прав и ограничений.

Войдите в систему под учётной записью «Администратор». Откройте «Свойства» созданной учётной записи. На вкладке «Членство в группах» добавьте пользователя в группу «Опытные пользователи» (рис. 13). Имя группы можно ввести самостоятельно или выбрать из списка, предоставляемого после последовательного нажатия кнопок «Дополнительно» и «Поиск».

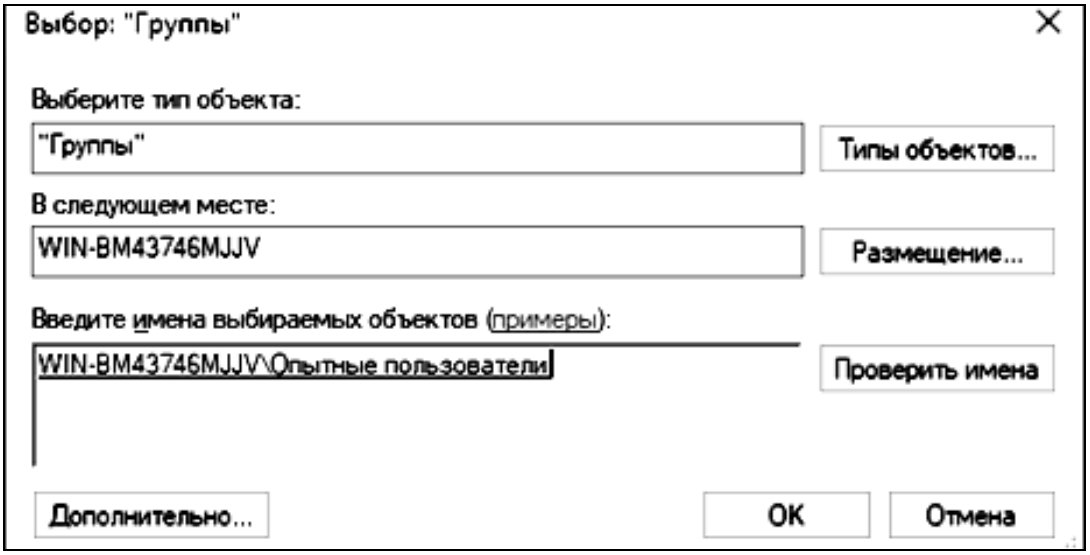


Рис. 13. Добавление группы

В разделе «Группы» откройте «Свойства» группы «Опытные пользователи» и проверьте наличие в группе добавленной учётной записи. Создайте новую группу и добавьте в неё этого же пользователя.

Вызовите командную строку и выполните команду «net user». Консоль выведет перечень всех имеющихся учетных записей (рис. 14)

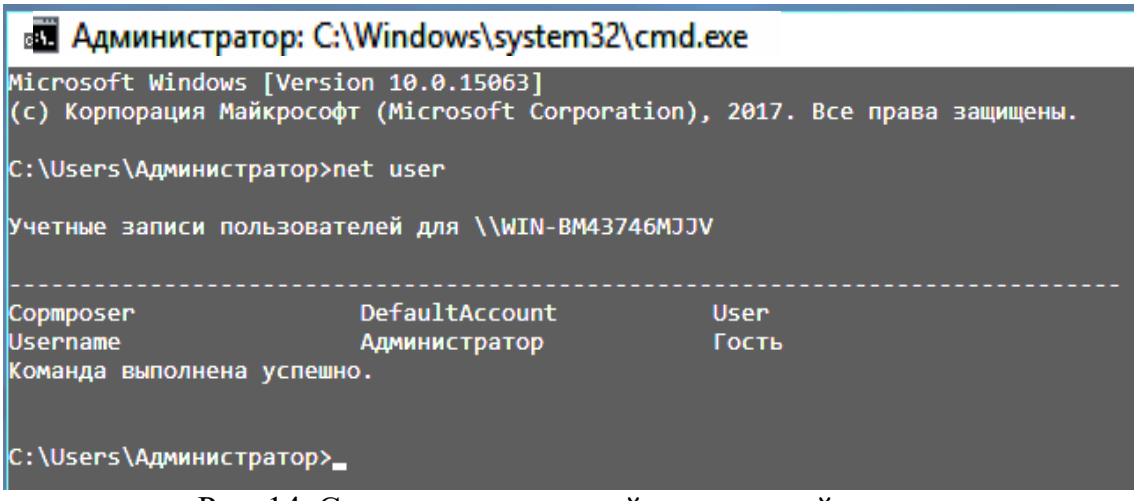


Рис. 14. Список пользователей в командной строке

Создание и изменение учётных записей осуществляется при помощи команды «net user». Подробную информацию о команде можно получить, введя «net user /help» (рис. 15). Изучите предлагаемые функции команды.

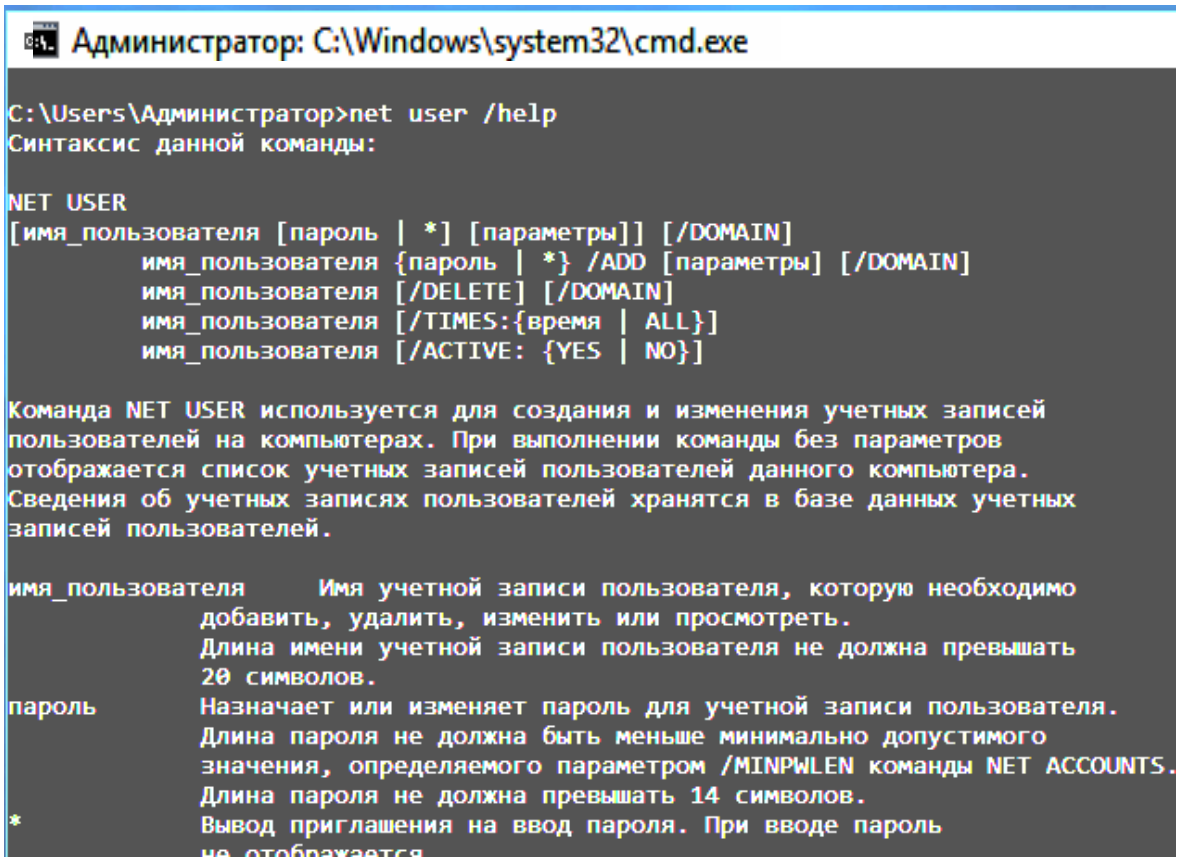


Рис. 15. Справка по команде Net user

Создайте учётную запись пользователя с именем, совпадающим с Вашим именем в кафедральной сети, явно указав пароль. При создании дополнительно к логину укажите полное имя пользователя (рис. 16).

Синтаксис команды Net user при создании учётной записи пользователя:

Net user имя_пользователя {пароль | *} /ADD [параметры].

Для добавления полного имени пользователя нужно в качестве параметра ввести: /FULLNAME: «имя».

```
C:\Users\Администратор>net user XXX 12345 /add /fullname:"XXX YYY"
Команда выполнена успешно.
```

Рис. 16. Создание нового пользователя

Проверьте наличие созданной учётной записи в списке пользователей при помощи команды Net user. Команда Net user имя_пользователя, введённая без параметров, позволяет просмотреть информа-

цию об указанном пользователе. Просмотрите информацию о созданной учетной записи.

Возможен ввод пароля без отображения на экране – для этого вместо пароля нужно ввести «*». Измените пароль созданного пользователя при помощи команды Net user имя_пользователя * (рис. 17).

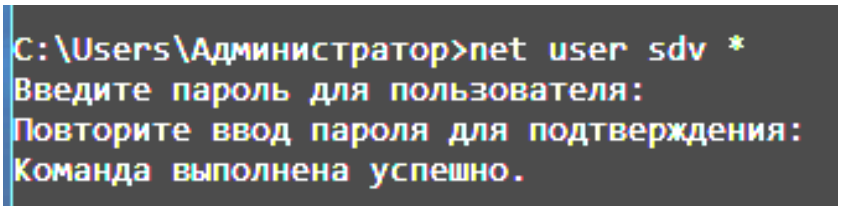


Рис. 17. Изменение пароля пользователя

Существует возможность установки ограничений на работу пользователя в операционной системе по времени. Для этого используется параметр /TIMES:{промежуток | ALL}. Значение ALL указывает, что пользователь может войти в систему в любое время, а пустое значение указывает, что пользователь не может войти в систему никогда. Ограничьте время работы созданного пользователя рамками рабочего времени (рис. 18). Переведите часы на время, не входящее в интервал рабочего, и протестируйте возможность входа пользователя в операционную систему.

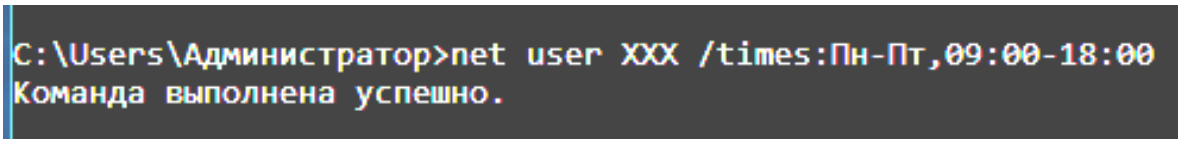


Рис. 18. Задание интервала действия учетной записи

В случае необходимости администратор может заблокировать учётную запись пользователя. Заблокируйте учётную запись созданного пользователя при помощи параметра /ACTIVE:{YES | NO} (рис. 19).

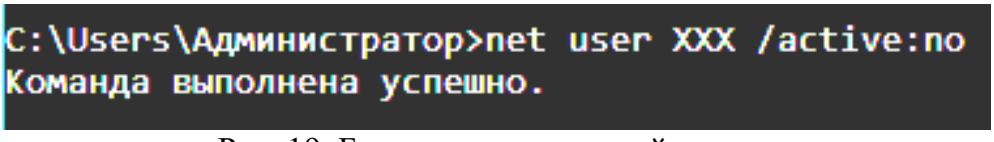


Рис. 19. Блокирование учетной записи

Проверьте применение блокирования к учётной записи при помощи команды Net user имя_пользователя. В выдаваемой о пользователе информации есть графа «Учётная запись активна», показывающая состояние блокирования учётной записи. Разблокируйте учётную запись пользователя.

Если пользователь временно работает в организации, то администратор может ограничить время действия учётной записи пользователя. Для этого служит параметр: /EXPIRES:{дата | NEVER}. Если используется значение NEVER, то время действия учётной записи не имеет ограничений срока действия. Ограничьте время действия учётной записи созданного пользователя (рис. 20). Установите системное время на срок более поздний, чем установленное ограничение. Попытайтесь войти в систему под данной учётной записью – операционная система выдаст ошибку (рис. 21).

```
C:\Users\Администратор>net user XXX /expires:19.09.2017
Команда выполнена успешно.
```

Рис. 20. Ограничение времени действия учётной записи

Рис. 21. Ошибка при попытке входа под просроченной учётной записью

Команда Net localgroup служит для создания локальных групп и управления ими. При использовании этой команды без указания параметров выводится перечень групп пользователей, существующих в операционной системе (рис. 22). Выведите список всех существующих групп.

Синтаксис команды Net net при создании локальной группы: Net localgroup имя_группы {/ADD }. Создайте локальную группу Students (рис. 23).

Проверьте наличие созданной группы пользователей при помощи команды Net localgroup. Добавление пользователей в группу осуществляется командой Net localgroup имя_группы имя [...] {/ADD }, где имя [...] – имя одного или нескольких пользователей (имена разделяются пробелами).

Добавьте ранее созданного пользователя в группу Students. Команда Net localgroup имя_группы выводит список пользователей, входящих в указанную группу. Выведите список пользователей группы Students (рис. 24).

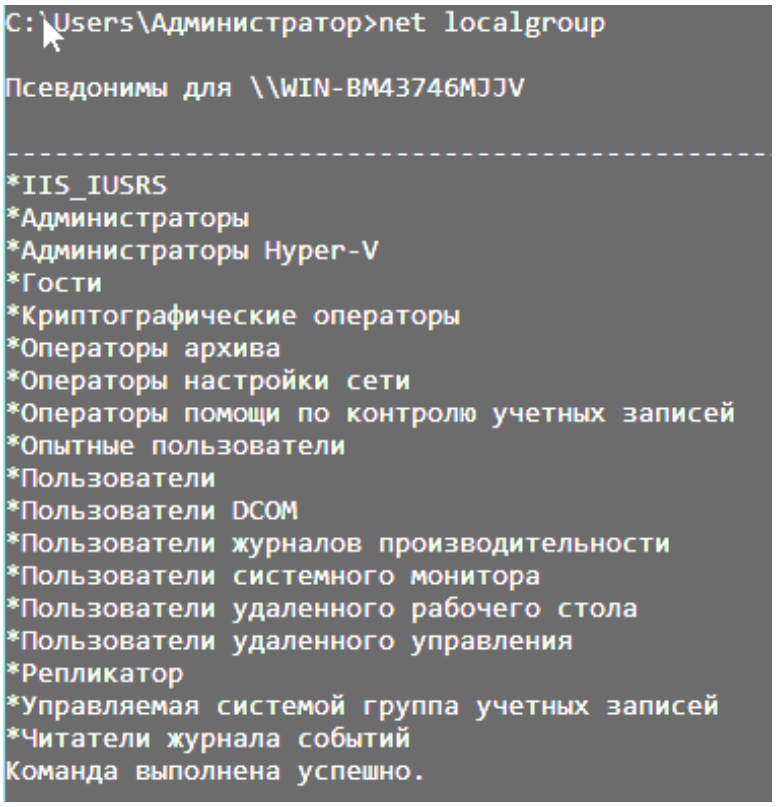


Рис. 22. Список групп

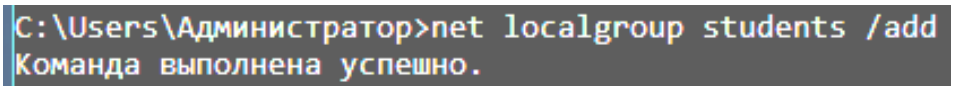


Рис. 23. Создание группы

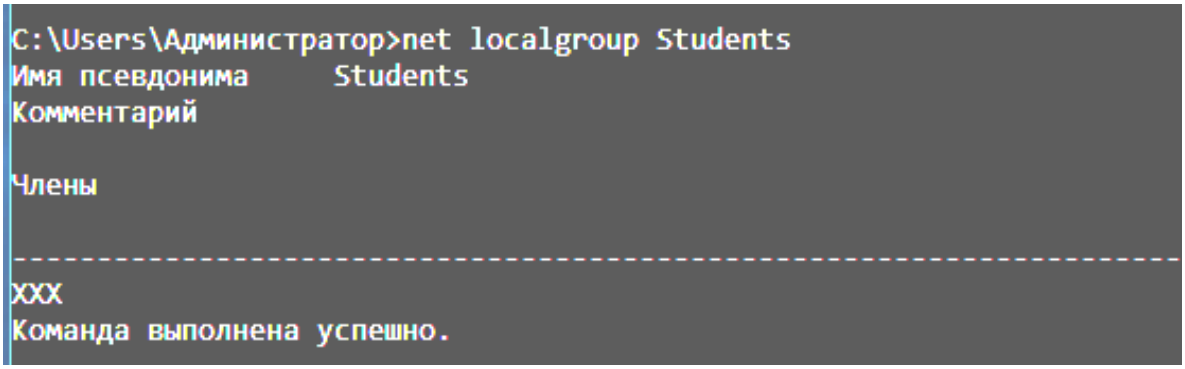


Рис. 24. Просмотр списка пользователей заданной группы

Для удаления пользователя из группы используется команда Net localgroup имя_группы имя_пользователя {/DELETE}. Удалите группу Students (рис. 25).

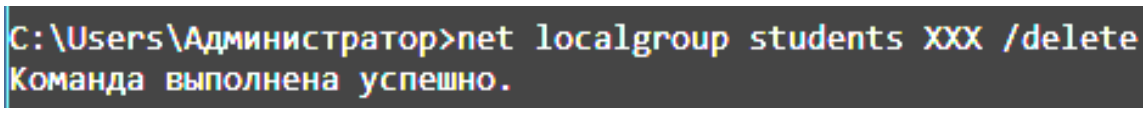


Рис. 25. Исключение пользователя из группы

Для удаления группы используется команда Net localgroup имя_группы {/DELETE}. Удалите группу Students (рис. 26).

```
C:\Users\Администратор>net localgroup students /delete
Команда выполнена успешно.
```

Рис. 26. Удаление группы пользователей

Проверьте отсутствие группы Students, используя команду вывода списка существующих групп пользователей.

3.2. Настройка политики учётной записи

Откройте «Локальную политику безопасности», вызвав её запросом secpol.msc в меню «Пуск». Основное окно «Локальной политики безопасности» представлено на рисунке 27. Значения параметров, заданные при настройке политики, будут применяться ко всем пользователям локального компьютера.

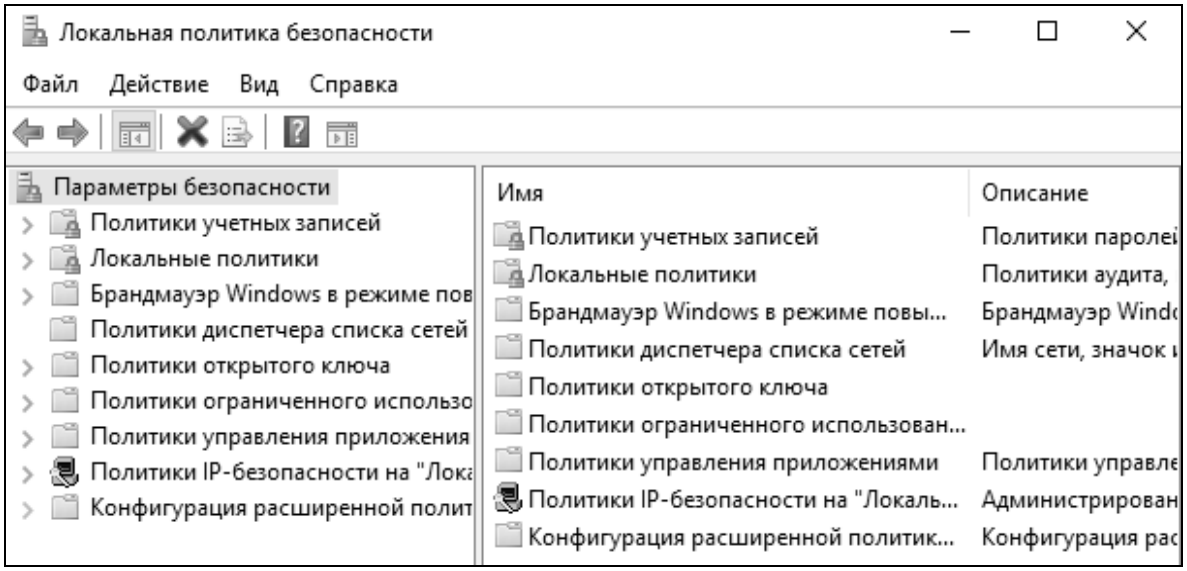


Рис. 27. Локальная политика безопасности

Раздел «Политики учётных записей» «Локальной политики безопасности» включает в себя настройки, применяющиеся к паролям пользователей.

Выберите раздел «Политика паролей» («Параметры безопасности – Политики учётных записей – Политика паролей»). Настройки, входящие в раздел «Политика паролей», представлены на рис. 28.

Выполните следующие задания:

– установите максимальный срок действия пароля – 30 дней;

– установите минимальную длину пароля – 10 символов;

– для параметра «Вести журнал паролей» установите значение 3 хранимых пароля, означающее, что новый пароль должен отличаться от 3 последних паролей пользователя;

– включите параметр «Пароль должен отвечать требованиям сложности».

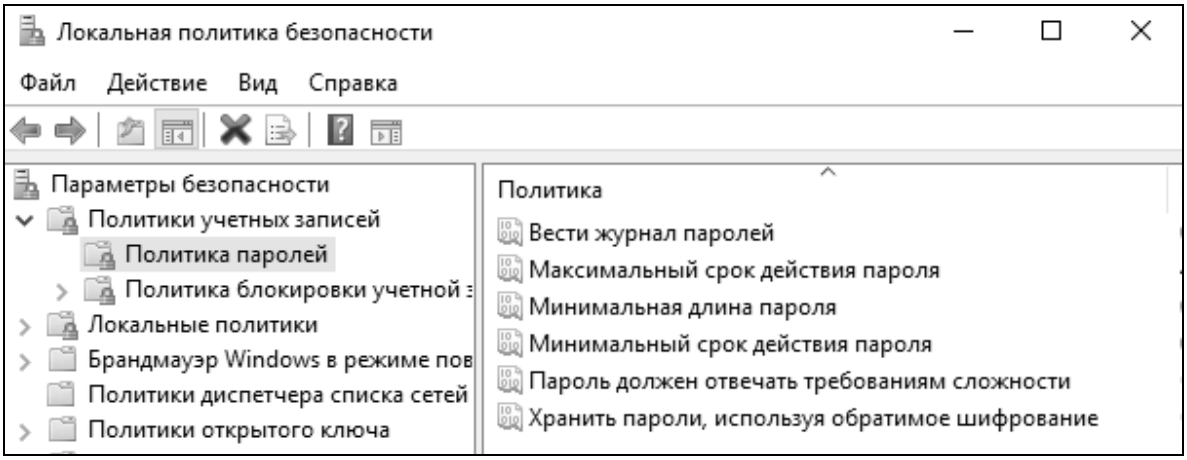


Рис. 28. Политика паролей

Параметр «Пароль должен отвечать требованиям сложности» определяет требования сложности для паролей. Если эта политика включена, то пароли должны удовлетворять следующим минимальным требованиям:

– пароль не может содержать имя учётной записи пользователя или какую-либо его часть;

– пароль должен состоять не менее чем из шести символов;

– в пароле должны присутствовать символы трёх категорий из числа следующих четырёх:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) неалфавитные символы (например !, $, #, %).

Проверка соблюдения этих требований выполняется при изменении или создании паролей. При помощи этого параметра можно избавиться от легко подбираемых паролей типа «111», «qwerty», «12345» и т.д.

Убедитесь, что для пользователя не включена опция «Срок действия пароля неограничен» в оснастке «Локальные пользователи и группы». Переведите системное время более чем на 30 дней вперёд. Попытайтесь войти под созданной учётной записью. Пользователю будет выдано сообщение об истечении срока действия пароля (рис. 29). При

смене пароля попытайтесь заменить пароль на более простой (например, abc12345 или включающий имя учётной записи).

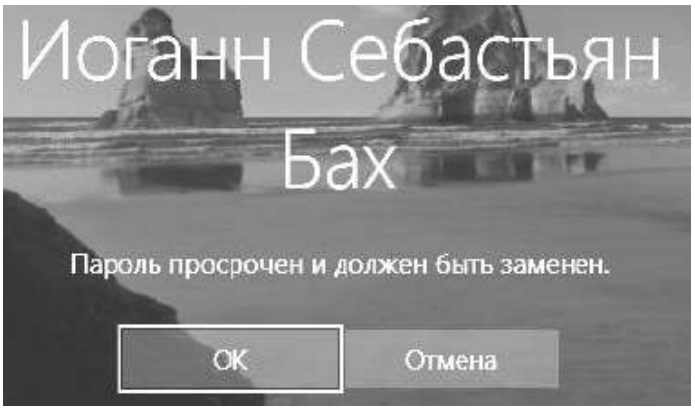


Рис. 29. Сообщение об истечении срока действия пароля

В этом случае пользователю будет выдано сообщение об ошибке при смене пароля (рис. 30). Введите пароль, удовлетворяющий требованиям.

Рис. 30. Сообщение о несоответствии пароля требованиям

Войдите в систему под учётной записью «Администратор». Переведите системное время в исходное состояние. Выберите раздел «Политика блокировки учётной записи» («Параметры безопасности – Политики учётных записей – Политика блокировки учётной записи»). Настройки, входящие в раздел «Политика блокировки учётной записи», представлены на рисунке 31.

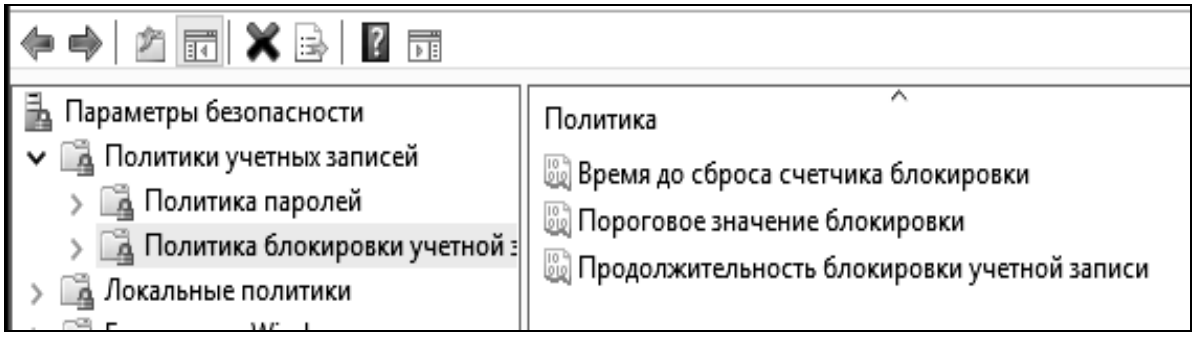


Рис. 31. Политика блокировки учетной записи

Настройте параметры следующим образом:

– установить пороговое значение блокировки, равное 3 ошибкам входа в систему (после 3 неудачных попыток входа учётная запись блокируется);

– установить длительность блокировки в параметре «Блокировка учётной записи на», равную 30 мин (значение 0 означает, что блокировку может снять только администратор);

– установите сброс счётчика блокировки через 15 мин. Если в течение установленного времени будет 3 неудачных попытки входа, то учётная запись блокируется. Если неудачных попыток в течение установленного времени будет меньше, то опять допускается 3 неудачных попытки (значение этого параметра не должно превышать длительность блокировки учётной записи).

Завершите сеанс учётной записи «Администратор». При входе в систему под созданной учётной записью три раза введите неправильный пароль. При следующей попытке входа в систему будет выдано сообщение о блокировании созданной учётной записи (рис. 32).

Рис. 32. Сообщение о блокировке учетной записи

Войдите в систему под учётной записью «Администратор». Разблокируйте созданную учётную запись. Для этого в окне «Свойства» этой учётной записи отключите настройку «Заблокировать учётную запись».

Вызовите командную строку. Net accounts используется для обновления базы данных регистрационных записей и изменения параметров входа в сеть (LOGON) и требований к паролям для всех регистрационных записей. При использовании этой команды без указания параметров выводятся текущие значения параметров, определяющих требования к паролям и другие параметры. Выведите текущие параметры входа в систему (рис. 33).

Задайте следующие требования к паролю:

– минимальную длину – 6 символов;

– максимальный срок действия пароля – 40 дней;

– запрет использования 3 последних паролей пользователя.

```
C:\Users\Администратор>net accounts
Принудительный выход по истечении времени через:        Никогда
Минимальный срок действия пароля (дней):                0
Максимальный срок действия пароля (дней):               10
Минимальная длина пароля:                               10
Хранение неповторяющихся паролей:                       3
Блокировка после ошибок ввода пароля:                   3
Длительность блокировки (минут):                        30
Сброс счетчика блокировок через (минут):                15
Роль компьютера:                                        РАБОЧАЯ СТАНЦИЯ
Команда выполнена успешно.
```

Рис. 33. Просмотр информации о требованиях к качеству паролей

Применение этих требований (рис. 34) производится при помощи следующих параметров команды Net accounts:

/MINPWLEN:длина

/MAXPWAGE:дни

/UNIQUEPW:число

```
C:\Users\Администратор>net accounts /minpwlen:6 /maxpwage:40 /uniquepw:3
Команда выполнена успешно.
```

Рис. 34. Изменение требований к качеству паролей

3.3. Групповые политики

Откройте оснастку «Групповая политика» («Пуск – Выполнить – gpedit.msc»). Оснастка «Групповая политика» состоит из двух основных частей: конфигурация компьютера и конфигурация пользователя (рис. 35).

«Конфигурация компьютера» используется для задания политики, применяемой к компьютерам, вне зависимости от того, какой пользователь работает на них. «Конфигурация пользователя» используется для задания политики, применяемой к пользователям независимо от того, какой компьютер используется для входа в систему.

Созданная групповая политика может быть экспортирована на другой локальный компьютер. Для того чтобы произвести экспорт данных необходимо в оснастке «Групповая политика» выделить нужный узел и во вкладке «Действие» выбрать пункт «Экспортировать список». В появившемся окне выбрать путь сохранения и указать имя файла.

«Конфигурация компьютера» по умолчанию состоит из следующих разделов: конфигурация программ, конфигурация Windows и административные шаблоны (рис. 36).

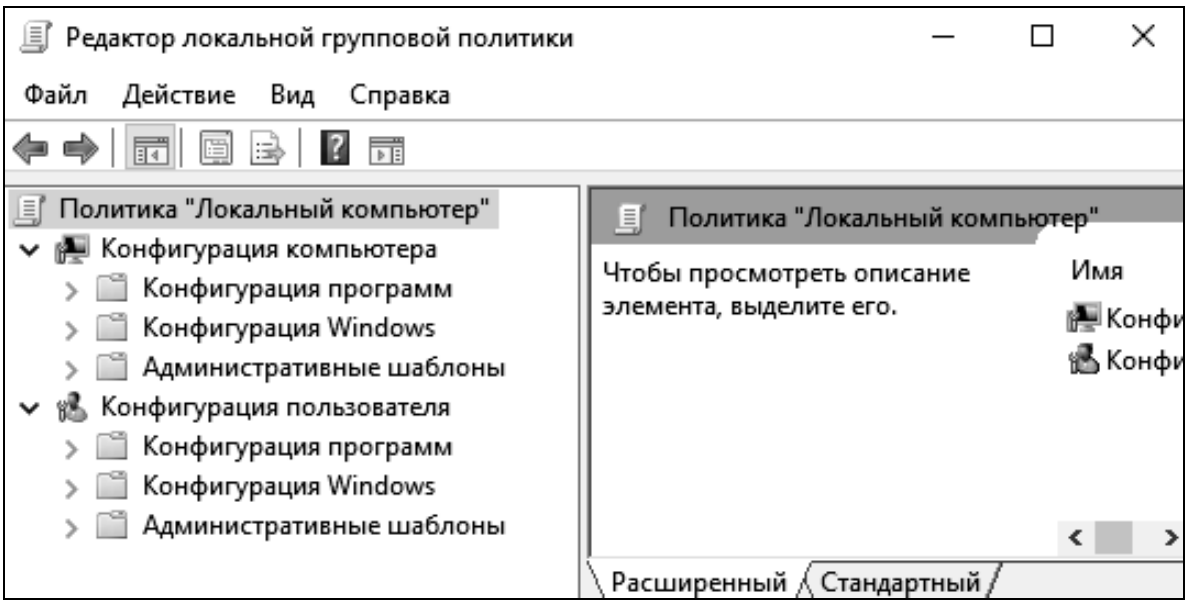


Рис. 35. Редактор групповых политик

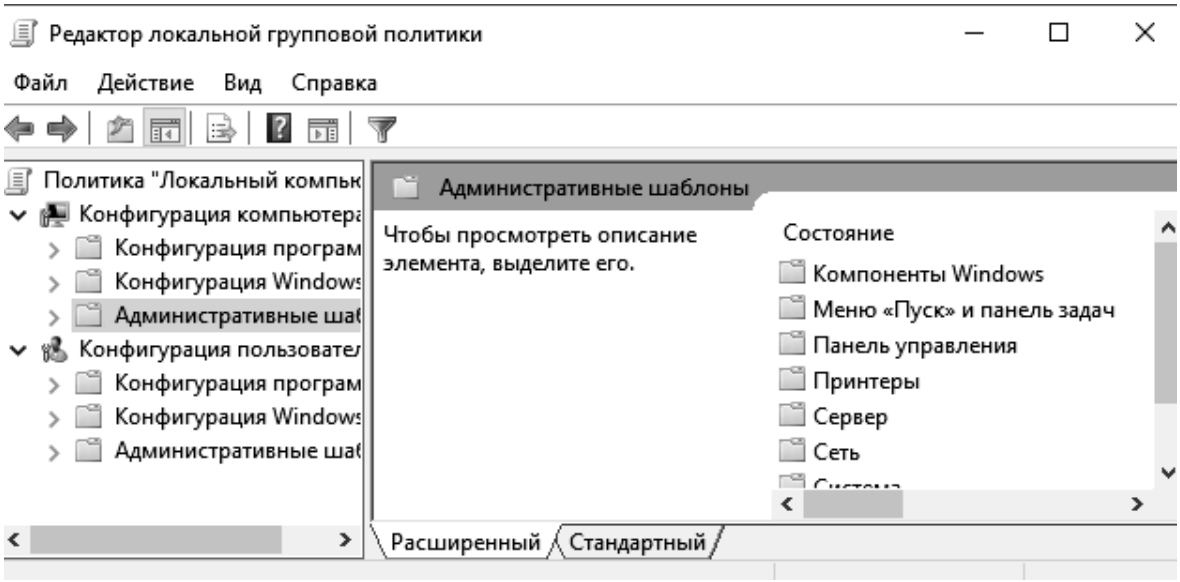


Рис. 36. Раздел «Административные шаблоны»

Средствами виртуальной машины подключите компакт-диск. В разделе «Административные шаблоны» выберите подраздел «Компоненты Windows» – «Политики автозапуска». Включите параметр «Выключение автозапуска» (рис. 37). Чтобы проверить выполнение данного параметра, необходимо повторно вставить диск в CD-привод. Система не будет производить его автозапуск, как это делалось раньше.

В разделе «Система» откройте подраздел «Вход в систему» и выберите параметр «Выполнять эти программы при входе в систему». Включите этот параметр и добавьте несколько программ, которые будут запускаться при входе пользователя в систему (рис. 38).

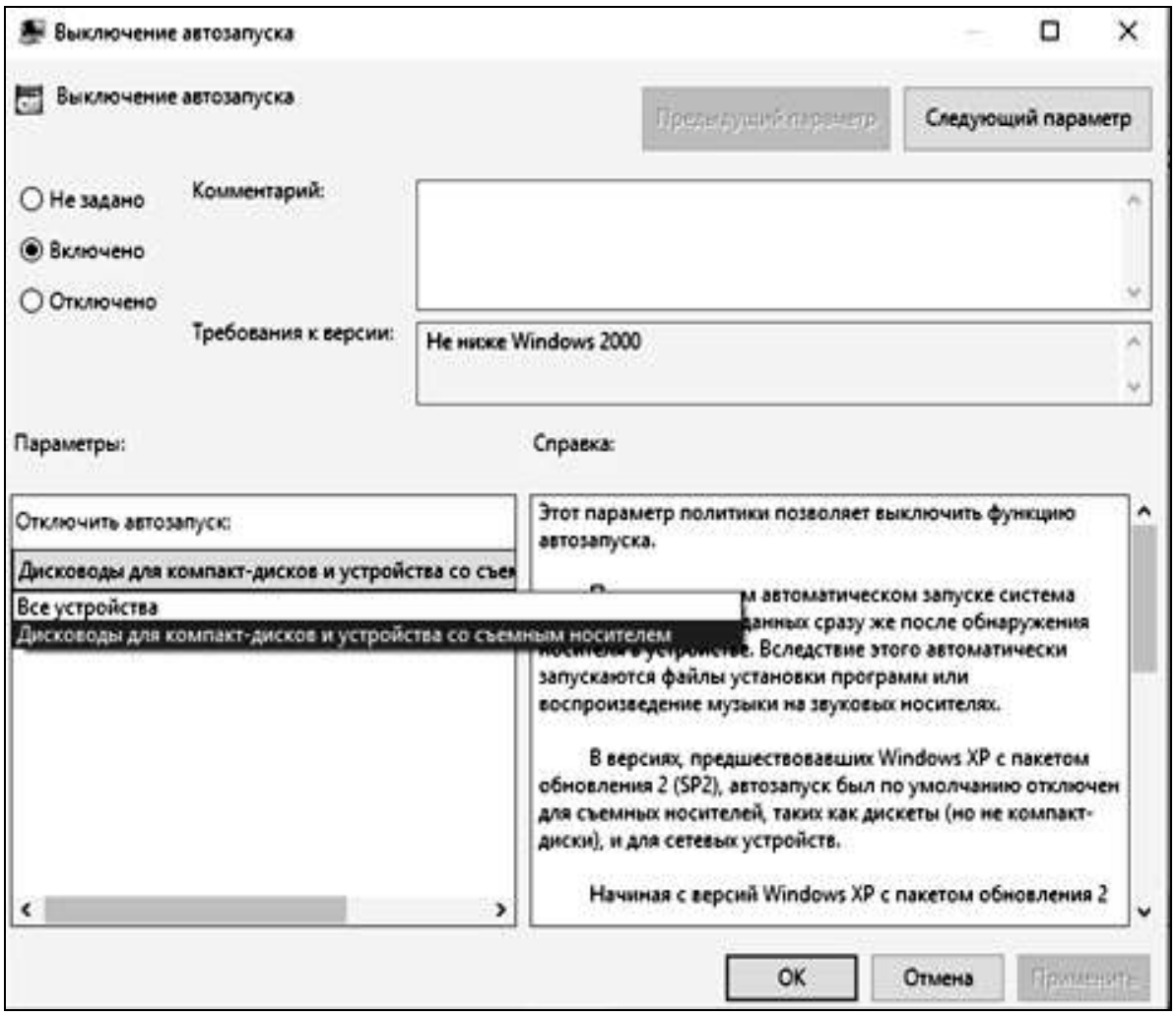


Рис. 37. Выключение автозапуска носителя

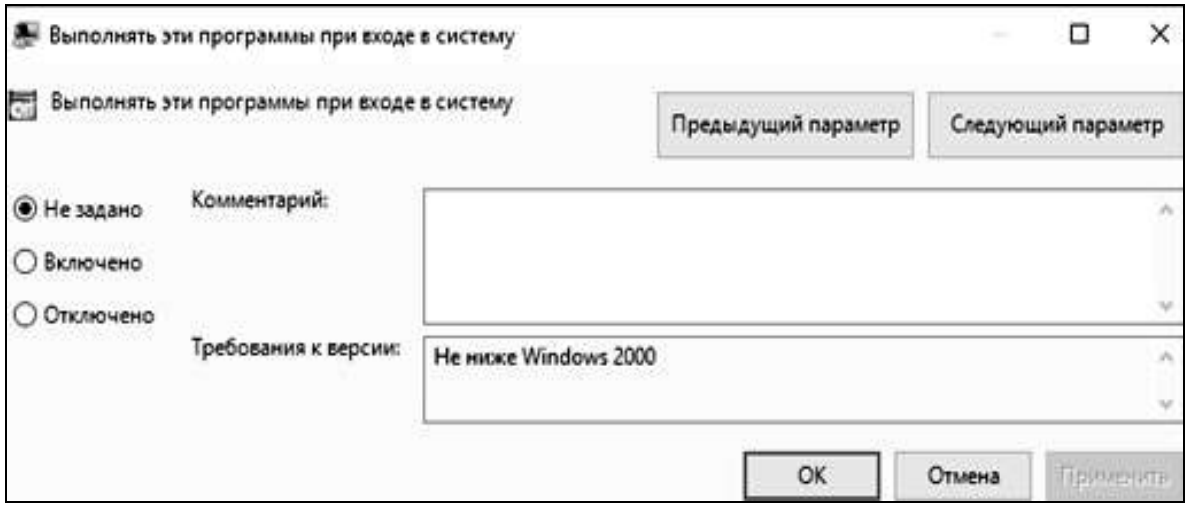


Рис. 38. Включение параметра

Добавленные программы (рис. 39) будут запускаться при каждом входе пользователя в систему. Для проверки повторно войдите в систему.

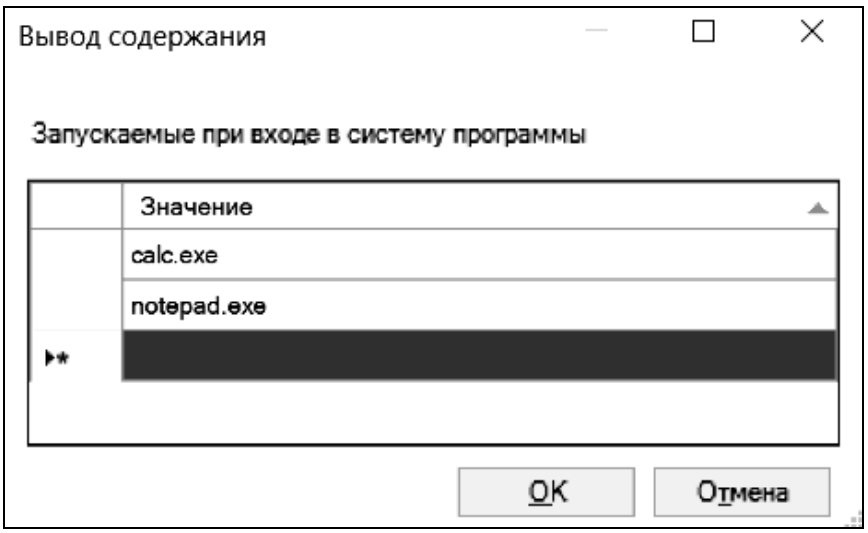


Рис. 39. Список запускаемых программ

«Конфигурация пользователя» по умолчанию состоит из тех же разделов, что и «Конфигурация компьютера». При помощи параметров групповой политики существует возможность ограничения доступа пользователя к логическим дискам. Можно скрыть выбранный диск из «Проводника», а также запретить доступ к нему.

Выберите параметр «Запретить доступ к дискам через «Мой компьютер», расположенный в подразделе «Компоненты Windows – Проводник» и запретите доступ к логическому диску C:\ (рис. 40).

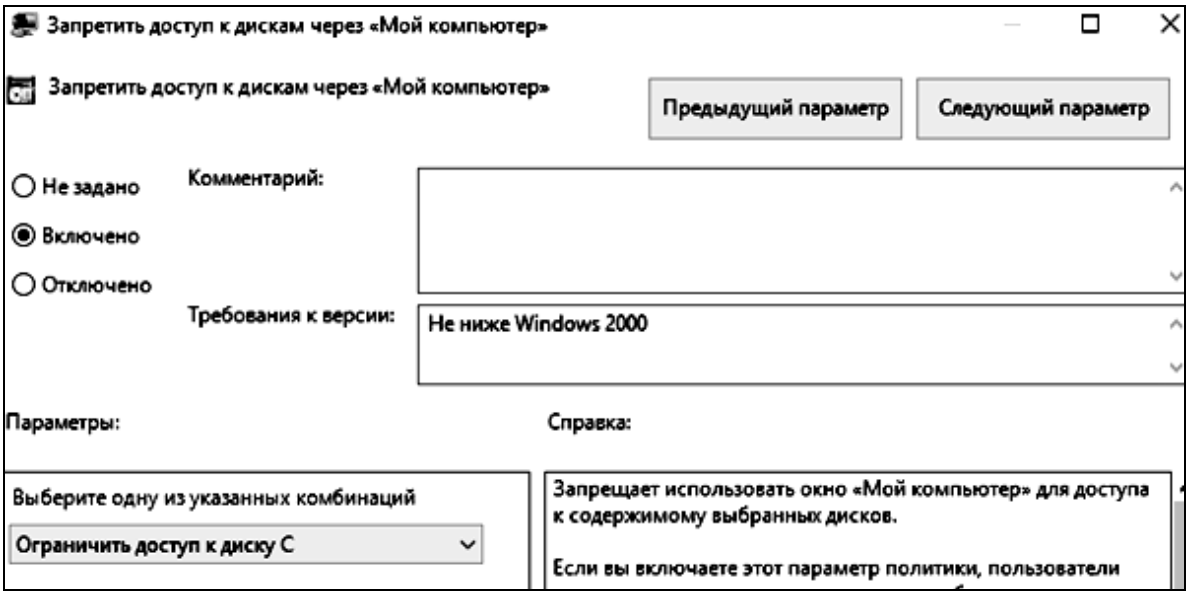


Рис. 40. Включение ограничения доступа к диску D

Попытайтесь открыть диск D:\ через «Мой компьютер» (рис. 41) и командную строку (рис. 42). В первом случае система откажет в до-

ступе, а во втором – доступ будет предоставлен (т.к. доступ запрещён только через «Проводник»).

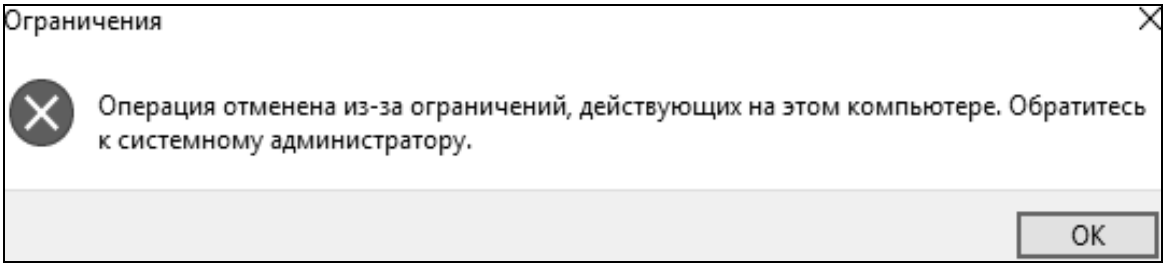


Рис. 41. Попытка доступа через проводник

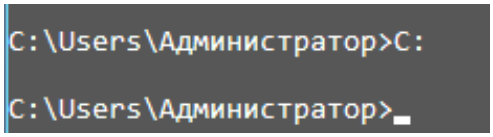


Рис. 42. Попытка доступа через командную строку

Ограничение доступа к средствам администрирования возможно за счёт запрета доступа к «Панели управления». Включите параметр «Запретить доступ к панели управления», находящийся в подразделе «Панель управления» (рис. 43). Попытайтесь открыть «Панель управления».

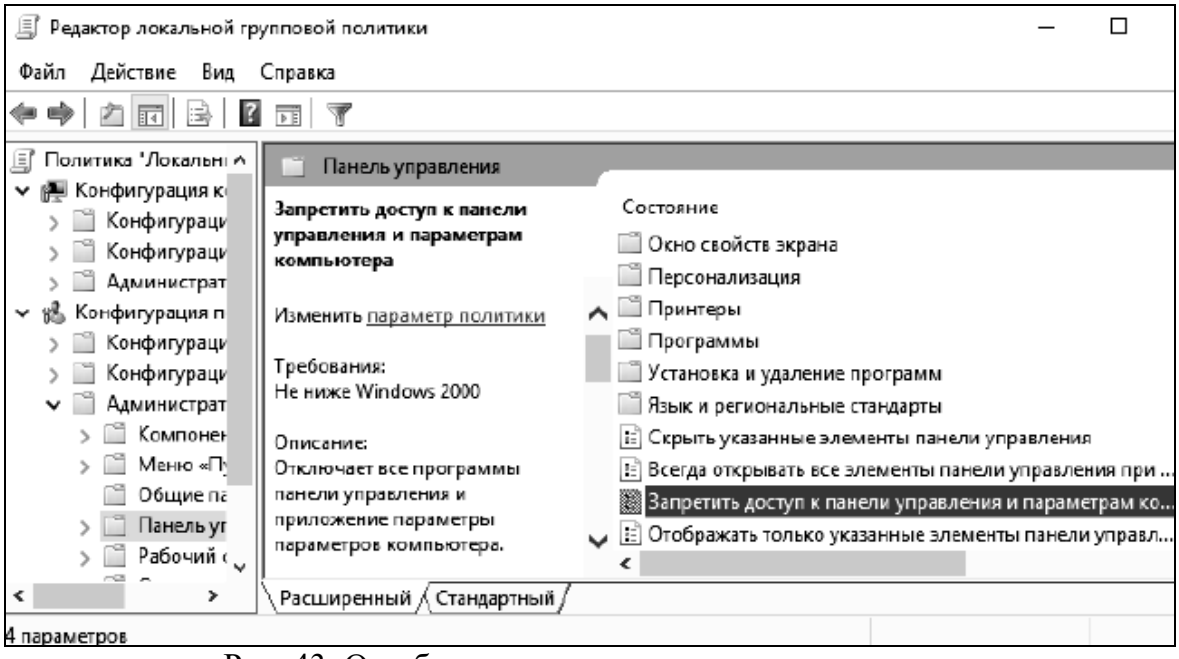


Рис. 43. Ошибка при открытии панели управления

Для полного запрета использования командной строки включите параметр «Запретить использование командной строки» в подразделе «Система». Попытайтесь запустить cmd.exe (рис. 44).

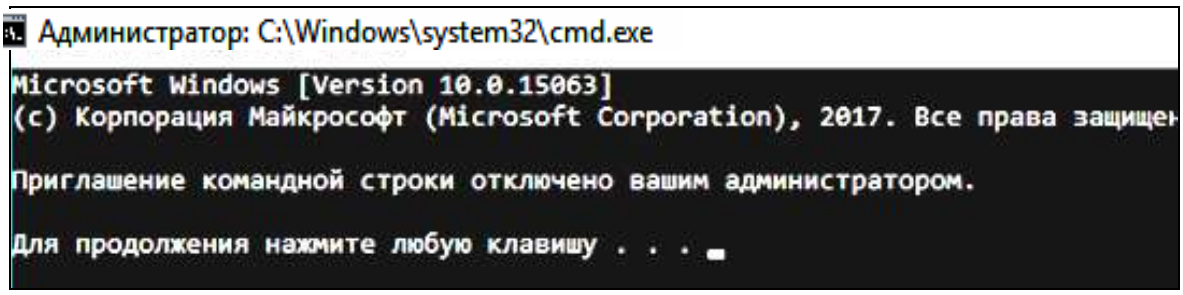


Рис. 44. Попытка запуска командной строки

Кроме того, в подразделе «Система» можно запретить использование редактора реестра. Для этого нужно включить параметр «Сделать недоступными средства редактирования реестра». Включите данный параметр и попытайтесь запустить редактор реестра C:\Windows\regedit.exe.

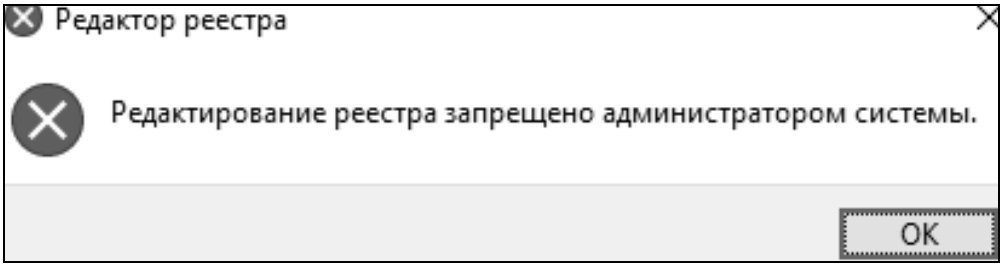


Рис. 45. Попытка запуска реестра

Добавление и удаление шаблонов может производиться через контекстное меню раздела «Административные шаблоны» (рис. 46). В появившемся контекстном меню выберите «Добавление и удаление шаблонов». В появившемся окне можно удалить любой шаблон, а также добавить новый шаблон политики.

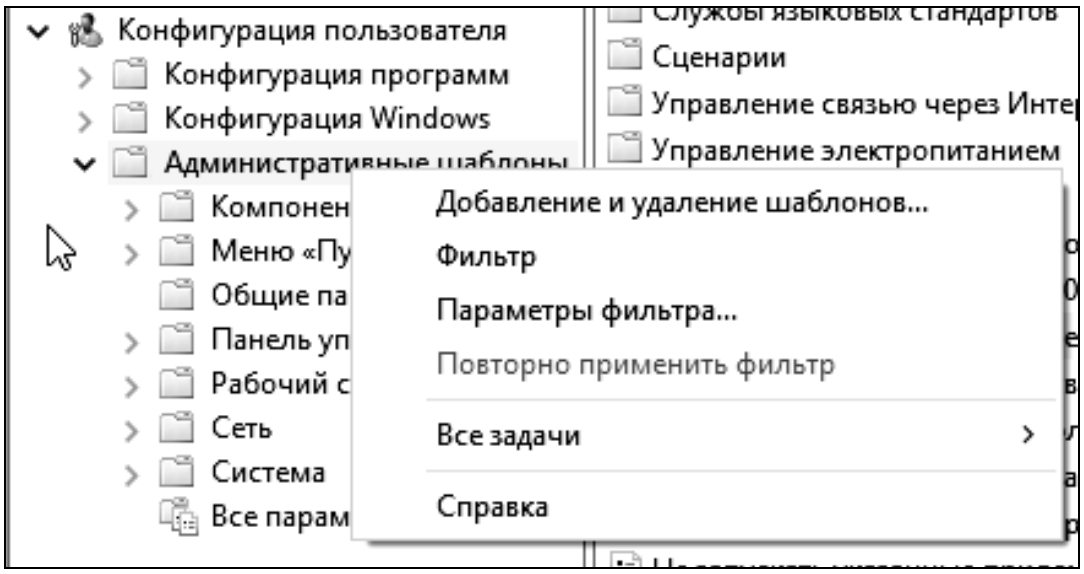


Рис. 46. Контекстное меню административных шаблонов

4. Задание на лабораторную работу

1. Ознакомьтесь с теорией.
2. Выполните представленные задания и составьте по проделанной работе отчет.
3. В оснастке «Локальные пользователи и группы» создайте новую группу пользователей. В качестве имени группы пользователей используйте номер Вашей учебной группы.
4. Создайте учётную запись с именем Вашей учётной записи в кафедральной сети и включите её в созданную группу.
5. Примените к созданной учётной записи настройки, указанные в Вашем варианте (табл. 1).
6. Создайте новую консоль. Добавьте в корень консоли оснастки «Редактор объекта групповой политики» и «Результирующая политика». Сохраните консоль в режиме, указанном в Вашем варианте (табл. 2.).

Таблица 1

Варианты заданий работы с пользователями

Вариант / Параметр	1	2	3	4	5	6	7	8	9	10
Максимальный срок действия пароля	30	90	60	30	90	60	30	90	60	30
Минимальная длина пароля	6	7	8	9	10	6	7	8	9	10
Требовать неповторяемости паролей	6	5	4	3	2	6	5	4	3	2
Отвечать требованиям сложности	+	–	–	+	–	–	+	–	+	+
Пороговое значение блокировки	3	4	5	6	7	3	4	5	6	7
Блокировка учётной записи на…	10	20	30	45	60	10	20	30	45	60
Сброс счётчика блокировки через…	5	10	15	20	30	10	20	30	45	60
Завершение работы системы	+	+			+		+		+	
Локальный вход в систему	+	+	+	+	+	+	+	+	+	+
Изменение системного времени	+		+		+		+		+	

Таблица 2

Варианты работы с групповыми политиками

Вар.	Режим работы с консолью	Параметры групповой политики
1	*2*	*3*
1	Авторский	Запретить редактирование реестра. Ограничить размер профиля пользователя значением 5 МБ
2	Пользовательский – полный доступ	Запретить использование командной строки. Запретить изменение рисунка рабочего стола
3	Пользовательский – многооконный	Запретить использование сочетаний клавиш, включающих кнопку «Windows». Удалить имя пользователя из меню «Пуск»

Продолжение табл. 2

1	*2*	*3*
4	Пользовательский – однооконный	Запретить использование диспетчера задач. Установить обязательный запрос пароля при выходе из спящего режима
5	Авторский	Запретить доступ к «Панели управления». Запретить запуск «Блокнота»
6	Пользовательский – полный доступ	Установить обязательный запрос пароля при выходе из экранной заставки. Удалить «Завершение сеанса» из меню «Пуск»
7	Пользовательский – многооконный	Скройте диск D: (CD-привод) из окна «Мой компьютер». Удалить значок «Мои документы» с «Рабочего стола»
8	Пользовательский – однооконный	Удалите «Общие документы» из окна «Мой компьютер». Скрыть общие группы программ из меню «Пуск»
9	Авторский	Запретите доступ к диску C: из окна «Мой компьютер». Удалить «Сетевые подключения» из меню «Пуск»
10	Пользовательский – полный доступ	Запретить вызов «Свойств» объекта «Мой компьютер». Установить очистку списка последних использовавшихся документов при выходе из системы

7. Установите параметры групповой политики, указанные в Вашем варианте (табл. 2), и продемонстрируйте преподавателю результат применения параметров (например, невозможность запуска редактора реестра).

8. Продемонстрируйте преподавателю изменённые параметры при помощи «Результирующей политики» для пользователя «user».

5. Контрольные вопросы

1. Поясните параметр «Пароль должен отвечать требованиям сложности» и перечислите минимальные требования, которым должны удовлетворять пароли, если параметр включен.
2. Какие параметры входят в политику блокировки учётной записи?
3. Возможно ли, что учётная запись не будет блокирована при количестве ошибок большем, чем установленное пороговое значение?
4. Что такое и для чего применяется MMC?
5. Что такое оснастка?
6. В чём состоит отличие конфигурации компьютера от конфигурации пользователя в групповой политике?
7. Каким образом можно включить автозапуск программ через групповую политику?
8. При помощи какой команды можно получить список пользователей операционной системы?
9. При помощи какой команды можно получить список групп пользователей операционной системы?
10. При помощи какой команды можно создать нового пользователя?

Лабораторная работа № 2
Дискреционный механизм разграничения доступа к файловым объектам

Целью данной работы является практическое изучение дискреционного механизма разграничения доступа на основе встроенных средств операционной системы Windows XP Professional, позволяющих управлять доступом к файлам и папкам файловой системы NTFS.

Ход работы

Войдите в операционную систему под учётной записью «Администратор».

Для применения правил разграничения доступа необходимо воспользоваться вкладкой «Безопасность». Так как она по умолчанию отключена, её необходимо активировать. Для этого необходимо в разделе «Свойства папки» отключить опцию «Использовать простой общий доступ к файлам» (рис. 1).

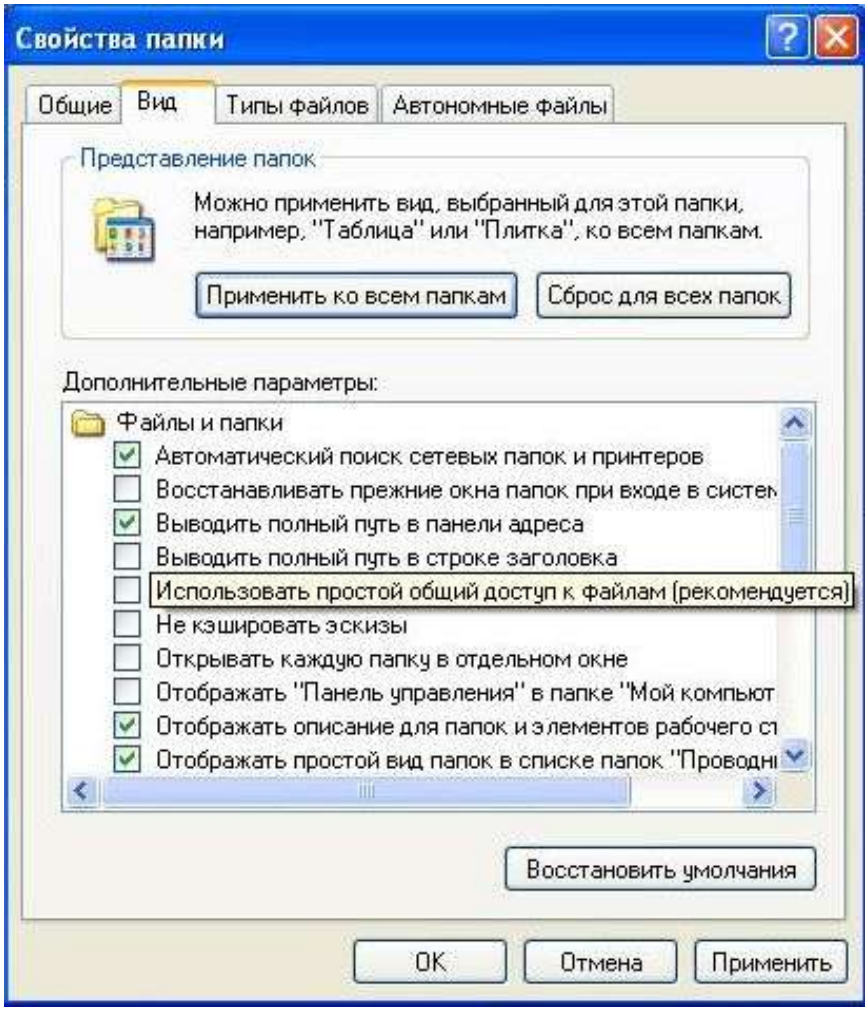


Рисунок 1 – Раздел «Свойства папки»

1. Основные права доступа к файловым объектам

В NTFS все разрешения сводятся к шести стандартным разрешениям (Полный доступ, Изменить, Чтение и выполнение, Список содержимого папки, Чтение, Запись). Данные разрешения могут предоставляться пользователю (или группе пользователей) на доступ к объектам – каталогам и файлам. Право «Полный доступ» не только включает в себя все остальные разрешения, но и позволяет управлять разграничением доступа к данному объекту.

Назначение прав доступа пользователей осуществляется для каждого объекта. Назначить или изменить права доступа можно в «Свойствах» выбранного каталога или файла во вкладке «Безопасность». Сначала необходимо выбрать пользователя (или группу), которому будут назначаться разрешения.

Откройте вкладку «Безопасность» в «Свойствах» каталога «D:\Список содержимого папки». Для изменения списка пользователей, имеющих право на доступ к объекту, нажмите на кнопку «Добавить» и выберите пользователя «user» (рис. 2).

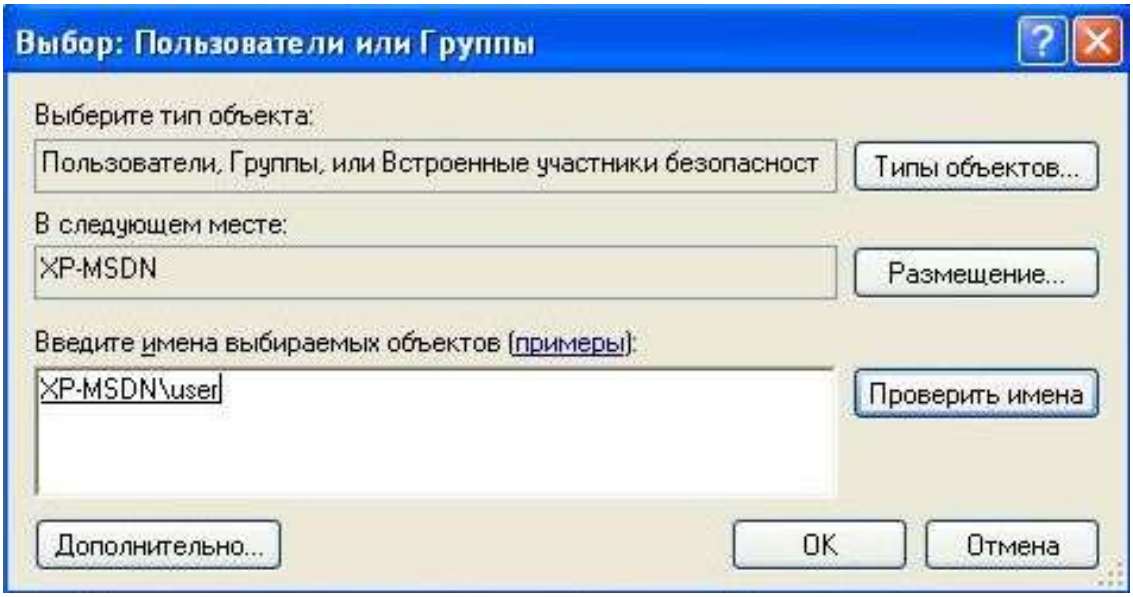


Рисунок 2 – Добавление нового пользователя

Установите пользователю «user» разрешение «Список содержимого папки» на доступ к текущему каталогу «D:\Список содержимого папки» (рис. 3).

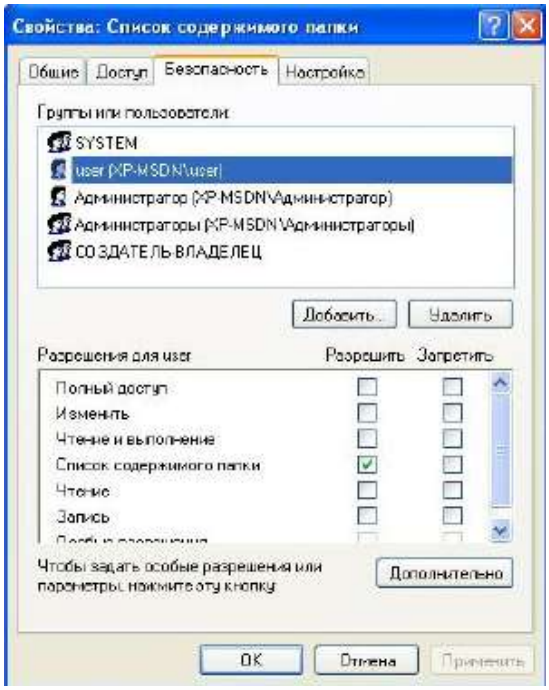


Рисунок 3 – Установка разрешения «Список содержимого папки»

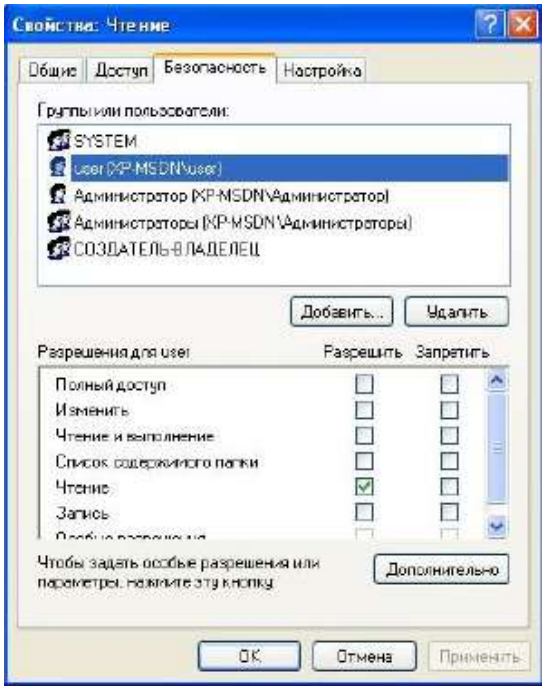


Рисунок 4 – Установка разрешения «Чтение»

Аналогично для пользователя «user» на каталоги «Чтение», «Чтение и выполнение», «Запись», «Изменение» и «Полный доступ» установите разрешения соответствующие названиям этих каталогов (рис. 4-8).

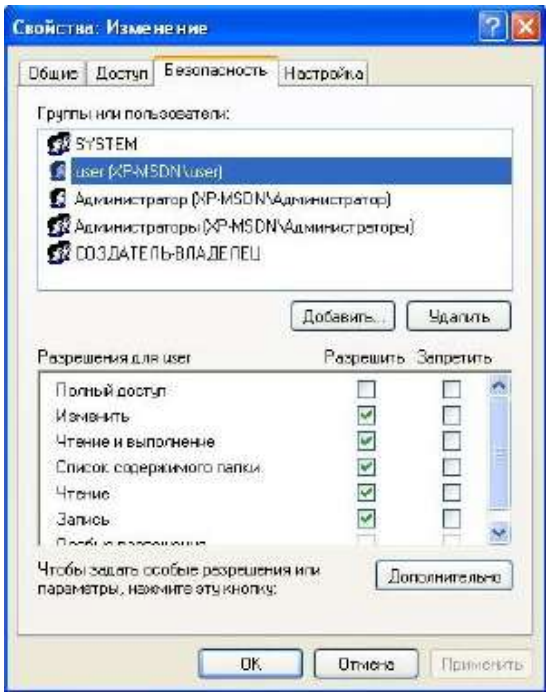


Рисунок 5 – Установка разрешения «Изменить»

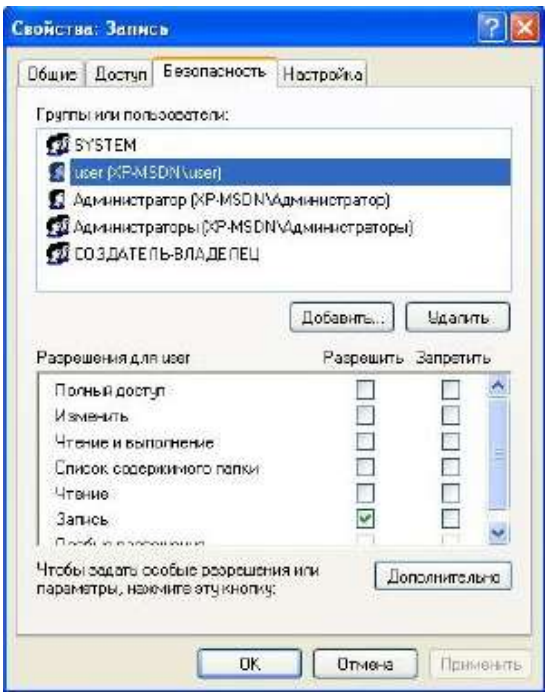


Рисунок 6 – Установка разрешения «Запись»

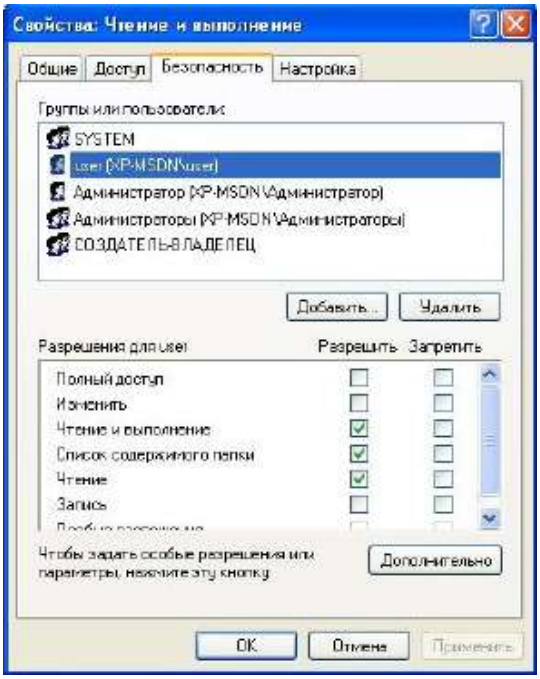


Рисунок 7 – Установка разрешения «Чтение и выполнение»

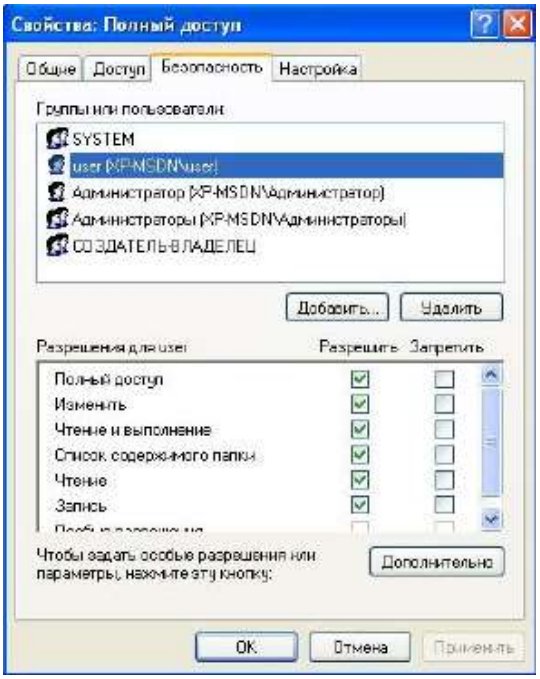


Рисунок 8 – Установка разрешения «Полный доступ»

Для проверки прав доступа, предоставленных пользователю при установке разрешений к заданным каталогам, войдите под учётной записью «user».

Разрешение «Список содержимого папки» предоставляет возможность просмотреть перечень объектов в данном каталоге. Войдите в соответствующий каталог и попытайтесь запустить исполняемый файл. Операционная система выдаст ошибку доступа к этому файлу (рис. 9). Попытайтесь открыть текстовый файл. Операционная система также выдаст ошибку доступа (рис. 10).

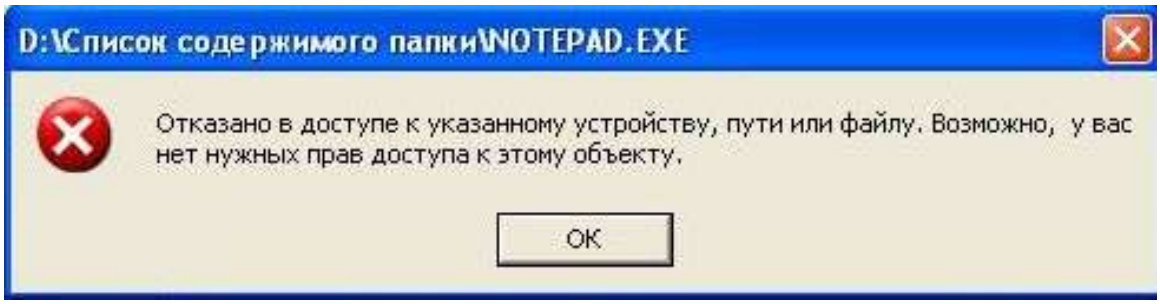


Рисунок 9 – Ошибка доступа к исполняемому файлу

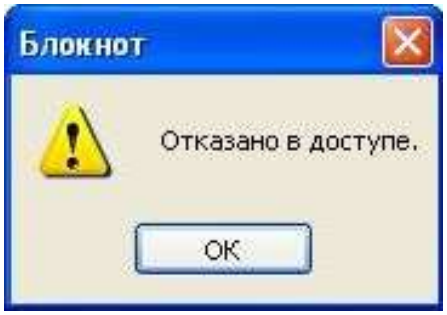


Рисунок 10 – Ошибка доступа к текстовому файлу

Разрешение «Чтение» предоставляет возможность открывать в данном каталоге все файлы, кроме исполняемых. Войдите в соответствующий каталог и откройте текстовый файл. Измените текст в открытом файле и попытайтесь сохранить его. Операционная система выдаст ошибку доступа на создание файла (рис. 11). Попытайтесь запустить исполняемый файл для проверки отказа в доступе.

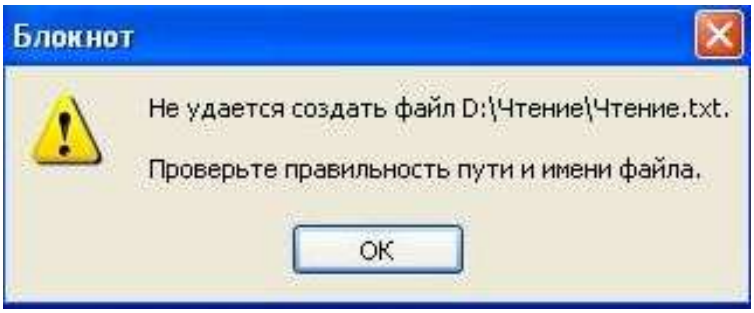


Рисунок 11 – Ошибка доступа на создание и сохранение измененённого текстового файла

Разрешение «Чтение и выполнение» предоставляет возможность открывать в данном каталоге все файлы. Войдите в соответствующий каталог и запустите исполняемый файл. Откройте текстовый файл, измените в нём текст и попытайтесь сохранить для проверки отказа в доступе на сохранение.

Разрешение «Запись» предоставляет возможность добавления файлов в данный каталог без права на доступ к вложенным в него объектам, в т.ч. на просмотр содержимого каталога. Попытайтесь войти в соответствующий каталог. Операционная система выдаст ошибку доступа к каталогу (рис. 12). Для проверки возможности добавления файла создайте файл с именем «Запись» (например, на «Рабочем столе») и попытайтесь перетащить его в каталог «Запись». Операционная система выдаст ошибку копирования, т.к. файл с таким именем в каталоге существует. Переименуйте файл и повторно попытайтесь его перетащить – копирование выполнится (кроме ого, наличие файла в каталоге можно проверить из под учётной записи «Администратор»).

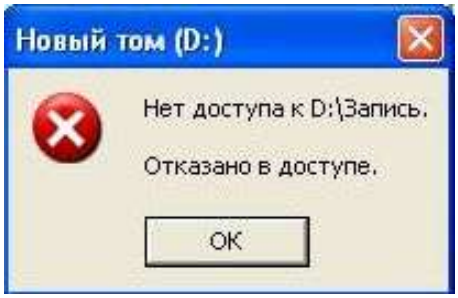


Рисунок 12 – Ошибка доступа к каталогу

Разрешение «Изменить» предоставляет возможность открывать и создавать (изменять) файлы в данном каталоге. Войдите в соответствующий каталог и запустите исполняемый файл. Откройте текстовый файл, измените в нём текст и сохраните его, создайте новый файл в каталоге. Откройте вкладку «Безопасность» у каталога «Изменение» или у любого вложенного файла и попытайтесь изменить права доступа к нему. Изменить права доступа нельзя (параметры включения разрешений неактивны), т.к. разрешение «Изменить» не включает возможность управления правами доступа (рис. 13).

Разрешение «Полный доступ» предоставляет все возможности для работы с каталогом и вложенными файлами, включая изменение разрешений. Для проверки откройте вкладку «Безопасность» у каталога «Полный доступ» или у любого вложенного файла и измените права доступа к нему.

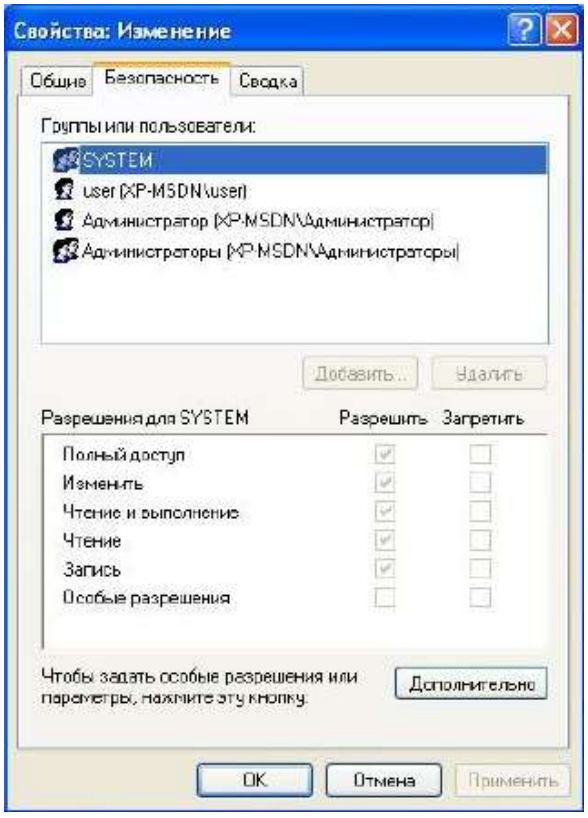


Рисунок 13 – Невозможность изменения разрешений на доступ

2. Элементы разрешений на доступ

Каждое стандартное разрешение состоит из нескольких элементов. Элементы разрешений позволяют более гибко настраивать права доступа пользователей.

Войдите под учётной записью «Администратор».

Просмотреть элементы разрешений на доступ можно, нажав на кнопку «Дополнительно» во вкладке «Безопасность» и выбрав любой элемент разрешений (рис. 14). Наборы элементов, включаемых в стандартные разрешения, приведены на рис. 15-20.

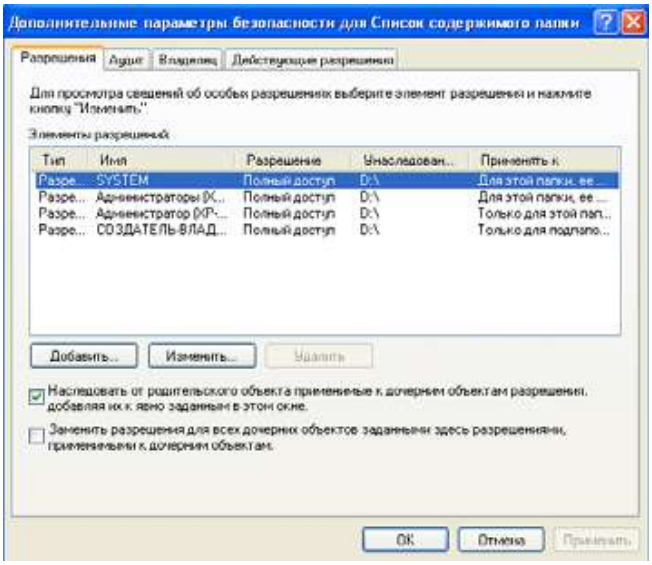


Рисунок 14 – Дополнительные параметры безопасности

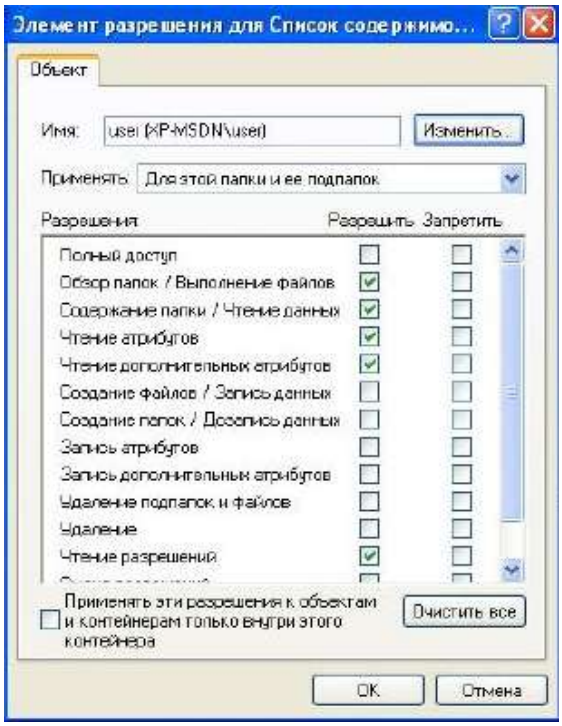


Рисунок 15 – Элементы разрешений для «Списка содержимого папки»

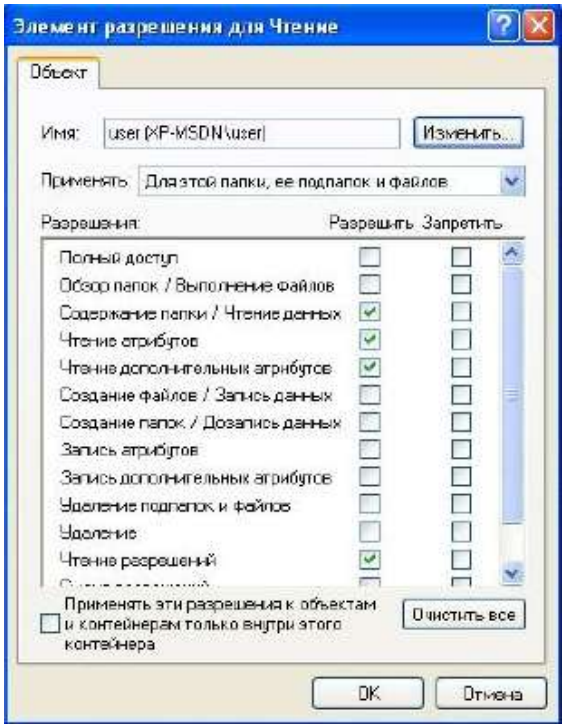


Рисунок 16 – Элементы разрешений для «Чтения»

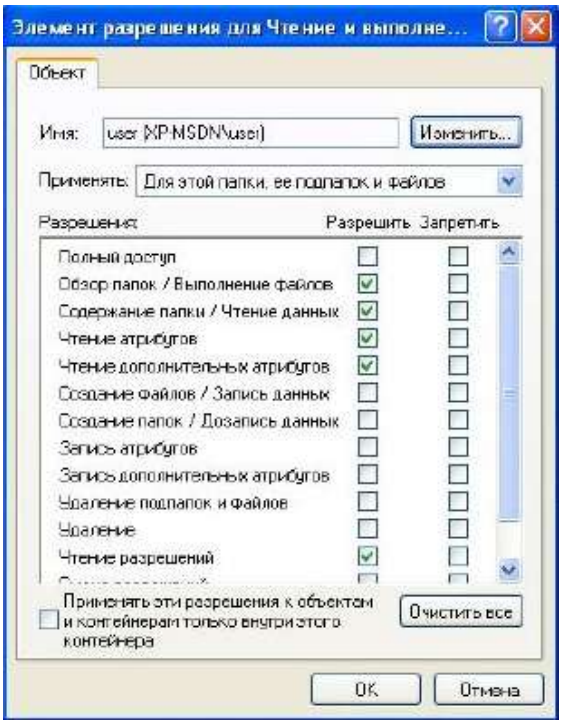


Рисунок 17 – Элементы разрешений для «Чтения и выполнения»

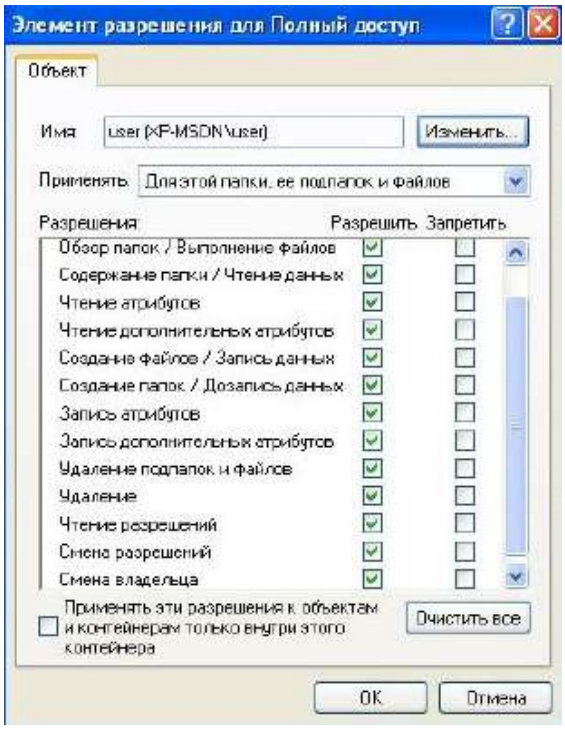


Рисунок 18 – Элементы разрешений для «Полного доступа»

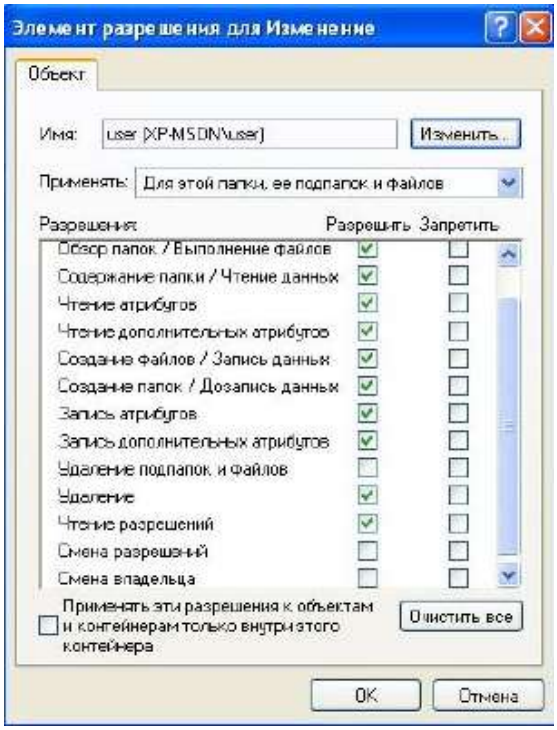


Рисунок 19 – Элементы разрешений для «Изменить»

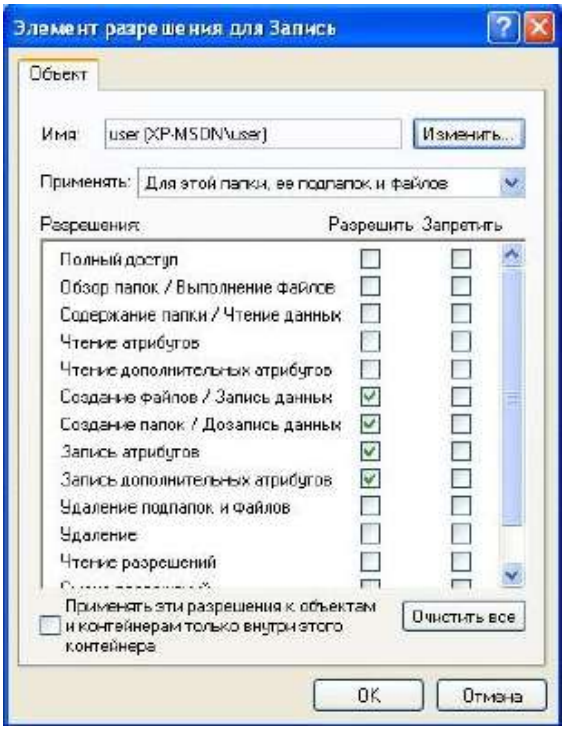


Рисунок 20 – Элементы разрешений для «Записи»

Использование возможностей элементов разрешений наиболее оправдано при разграничении доступа на удаление файла или каталога. Через элементы разрешений запретите пользователю «user»

удаление каталога «Изменение», а также разрешите запись атрибутов на каталог «Чтение» (рис. 21-22).

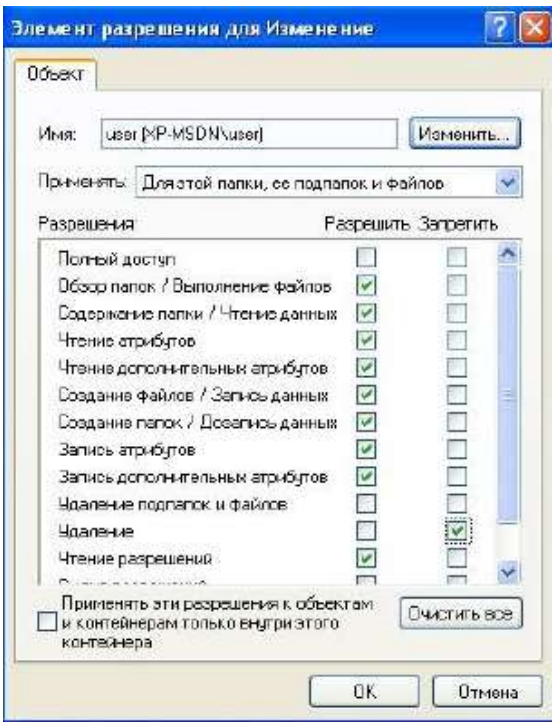


Рисунок 21 – Запрет удаления

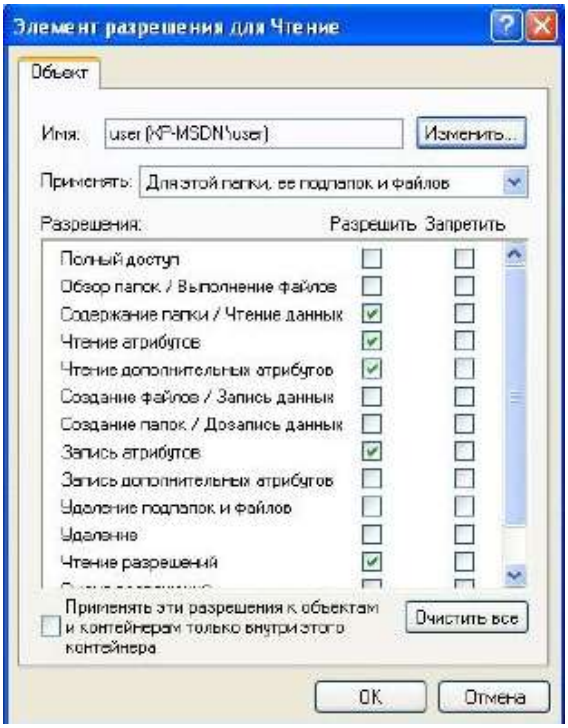


Рисунок 22 – Разрешение записи атрибутов

Для проверки установленных прав доступа войдите под учётной записью «user». Попытайтесь удалить файл из каталога «Изменение». Операционная система выдаст ошибку доступа на удаление файла (рис. 23).

Измените атрибуты файла в каталоге «Чтение» (например, атрибут «Скрытый» в свойствах файла). Примените сделанные изменения. Измените дополнительные атрибуты текстового файла в каталоге «Чтение» (например, автора документа во вкладке «Сводка» свойств файла). Попытайтесь применить сделанные изменения. Операционная система выдаст ошибку сохранения дополнительных атрибутов (рис. 24).

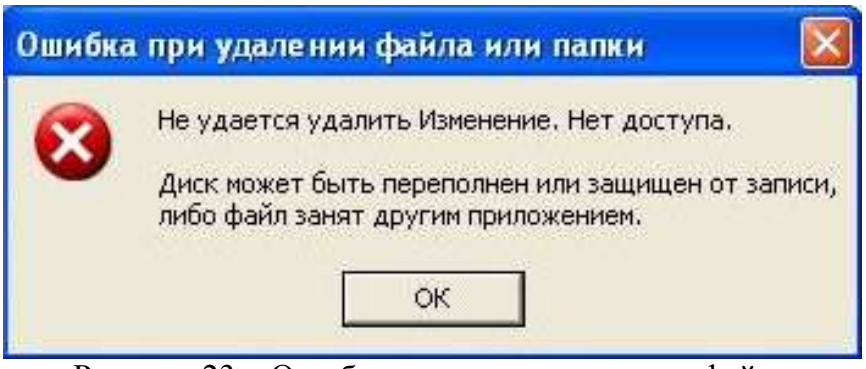


Рисунок 23 – Ошибка доступа на удаление файла

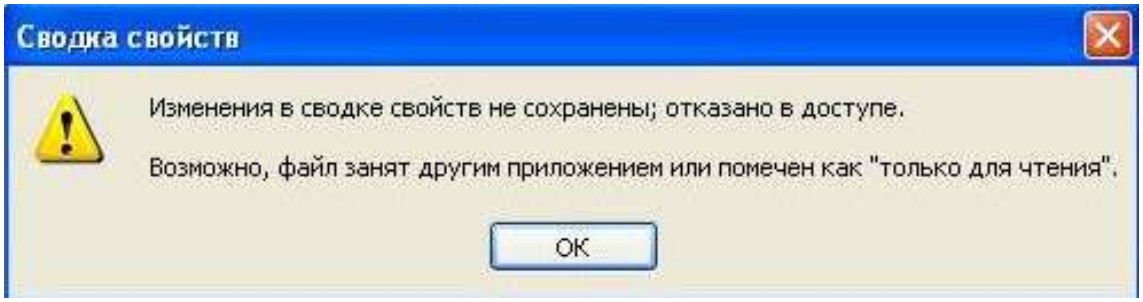


Рисунок 24 – Ошибка доступа на изменение дополнительных атрибутов

3. «Владелец» файла

В файловой системе NTFS у каждого объекта есть владелец. Владелец управляет назначением разрешений на доступ к объекту независимо от установленных разрешений.

Создайте под учётной записью «user» в каталоге «Изменение» новый каталог (например, «test») и в нём текстовый файл (например, «test.txt»). Скопируйте в созданный текстовый файл информацию из файла «Изменение». Откройте вкладку «Владелец» файла «test.txt». В ней указывается текущий владелец объекта (рис. 25). Предоставьте полный доступ к созданному каталогу пользователю «user1» (рис. 26).

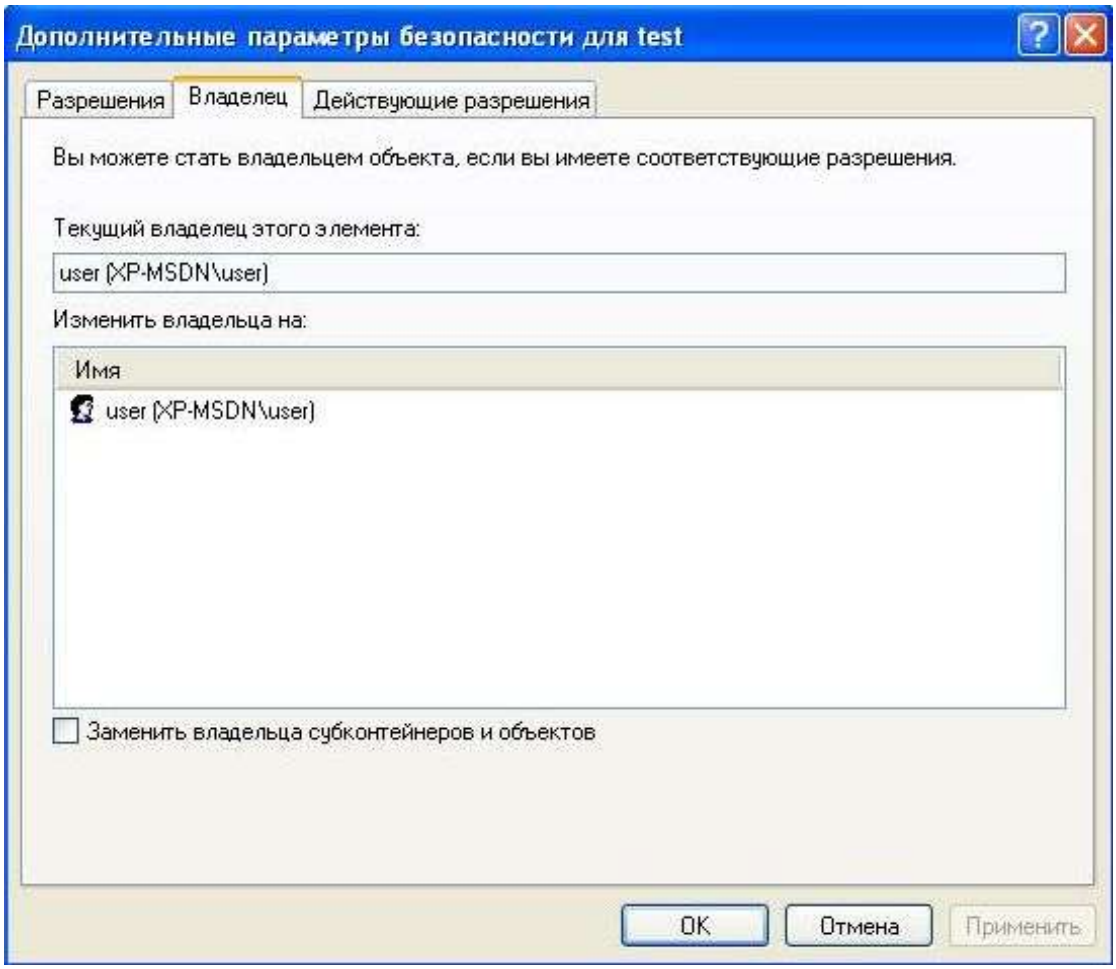


Рисунок 25 – Вкладка «Владелец»

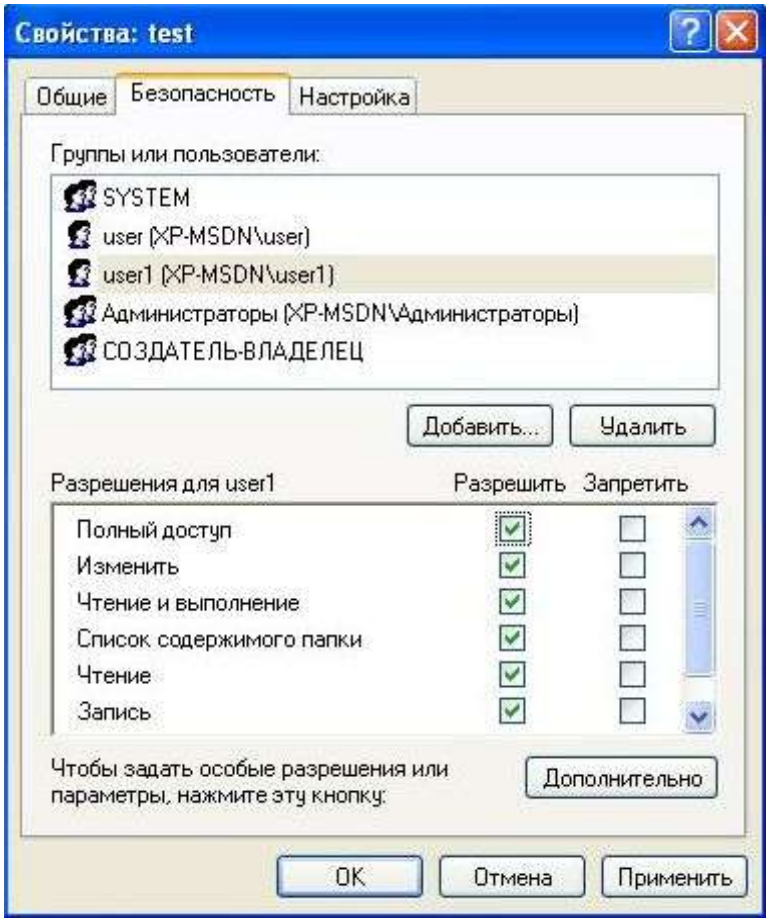


Рисунок 26 – Предоставление прав пользователю «user1»

Войдите под учётной записью «user1».

Попытайтесь перейти в каталог «D:\Изменение\test» при помощи иерархического представления каталогов в «Проводнике». Переход невозможен, потому что у пользователя «user1» нет доступа к промежуточным каталогам. Попытайтесь перейти в тот же каталог, указав его полный путь в адресной строке «Проводника» (рис. 27). Откройте файл «test.txt». Таким образом, пользователь «user» может несанкционированно предоставить доступ пользователю «user1» к конфиденциальной информации.

Наличие полного доступа у пользователя «user1» к каталогу «test» позволяет ему изменять разрешения. Запретите доступ пользователя «Администратор» к файлу «test.txt» (рис. 28).

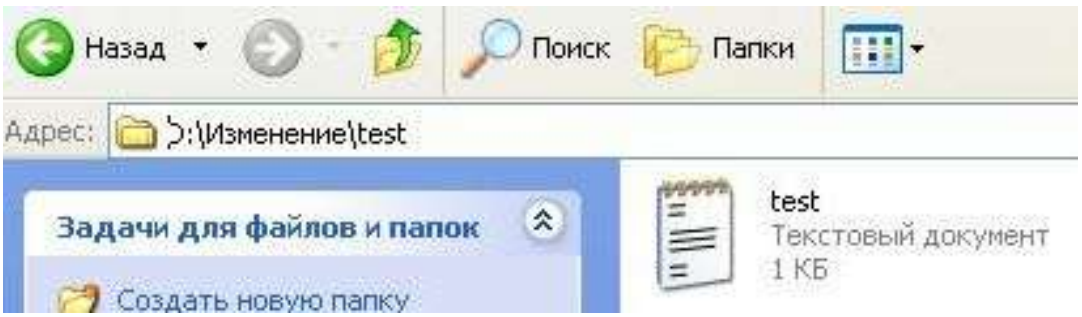


Рисунок 27 – Доступ к каталогу через адресную строку

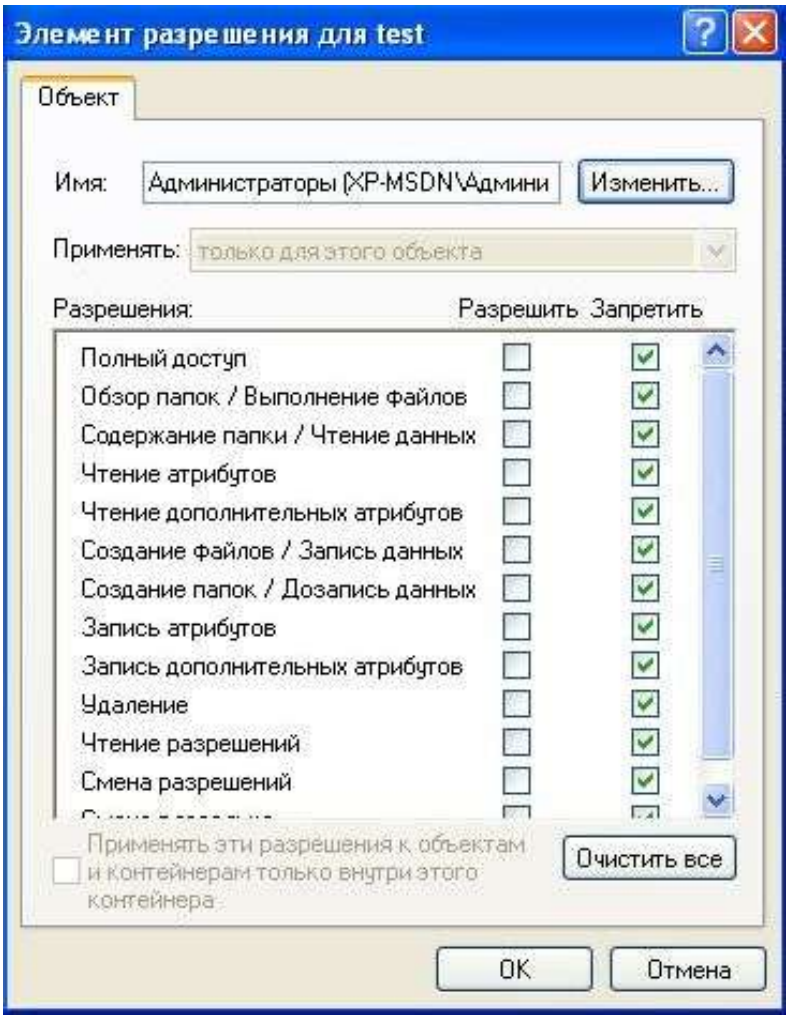


Рисунок 28 – Запрет доступа к файлу

Дополнительно разрешение «Полный доступ» даёт возможность смены владельца файла. Смените владельца файла «test.txt» на пользователя «user1» (рис. 29).

Попытайтесь изменить владельца другого файла/каталога, к которому нет полного доступа (например, диска D:\). Операционная система выдаст ошибку изменения владельца (рис. 30).

Войдите под учётной записью «Администратор».

Попытайтесь получить доступ к файлу «test.txt». Несмотря на то, что «Администратор» не может получить доступ к файлу, он может сменить владельца. Измените владельца файла на группу «Администраторы». Закройте свойства файла. При повторном входе в свойства файла у пользователя появляется возможность устанавливать права доступа (рис.31). Пользователи и группы, имеющие право менять владельца, не обладая полным доступом к нему, перечисляются в групповых политиках в параметре «Овладение файлами и другими объектами» (рис.32).

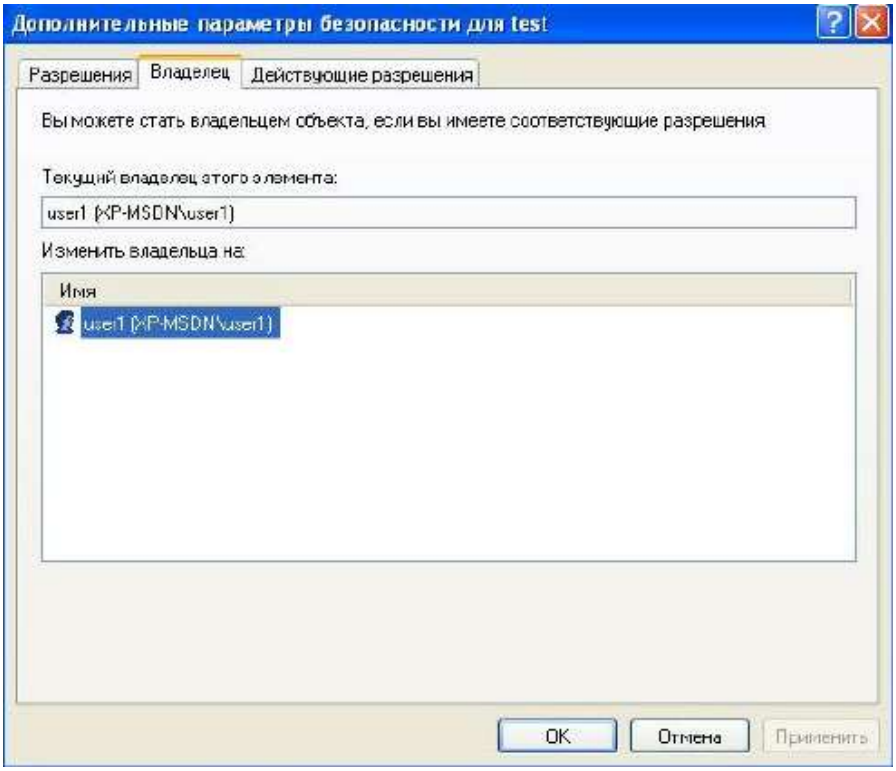


Рисунок 29 – Смена владельца файла

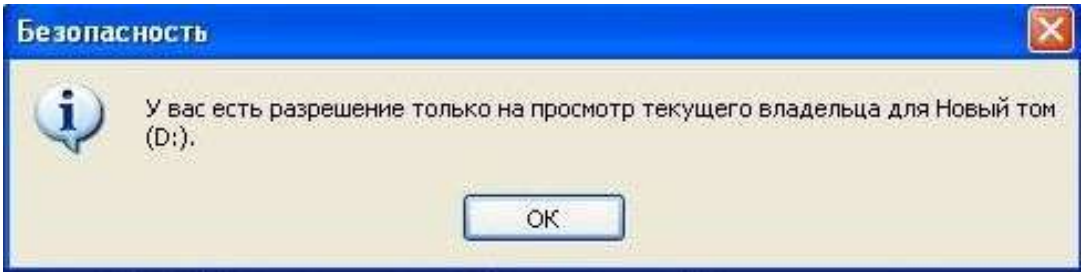


Рисунок 30 – Ошибка смены владельца файла

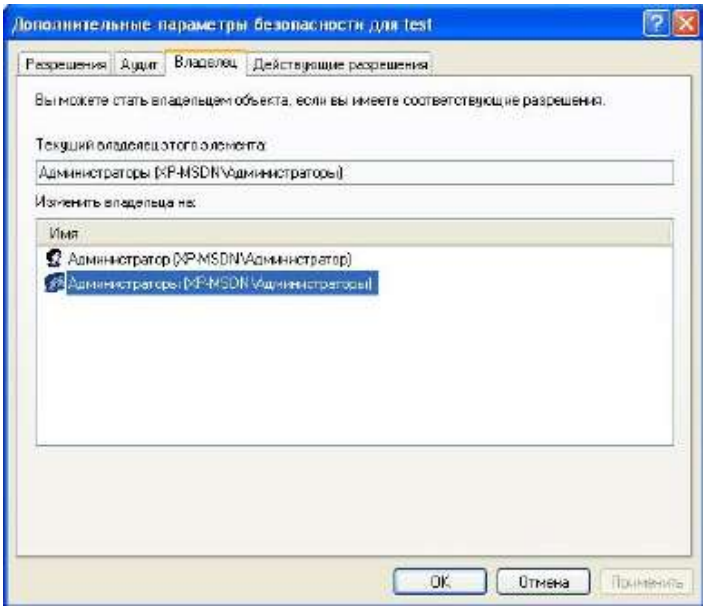


Рисунок 31 – Установка группы «Администраторы» в качестве владельца файла

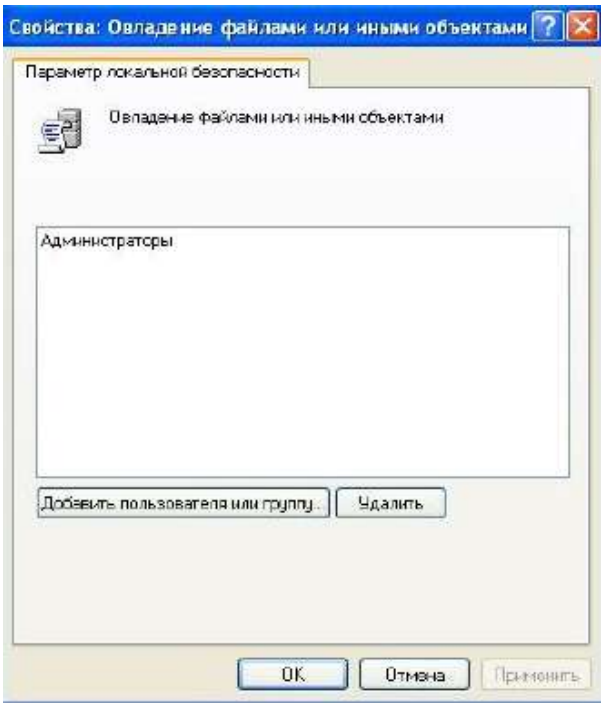


Рисунок 32 – Параметр «Овладение файлами и другими объектами»

4. Наследование прав доступа

NTFS поддерживает наследование разрешений, которое означает, что по умолчанию разрешения каталога распространяются на все его файлы и подкаталоги. Любые изменения разрешений на доступ к родительскому каталогу будут отражаться на его вложенных объектах.

Изменить унаследованные разрешения можно и со стороны вложенного объекта. Откройте вкладку «Разрешения» в дополнительных параметрах безопасности каталога «D:\Чтение\Чтение1» и отключите наследование (параметр «Наследовать от родительского объекта применимые к дочерним объектам разрешения, добавляя их к явно заданным в этом окне»). При отключении наследования скопируйте текущие разрешения (рис. 33).

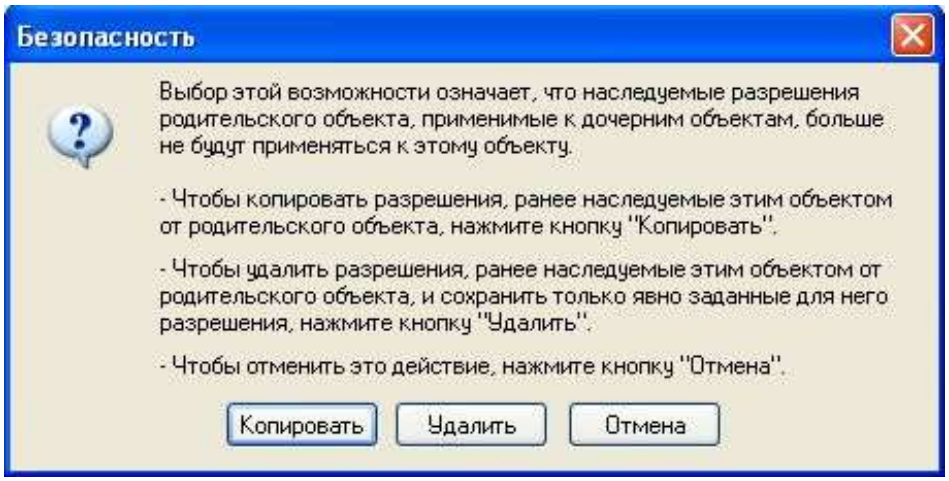


Рисунок 33 – Выбор действия при отключении наследования

После отключения наследования каталогом разрешений от родительского в разделе «Унаследовано» у каждого элемента устанавливается значение «не унаследовано» (рис. 34). Описание изменений в разделе «Унаследовано».

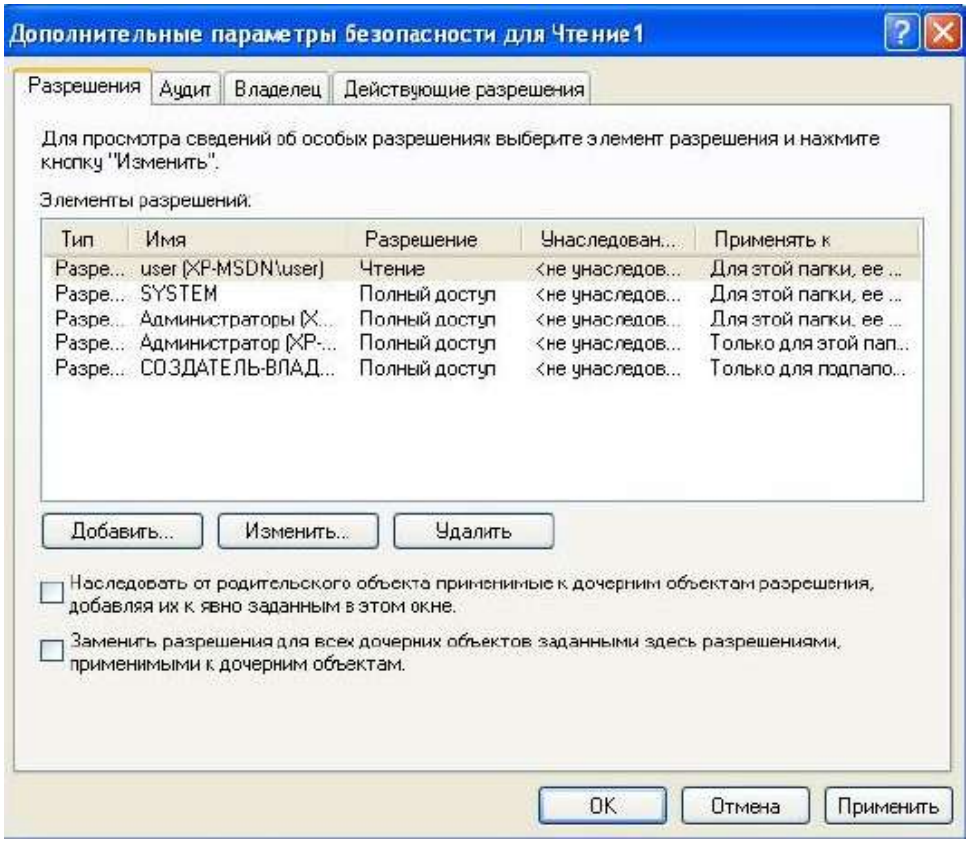


Рисунок 34 – Элементы разрешений при отключенном наследовании

Изменить действующие разрешения у вложенных объектов можно при помощи параметра «Заменить разрешения для всех дочерних объектов заданными здесь разрешениями, применимыми к дочерним объектам». Удалите учётную запись «user» из числа санкционированных пользователей каталога «Чтение1». В родительском для него каталоге «Чтение» установите изменение прав дочерних объектов (рис. 35). Проверьте восстановление учётной записи «user» в перечне санкционированных пользователей каталога «Чтение1».

При установке прав доступа на элементы можно выставлять не только разрешения, но и запреты. Запретите группе «Пользователи», членом которой является «user» (учётной записи «user» чтение разрешено) чтение файла «Чтение» (рис. 36). Войдите под учётной записью «user». Попытайтесь открыть файл «Чтение». Невозможность открыть файл обусловлена тем, что запреты приоритетнее разрешений.

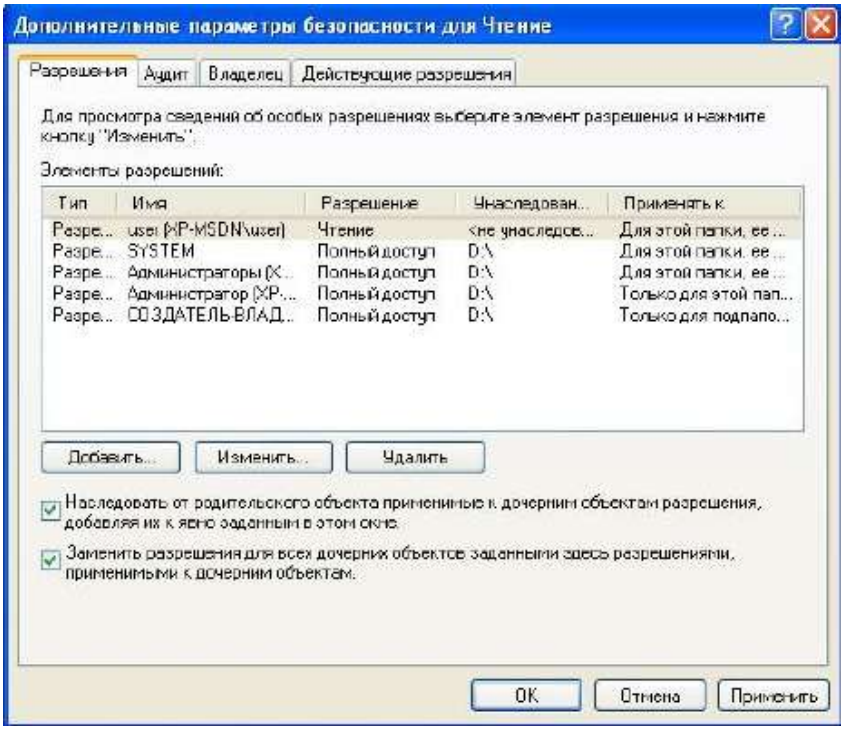


Рисунок 35 – Включение принудительного наследования

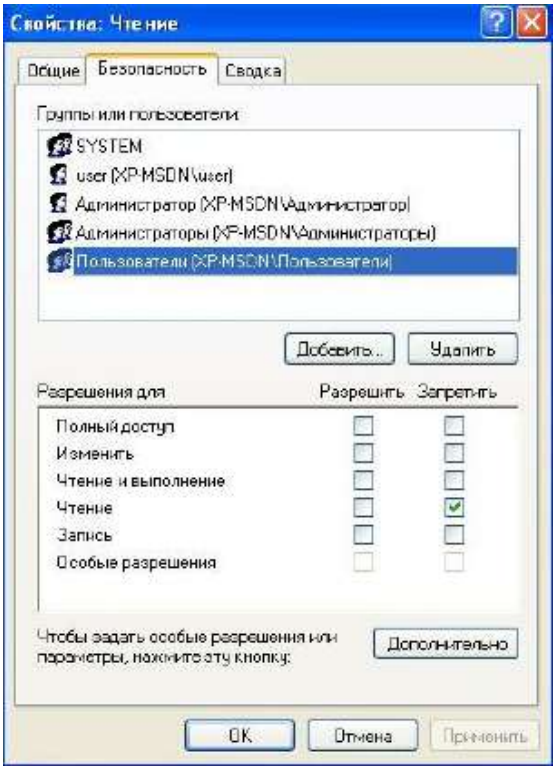


Рисунок 36 – Установка запрета на чтение

Действующие разрешения можно просмотреть в одноимённой вкладке Дополнительных параметров безопасности, выбрав интересующего пользователя или группу. Войдите под учётной записью «Администратор». Просмотрите действующие разрешения на файл «Чтение» для пользователя «user» (рис. 37). Удалите группу

«Пользователи» из перечня разрешений. Повторно просмотрите действующие разрешения пользователя «user» (рис. 38). Таким образом, разрешения предоставленные пользователю и группе, в которую он входит, суммируются. И после удаления элемента, запрещающего группе «Пользователи» чтение, у пользователя «user» остались только свои права.

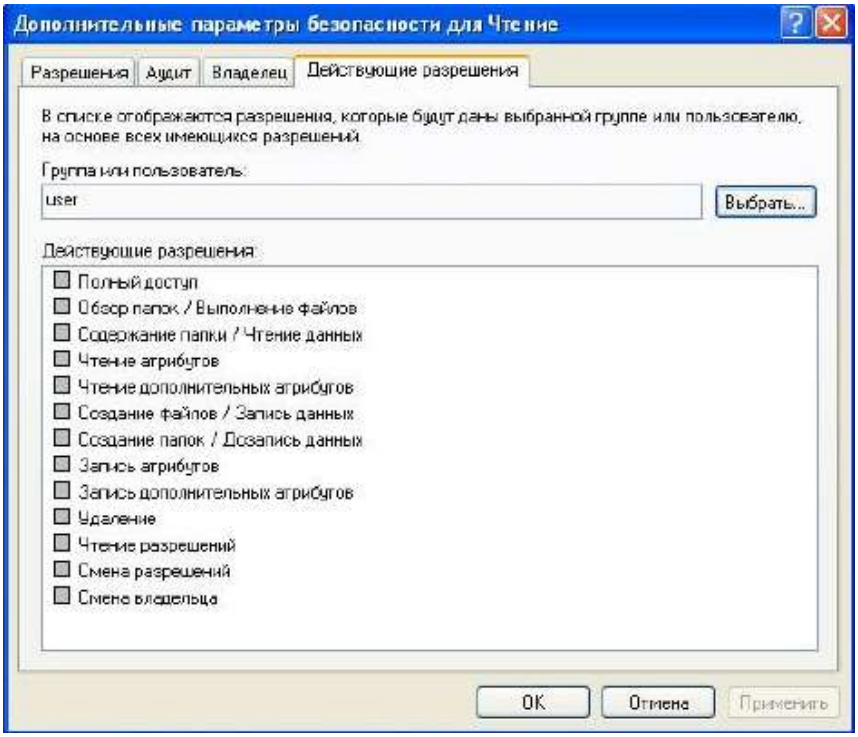


Рисунок 37 –Действующие разрешения пользователя

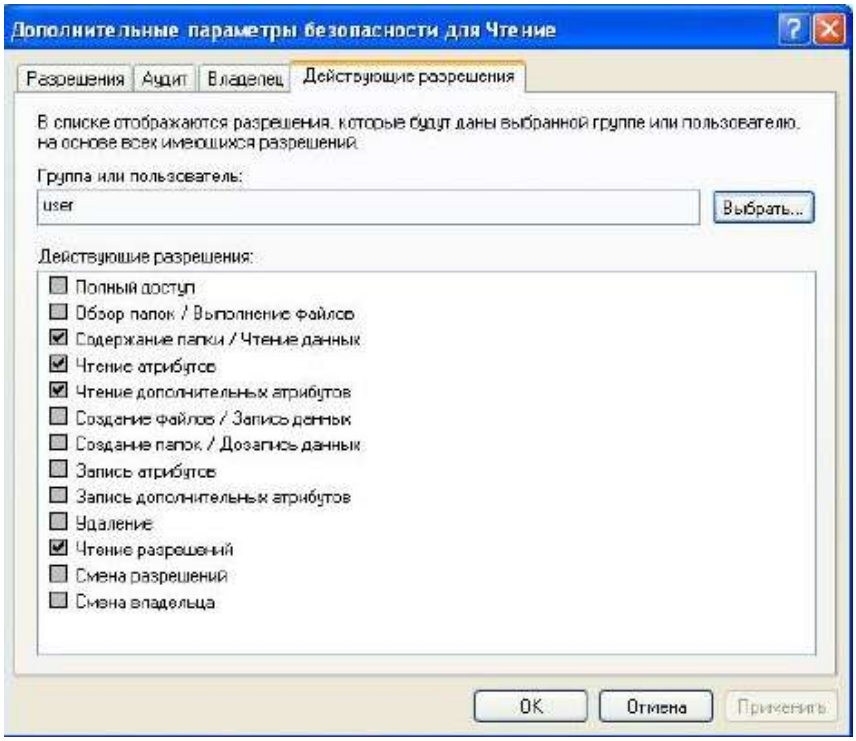


Рисунок 38 –Действующие разрешения пользователя после изменения разрешений

При выставлении разрешений существует возможность указывать глубину наследования и типы объектов. Можно распространить установленные разрешения на данный каталог, только на вложенные объекты или на каталог и все его вложенные объекты, а также можно указать на вложенные каталоги или файлы будут распространяться разрешения.

Разрешите на каталог «Чтение» пользователю «user» создание папок только для подпапок, вложенных в этот каталог (рис. 39), т.е. в каталогах «Чтение» и «Чтение2» подпапки создавать будет запрещено, а в каталоге «Чтение1» (непосредственно вложенном в «Чтение») – разрешено. Войдите под учётной записью «user». Проверьте возможность создания папок во всех указанных каталогах.

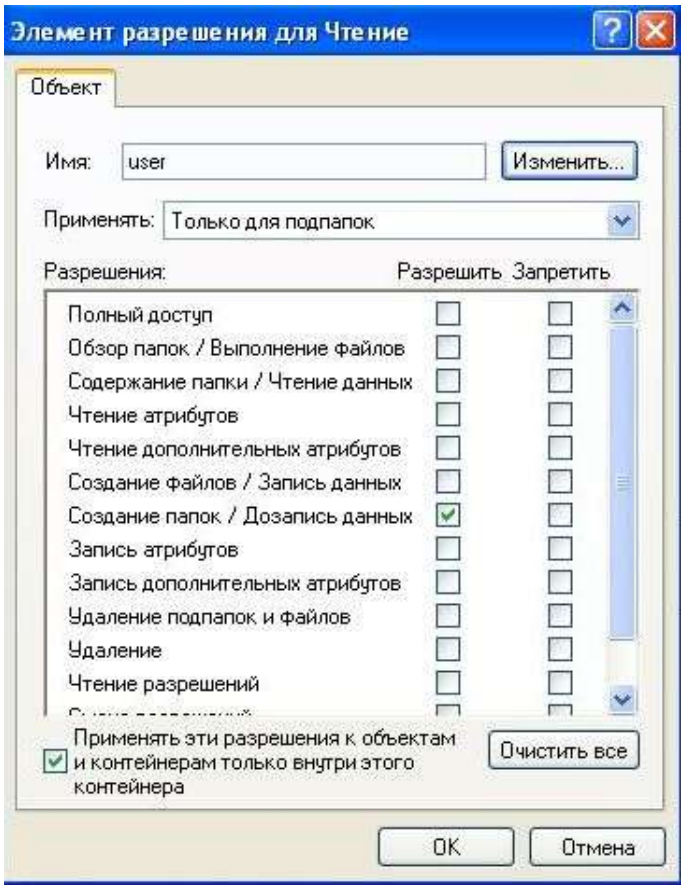


Рисунок 39 – Выбор глубины и типа объектов наследования

5. Разграничение доступа к принтерам

Под учётной записью «user» отправьте текстовый файл на печать при помощи принтера doPDF.

В разделе «Принтеры и факсы» меню «Пуск» попытайтесь изменить настройки принтера (рис. 40). Невозможность изменения настроек объясняется наличием у группы «Все» только права на «Печать» (отсутствием права на «Управление принтерами») (рис. 41).

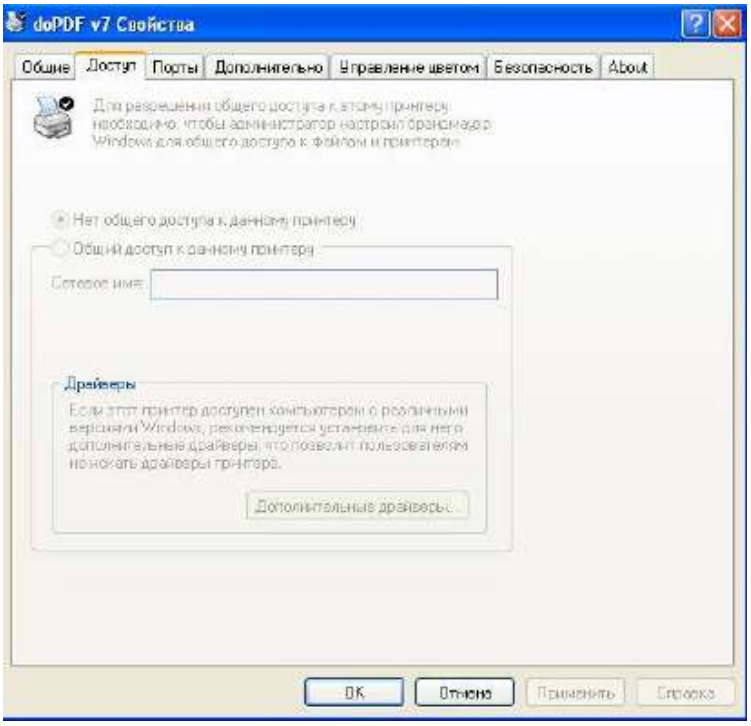


Рисунок 40 – Свойства принтера

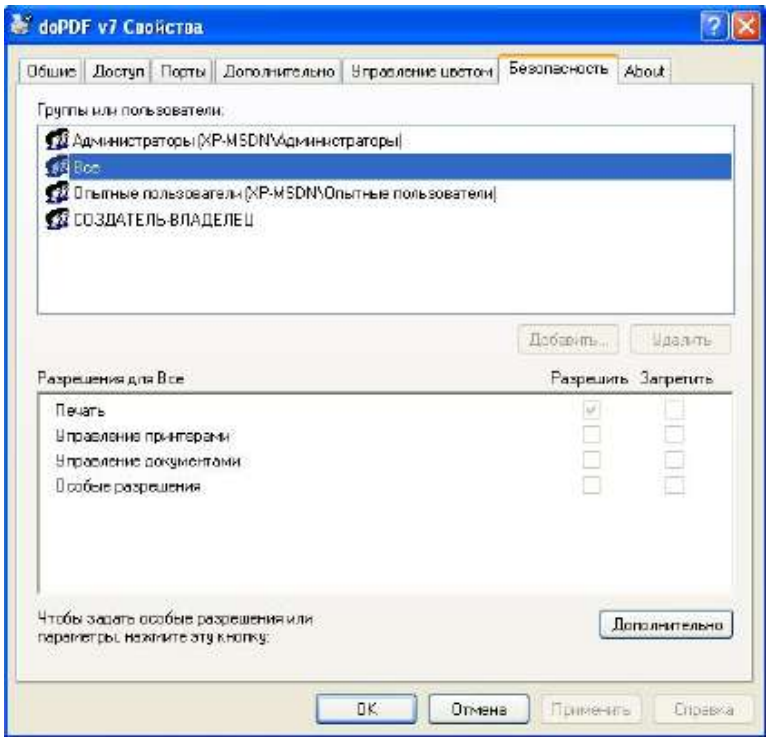


Рисунок 41 – Разграничение доступа к принтеру

Войдите под учётной записью «Администратор». Удалите из списка доступа к принтеру doPDF группу «Все».

Войдите под учётной записью «user».

Попытайтесь напечатать текстовый файл. Откройте раздел «Принтеры и факсы», в котором doPDF отсутствует, т.к. «user не» входит в список пользователей, имеющих право на работу с принтером.

Задание

Создайте каталоги «Общедоступно» и «Конфиденциально». В каждом из этих каталогов скопируйте исполняемый и текстовый файлы. Разграничьте доступ к принтеру, а также созданным каталогам и файлам в соответствии со своим вариантом.

Вариант 1

Субъекты	Объекты		
	Общедоступно	Конфиденциально	Принтер
Администратор	Полный доступ	Чтение	Полный доступ
user	Чтение	Изменить, кроме удаления	Печать Управление документами
user1	Изменить	Нет доступа	Печать

Вариант 2

Субъекты	Объекты		
	Общедоступно	Конфиденциально	Принтер
Администратор	Полный доступ	Чтение и выполнение	Полный доступ
user	Изменить	Чтение	Печать
user1	Чтение и выполнение	Изменить	Печать Управление документами

Вариант 3

Субъекты	Объекты		
	Общедоступно	Конфиденциально	Текстовый файл в «Конфиденциально»
Администратор	Полный доступ	Список содержимого	Нет доступа
user	Чтение	Изменить, кроме удаления	Изменить
user1	Изменить	Нет доступа	Нет доступа

Вариант 4

Субъекты	Объекты		
	Общедоступно	Конфиден-циально	Текстовый файл в «Конфиденциально»
Адми-нистратор	Изменить	Чтение и выполнение	Нет доступа
user	Чтение	Изменить	Запрет удаления
user1	Полный доступ, кроме смены владельца	Запись	Нет доступа

Вариант 5

Субъекты	Объекты		
	Общедоступно	Конфиден-циально	Исполняемый файл в «Конфиденциально»
Адми-нистратор	Полный доступ	Список содержимого	Выполнение
user	Чтение	Чтение и удаление	Выполнение, запрет удаления
user1	Изменить, кроме удаления	Запись	Нет доступа

Вариант 6

Субъекты	Объекты		
	Общедоступно	Конфиден-циально	Исполняемый файл в «Конфиденциально»
Адми-нистратор	Полный доступ	Чтение	Изменить
user	Чтение и удаление	Список содержимого	Выполнение
user1	Изменить	Нет доступа	Нет доступа

Вариант 7

Субъекты	Объекты		
	Общедоступно	Конфиден-циально	Текстовый файл в «Общедоступно»
Адми-нистратор	Список содержимого	Полный доступ	Нет доступа

user	Изменить, кроме удаления	Чтение	Изменить
user1	Нет доступа	Изменить	Нет доступа

Вариант 8

Субъекты	Объекты		
	Общедоступно	Конфиден-циально	Текстовый файл в «Конфиденциально»
Админи-стратор	Чтение и выполнение	Изменить	Нет доступа
user	Изменить	Чтение	Изменить, запрет изменения дополнит. атрибутов
user1	Запись	Изменить, кроме удаления	Нет доступа

Вариант 9

Субъекты	Объекты		
	Общедоступно	Конфиден-циально	Исполняемый файл в «Конфиденциально»
Админи-стратор	Список содержимого	Полный доступ	Выполнение
user	Чтение и удаление	Чтение	Выполнение, запрет удаления
user1	Запись	Полный доступ	Нет доступа

Вариант 10

Субъекты	Объекты		
	Общедоступно	Конфиден-циально	Исполняемый файл в «Конфиденциально»
Админи-стратор	Чтение	Полный доступ	Изменить
user	Список содержимого	Чтение и удаление	Выполнение
user1	Нет доступа	Изменить	Нет доступа

Контрольные вопросы

1. Охарактеризуйте дискреционную модель управления доступом.
2. Перечислите стандартные права доступа к файловым объектам, существующие в файловой системе NTFS.
3. Объясните принцип работы разрешения «Запись».
4. Перечислите элементы разрешений.
5. Кто может стать владельцем объекта?
6. Раскройте понятие наследования разрешений.
7. Как отключить наследование разрешений?
8. Как реализовать принудительное наследование вложенными объектами установленных разрешений?
9. Перечислите приоритеты применения разрешений при определении действующих разрешений на доступ к файловым объектам.
10. Перечислите стандартные права доступа к принтерам, существующие в файловой системе NTFS.

Лабораторная работа № 3
Разграничение доступа к запуску программного обеспечения

Целью данной работы является ознакомление и практическое применение встроенных средств ограничения использования программ в ОС Windows XP Professional.

Политики ограниченного использования программ позволяют осуществлять идентификацию программ, запускаемых в ОС семейства Windows и управлять возможностью их выполнения на локальном компьютере.

Политики ограниченного использования программ (ПОИП) – это вид политик безопасности, который позволяет администраторам разрешить или запретить использовать программные приложения. Применение основано на использовании алгоритма хеширования файла, связи путей файлов с программным обеспечением, сертификата издателя программного обеспечения или зоны Интернета, в которой работает программное обеспечение.

Ход работы:

1. Войдите в ОС под учетной записью администратора и перейдите по следующему пути: «Панель управления - Администрирование - Локальная политика безопасности», далее в дереве консоли раскройте узел «Политики ограниченного использования программ» (рис. 1). Также доступ к политикам ограниченного использования программ (далее ПОИП) можно получить через добавление оснастки «Локальные параметры безопасности» в консоль управления. Через контекстное меню создайте новую политику.

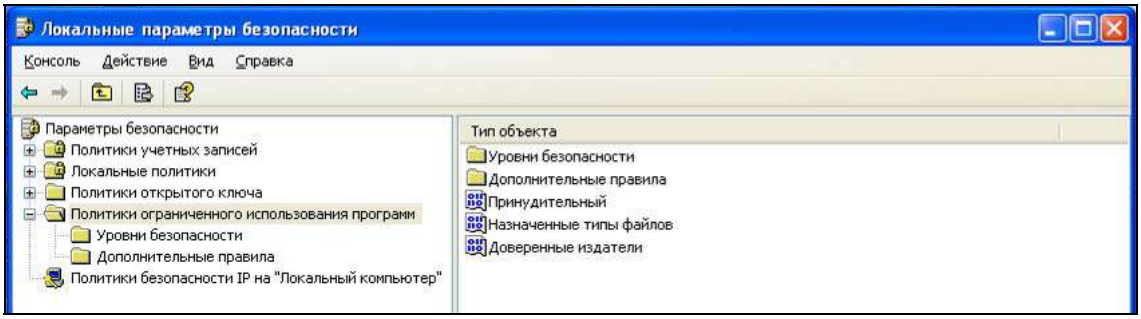


Рисунок 1 - Локальные параметры безопасности

2. Раскройте объект «Уровни безопасности» (рис. 2) в который включены два уровня: «Не разрешено», означающее запрет на запуск любого ПО, кроме разрешённого в ПОИП и «Неограниченный», означающий возможность работы с ПО в соответствии с правами пользователя. Уровень, используемый по умолчанию, обозначается «✔», чтобы его изменить дважды кликните на уровень безопасности и выберите пункт «По умолчанию». Установите уровень «Неограниченный», в качестве уровня безопасности по умолчанию.

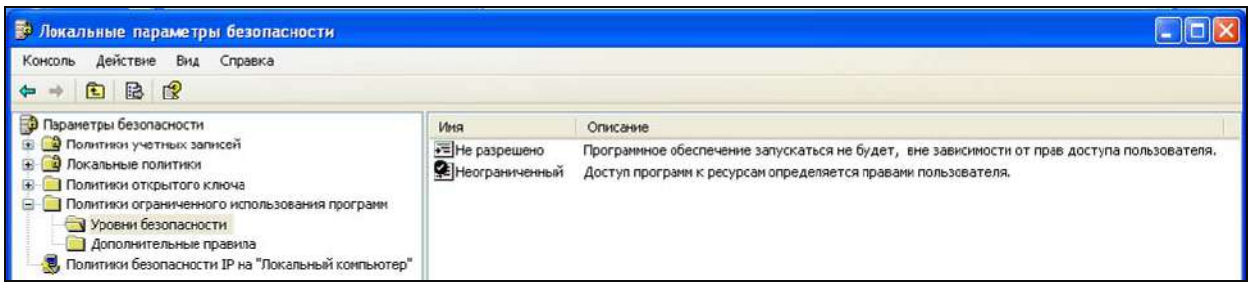


Рисунок 2 - Выбор уровня безопасности

3. Чтобы применить ПОИП к локальным администраторам, дважды кликните тип объекта «Принудительный» и выберите «Для всех пользователей» (рис. 3). Здесь же настраивается возможность исключать применение ПОИП к библиотекам программ, таких как DLL, которые могут использоваться другими разрешенными программами. Установите применение ПОИП ко всем пользователям и файлам.

4. В пункте «Назначенные типы файлов» раздела «Политики ограниченного использования программ» уже имеется список назначенных типов файлов, используемый для всех правил. Для того, чтобы определить с какими типами файлов будет работать ПОИП выберите пункт «Назначенные типы файлов», в появившемся окне (рис. 4) в поле «Расширение:» введите требуемое расширение, например, «exe». Таким образом, добавляются новые типы файлов, которые учитываются в правиле для пути.

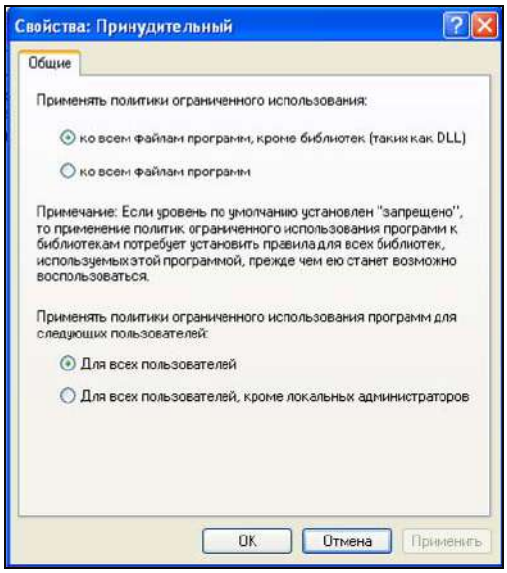


Рисунок 3 - Настройка дополнительных параметров

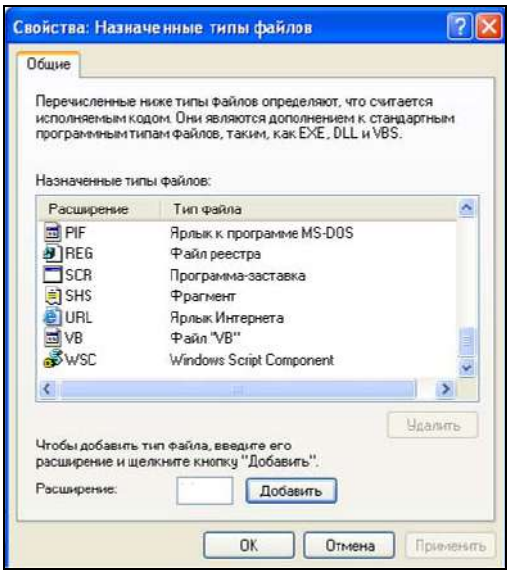


Рисунок 4 - Список файловых типов ПОИП

5. Перейдите в пункт «Дополнительные правила» (рис. 5) в нем уже имеются четыре правила пути. Они обеспечивают запуск ОС при выбранном по умолчанию уровне безопасности «Не разрешено». В меню выберите «Действие», далее «Создать правило для хеша…», в появившемся окне (рис. 6) при помощи кнопки «обзор» укажите файл, работу с которым вы хотите запретить, например, «utorrent.exe», информация о нем заполнится

автоматически. Также можно вносить само значение хеша, рассчитанное другим пользователем, например, хеш вируса.

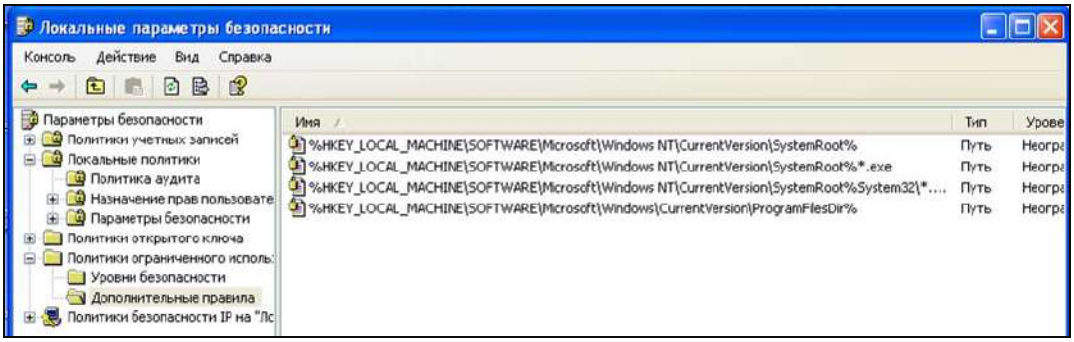


Рисунок 5 - Вкладка «Дополнительные правила»

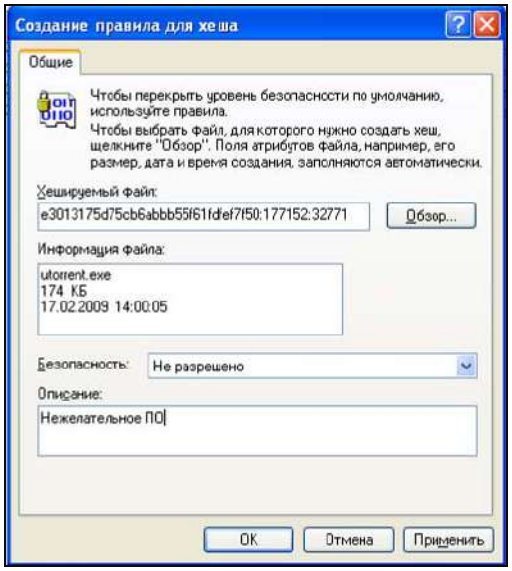


Рисунок 6 - Создание правила для хеша

Запустите файл «utorrent.exe», после чего отобразится сообщение (рис. 7), информирующее пользователя о запрете запуска файла. Необходимо помнить, что любые изменения в файле приводят к изменению хеша.

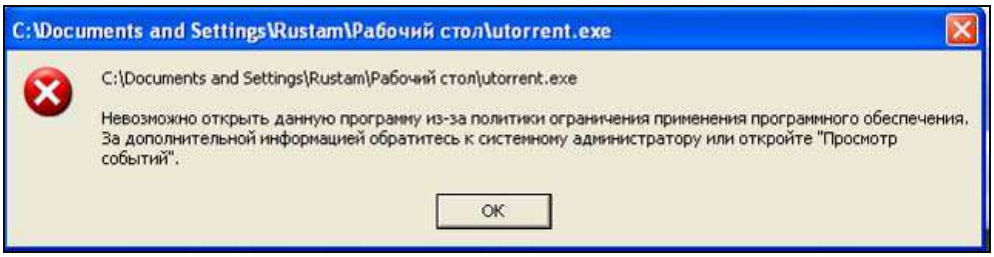


Рисунок 7 - Сообщение о запрете открытия

6. По аналогии с правилом хеша создайте правило пути. В появившемся окне (рис. 8) в поле «Путь:» введите путь к файлам, работу с которыми нужно ограничивать, например: «%programfiles%\Messenger» и выберите уровень безопасности «Не разрешено». Путь можно указывать и к

конкретному файлу, а так же использовать подстановочные знаки «*» и «?», например: «c:\downloads*.*».

Попробуйте запустить программу обмена сообщений «Windows Messenger». Убедитесь в запрете запуска.

В правиле для пути имеется возможность использовать системные переменные, такие как «%programfiles%», «%systemroot%», «%userprofile%», «%windir%», «%appdata%» и «%temp%», а так же переменные окружения. Переменные окружения создаются следующим образом: в свойствах системы по пути «Пуск – Панель управления – Свойства системы» во вкладке «Дополнительно», нажмите на кнопку «Перменные среды». Далее в появившемся окне (рис. 9) нажмите кнопку «Создать». Введите имя переменной, например, «Share» и значение переменной «C:\Documents and Settings\All Users\Документы». Создайте и проверьте правило пути, применив переменную «%Share%».

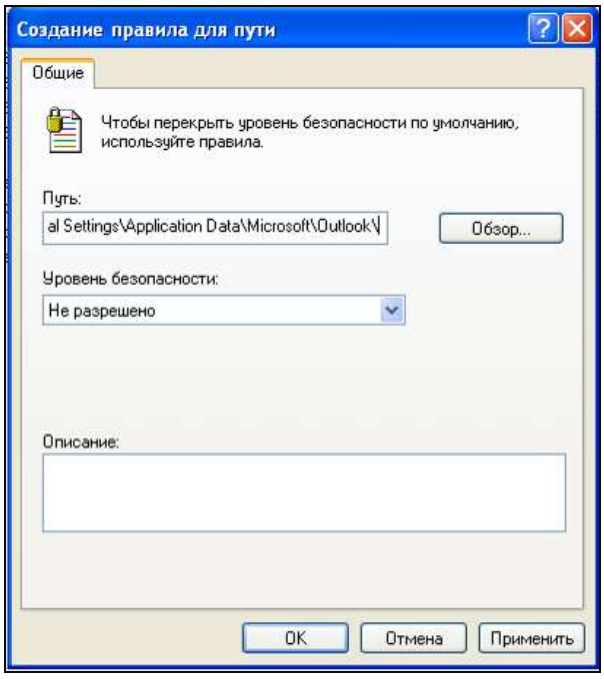


Рисунок 8 - Создание правила для пути

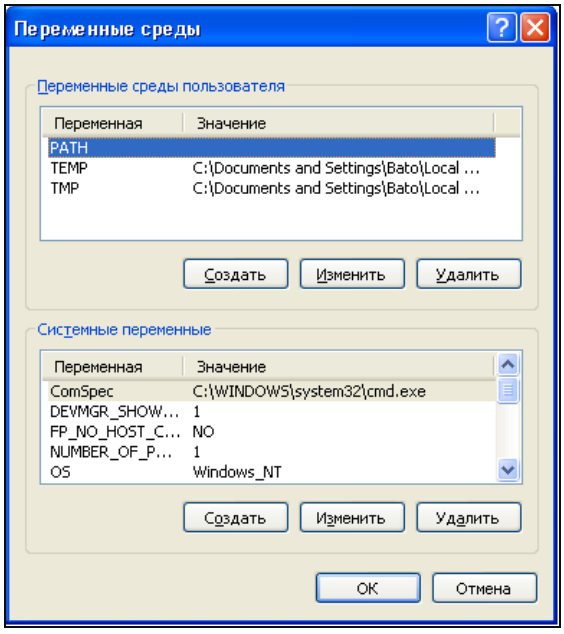


Рисунок 9 - Создание переменных окружения

7. Создаваемые «Правила для зоны Интернета…» применяются только к пакетам установщика программ Windows, добавление зон происходит с помощью свойств обозревателя «Internet Explorer» во вкладке безопасность.

8. Перед созданием правила для сертификата получите сертификат следующим образом: выберите, например, в свойствах файла программы «bootvis.msi», вкладку «Цифровые подписи» (рис. 10). Далее нажмите кнопку «Сведения» в появившемся окне (рис. 11) нажмите кнопку «Просмотр сертификата». Сертификат должен быть действителен. В появившемся окне (рис. 12) выберите вкладку «Состав» и нажмите кнопку «Копировать в файл…», при помощи мастера экспорта сертификатов сохраните сертификат, например, под именем «Microsoft.cer» (формат сохранения – X.509).

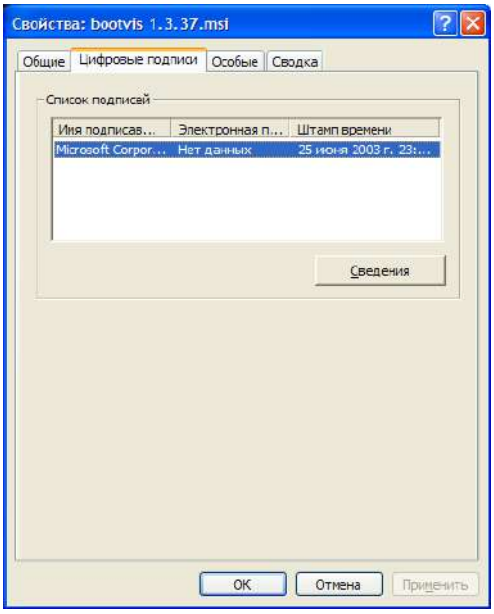


Рисунок 10 - Цифровые подписи файла

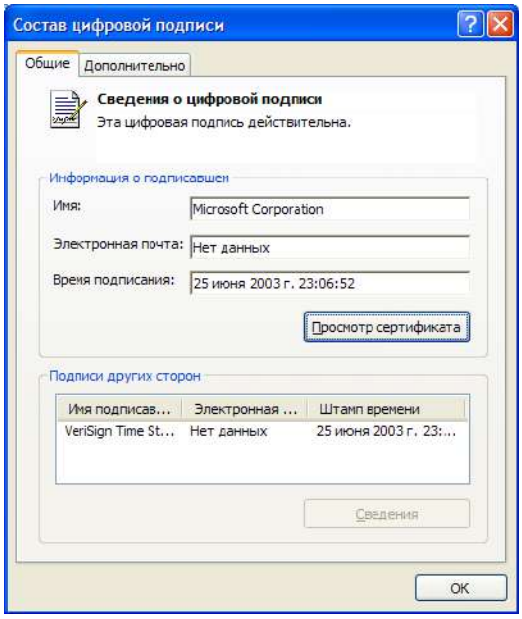


Рисунок 11 - Состав цифровой подписи файла

Назначьте по умолчанию уровень безопасности «Не разрешено». Далее в дополнительных правилах создайте «Правило для сертификата…», в появившемся окне (рис. 13 укажите путь к сохраненному файлу сертификата «Microsoft.cer» и выставите уровень безопасности «Неограниченный». Скопируйте файл «bootvis.msi» в папку «C:\Documents and Settings\All Users\Документы». При попытке запустить установочный пакет, подписанный данным сертификатом, выполнится приоритет правила сертификата над правилом пути. Проверьте возможность запуска. Правило сертификатов также может ограничить запуск подписанных программ с переносных носителей информации.

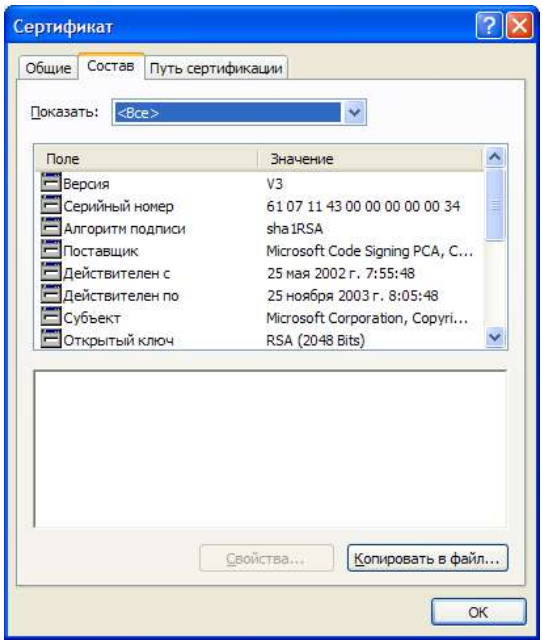


Рисунок 12 – Сертификат

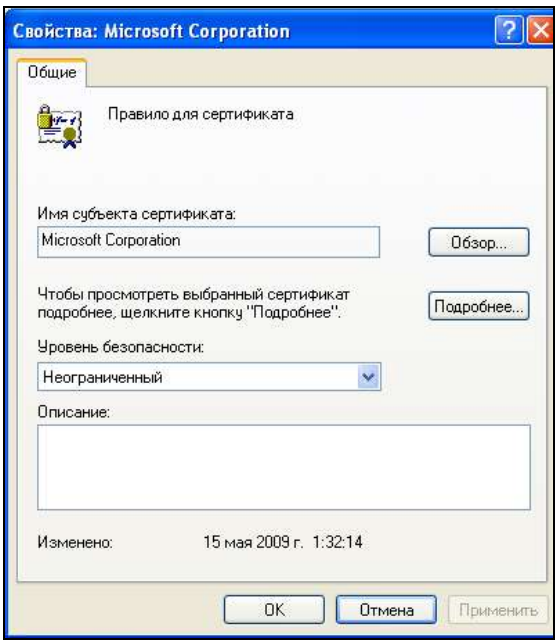


Рисунок 13 - Окно правила для сертификата

9. Для разрешения конфликтов, возникающих при использовании нескольких правил, используется приоритет. Ниже перечислены правила в порядке убывания приоритета.

1) Правило для хеша.

2) Правило для сертификата.

3) Правило для пути. При конфликте правил для пути приоритет имеет правило с большим ограничением. Ниже приведен набор путей в порядке от высшего приоритета (наибольшее ограничение) к низшему приоритету.

- диск:\папка1\папка2\имя_файла.расширение
- диск:\папка1\папка2*.расширение
- *.расширение
- диск:\папка1\папка2\
- диск:\папка1\

4) Правило для зоны Интернета.

При конфликте двух похожих правил для пути приоритет имеет правило с большим ограничением. Например, если имеется правило для пути «C:\Windows\» с уровнем безопасности «Не разрешено» и правило для пути «%windir%» с уровнем «Неограниченный», будет применяться более строгое правило с уровнем безопасности «Не разрешено».

В качестве примера создайте разрешающее правило хеша для программы «calc.exe», расположенного по запрещенному пути «c:\downloads». Далее попытайтесь запустить эту программу из ранее запрещенного пути. Приоритет правила для хеша позволит запустить программу из этой папки.

Удалите все созданные правила перед выполнением задания.

ЗАДАНИЕ:

Таблица 1 – Распределение требований по вариантам

Номер варианта	требования
1	с а по д
2	с б по е
3	с в по ж
4	с г по з
5	с д по и
6	с е по к
7	с ж по л
8	с з по м
9	с к по о
10	с л по п

1. Создайте следующую политику ограничения использования программ, которая будет удовлетворять следующим требованиям, согласно вашему варианту (табл. 1):

а) разрешает запуск ПО, подписанного сертификатом от «Microsoft»;

б) применяется ко всем пользователям, включая локальных администраторов;

в) не ограничивает использование программных библиотек, таких как «DLL»;

г) право выбора доверенных издателей разрешено только локальным администраторам;

д) запрещает запуск любых программ в качестве уровня безопасности по умолчанию;

е) разрешает запуск любых программ из папок: «C:\WINDOWS», «C:\Program Files», «C:\Documents and Settings\LocalService», «C:\Documents and Settings\All Users»;

ж) разрешает запуск любых программ пользователю из своей папки «C:\Documents and Settings\user» (где user – имя любого пользователя) при помощи переменной окружения;

з) при помощи приоритета правил пути пользователю запрещено запускать любые программы из папок других пользователей, как например, «C:\Documents and Settings\Администратор»;

и) разрешает установку ПО, подписанного сертификатом от «Microsoft»;

к) запрещает запуск программ «Паук», «Сапер» и «utorrent.exe» вне зависимости от их месторасположения;

л) запрещает запуск файла с именем «AUTORUN.INF» из любого места;

м) применяется ко всем пользователям, исключая локальных администраторов;

н) ограничивает использование программных библиотек, таких как «DLL»;

о) право выбора доверенных издателей разрешено любым пользователям;

п) запрещает установку ПО, подписанного сертификатом от «Microsoft».

2. Проверьте все созданные правила при помощи стандартного проводника «Explorer» и стороннего файлового менеджера, как например, «Far manager» или «Total Commander», игнорируют ли они ПОИП?

Контрольные вопросы:

1) Как создать политику ограниченного использования программ?
2) Возможно ли исключение из ПОИП локальных администраторов?
3) Для чего служит пункт «Назначенные типы файлов»?
4) В чем основное преимущество правила хеша перед правилом пути?
5) Приведите пример, когда запрещенная правилом хеша программа может выполниться.
6) Для чего служит правило для сертификата?
7) Как можно получить сертификат из файла?
8) Приведите три примера использования приоритета правил.
9) Как запретить открытие любых файлов с расширением «.swf» из любого места на жестком диске?
10) Объясните различие между уровнями безопасности «Неограниченный» и «Не разрешено».

Лабораторная работа № 4
Аудит событий безопасности операционной системы

Целью данной работы является ознакомление с интерфейсом управления подсистемой аудита безопасности и параметрами политики аудита на примере операционной системы Windows XP.

Ход работы

1. Политика аудита

Политика аудита определяет, какие категории сообщений о событиях отслеживаются и сохраняются в журнале безопасности. Настройка политики происходит при помощи оснастки «Локальная политика безопасности».

Войдите в операционную систему под учётной записью «Администратор». Откройте оснастку «Локальная политика безопасности» («Пуск – Панель управления – Администрирование»). Выберите раздел «Локальные политики – Политика аудита» (рис. 1).

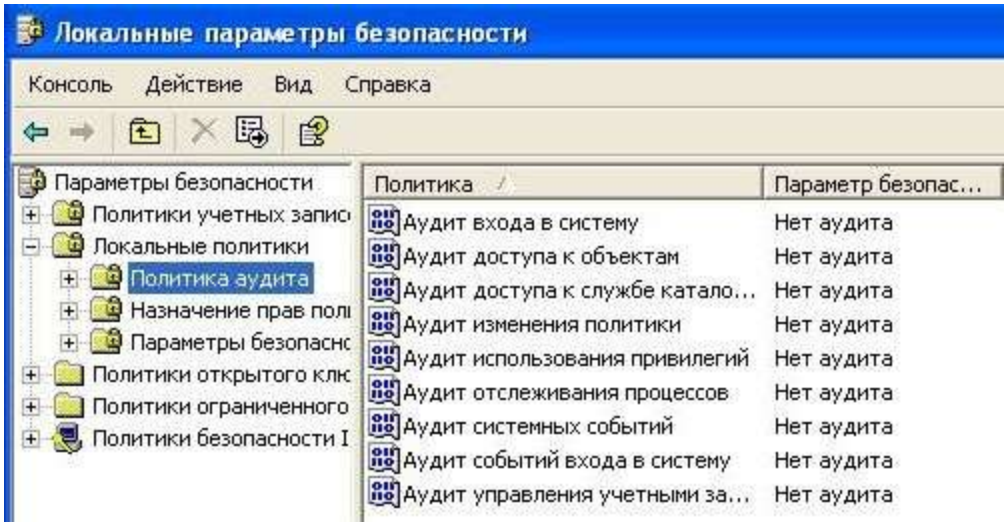


Рисунок 1 – Политика аудита Windows XP

В политике аудита представлен набор параметров, соответствующих различным категориям событий безопасности. В «Свойствах» каждого из параметров возможно включение фиксации событий, относящихся к соответствующей категории. Откройте параметр политики аудита «Аудит входа в систему» (рис.2). Включение аудита происходит по следующим типам событий:

- «Успех» – фиксируются события, осуществление которых было разрешено пользователю;
- «Отказ» – фиксируются события, осуществление которых было запрещено пользователю.

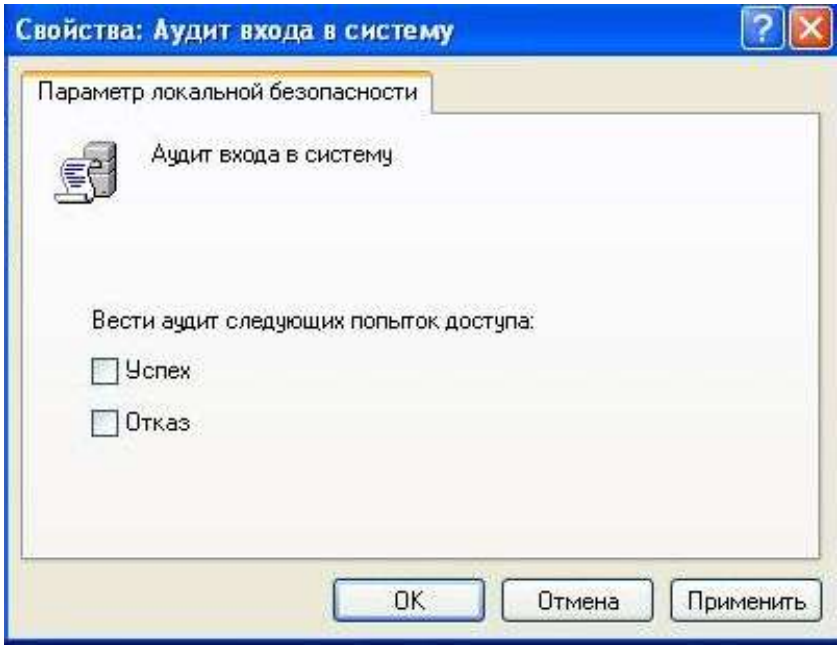


Рисунок 2 – Настройки параметра «Аудит входа в систему»

2. Аудит входа/выхода пользователей

Параметр «Аудит входа в систему» включает фиксацию каждой попытки входа пользователя в систему или выхода из неё на данном компьютере. Включите оба типа событий («Успех» и «Отказ») для параметра «Аудит входа в систему».

Включите оба типа событий («Успех» и «Отказ») для параметра «Аудит событий входа в систему». Параметр «Аудит событий входа в систему» включает фиксацию каждой проверки данным компьютером учётных данных (в т.ч. контроллером домена при входе в домен на рабочей станции).

Завершите сеанс текущего пользователя. Введите неверный пароль при входе в операционную систему, чтобы сгенерировать событие типа «Отказ».

Войдите под учётной записью «Администратор». Откройте журнал «Безопасность» оснастки «Просмотр событий» (рис. 3).

Рисунок 3 – Журнал «Безопасность»

Записи журнала «Безопасность» включают в себя следующую информацию о событии: время и дата события; имя учётной записи пользователя, сгенерировавшего событие; имя компьютера, на котором произошло событие; категорию и тип события; код события; дополнительную информацию в зависимости от категории события.

В журнале «Безопасность» откройте запись категории «Вход/выход» типа «Аудит отказов». Данная запись описывает событие, сгенерированное при вводе неправильного пароля (рис. 4). Так как пользователь ещё не прошёл аутентификацию, событие было сгенерировано от имени пользователя «System». В записи о событии указывается имя пользователя, использовавшееся при осуществлении неудачной попытки входа в систему, и тип входа. Код данного события – 529.

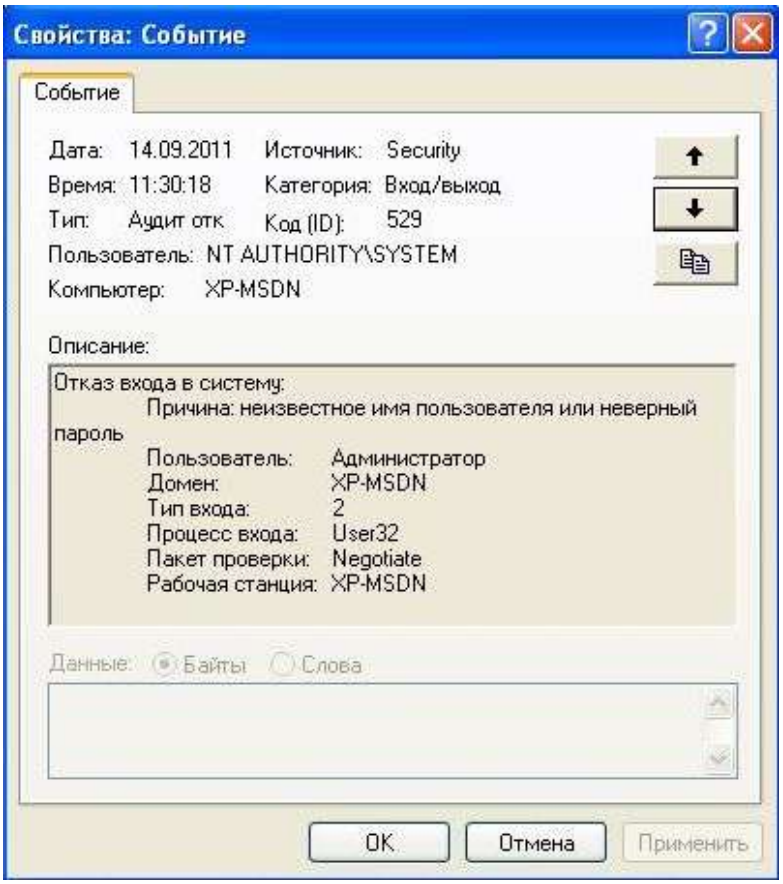


Рисунок 4 – Запись аудита об отказе входа в операционную систему

Откройте запись категории «Вход/выход» типа «Аудит успехов» с кодом 528. Данная запись описывает событие, сгенерированное при удачном входе в операционную систему (рис. 5).

В обеих записях (аудита успехов и отказов) указан тип входа в систему – 2. Этот тип означает интерактивный вход в систему. Типы входа в систему, фиксируемые в Windows XP, приведены в табл. 1.

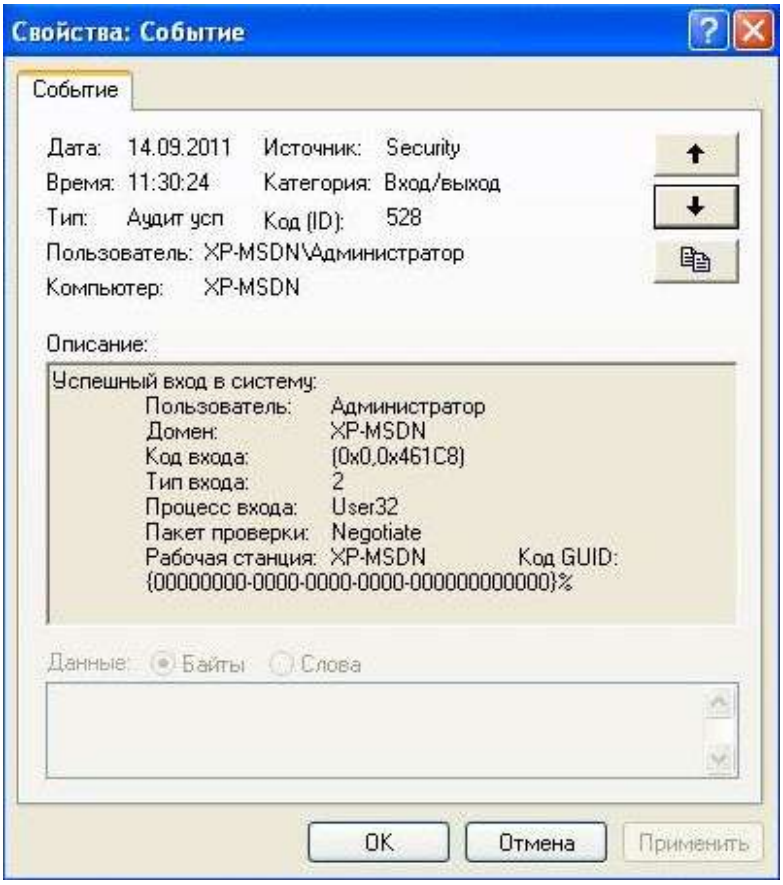


Рисунок 5 – Запись аудита об успешном входе в операционную систему

Таблица 1 – Описание типов входа в систему

Тип входа	Название типа входа	Описание
2	Интерактивный	Локальный вход пользователя на компьютер.
3	Сеть	Пользователь вошёл на данный компьютер через сеть.
4	Пакетный	Пакетный тип входа используется пакетными серверами.
5	Служба	Служба запущена Service Control Manager.
7	Разблокирование	Эта рабочая станция разблокирована.
8	NetworkCleartext	Пользователь вошёл на данный компьютер через сеть. Пароль пользователя передан в нехэшированной форме.
9	NewCredentials	Посетитель клонировал свой текущий маркер и указал новые учётные записи для исходящих соединений.

10	RemoteInteractive	Пользователь выполнил удалённый вход на этот компьютер, используя службу терминалов или удаленный рабочий стол.
11	CachedInteractive	Пользователь вошёл на этот компьютер с сетевыми учётными данными, которые хранились локально на компьютере.

Откройте запись категории «Вход/выход» типа «Аудит успехов» с кодом 551. Данная запись содержит информацию, связанную с успешным выходом пользователя из операционной системы.

Откройте записи категории «Вход учётной записи» (рис. 6, 7). Оба типа события («Успех» и «Отказ») имеют один код события – 680. Дополнительно в записи указывается механизм аутентификации – Microsoft Authentication Package.

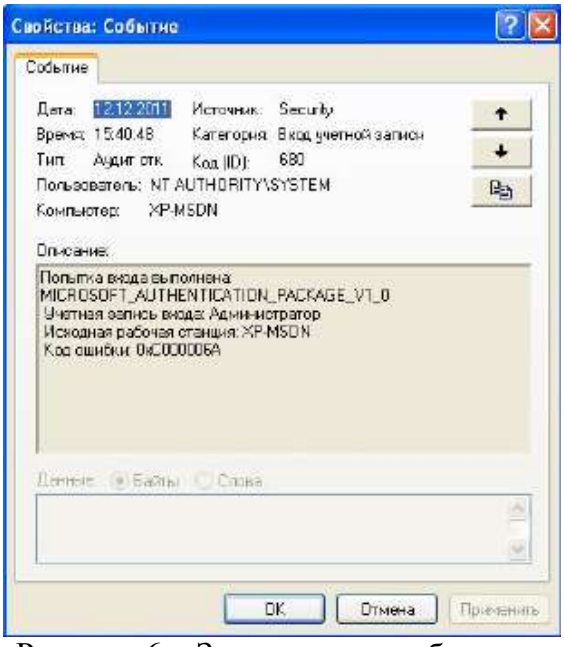


Рисунок 6 – Запись аудита об отказе входа учётной записи

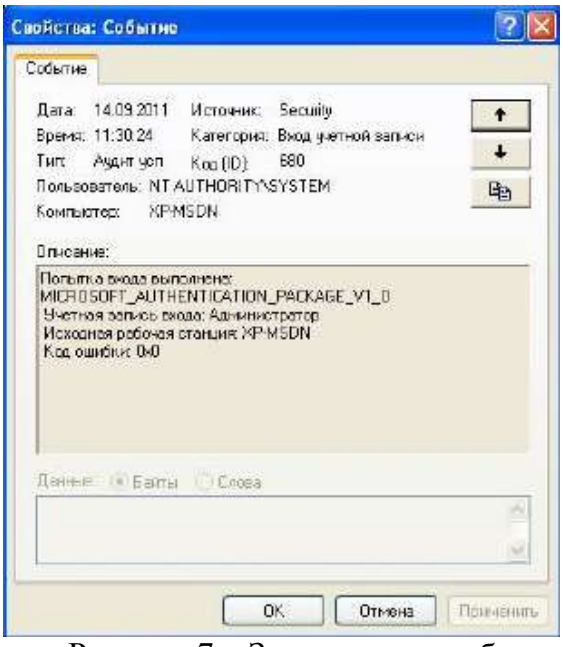


Рисунок 7 – Запись аудита об успешном входе учётной записи

3. Аудит событий, связанных с администрированием

Параметр «Аудит управления учётными записями» включает фиксацию событий, связанных с управлением учётными записями пользователей и групп пользователей. Включите тип событий «Успех» для «Аудита управления учётными записями».

Измените пароль пользователю «user», создайте нового пользователя «user1». Записи категории «Аудит управления учётными записями» содержат как имя учётной записи, у которой были

проведены изменения, так и имя учётной записи пользователя, изменявшего настройки.

Откройте в журнале «Безопасность» запись категории «Учётные записи» с кодом события 628 (при отсутствии записи обновите журнал). Данная запись содержит информацию об изменении пароля учётной записи (рис. 8). В записи аудита представлены имена учётных записей обоих пользователей – у которого пароль был изменён («user») и от имени которой он изменялся («Администратор»).

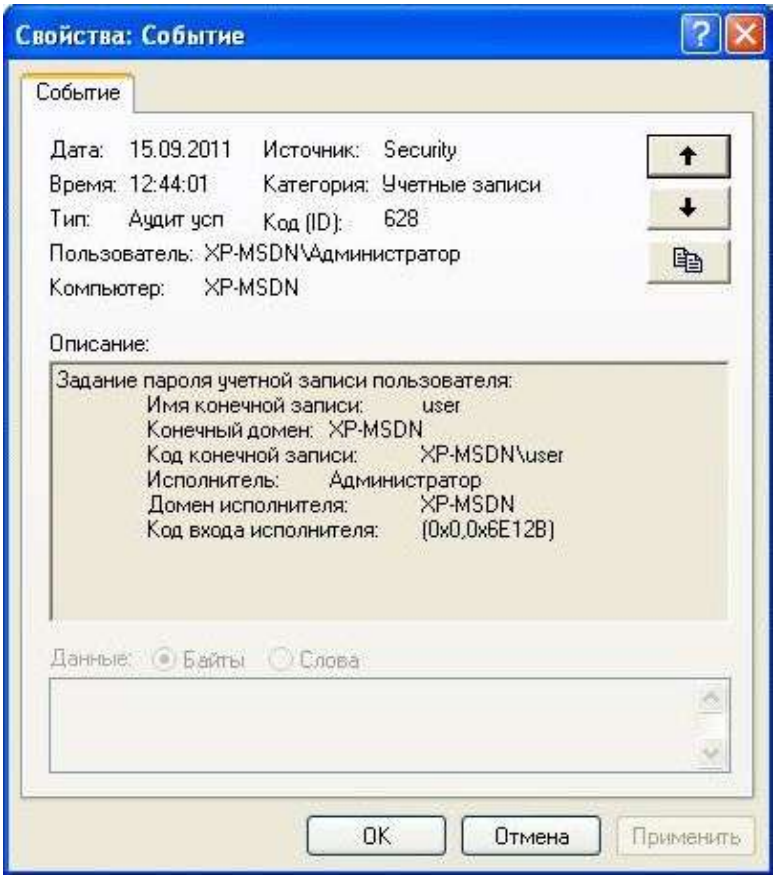


Рисунок 8 – Запись аудита об успешном изменении пароля учётной записи

Откройте запись категории «Учётные записи» с кодом события 626. Данная запись содержит информацию о включении (создании новой) учётной записи пользователя (рис. 9).

При создании нового пользователя автоматически происходит его добавление в группу. Откройте запись категории «Учётные записи» с кодом события 636. Данная запись содержит информацию о добавлении учётной записи пользователя в существующую группу (рис. 10). В записи указаны имя учётной записи пользователя, производившего добавление, имя учётной записи добавляемого пользователя и имя группы, в которую добавляется пользователь.

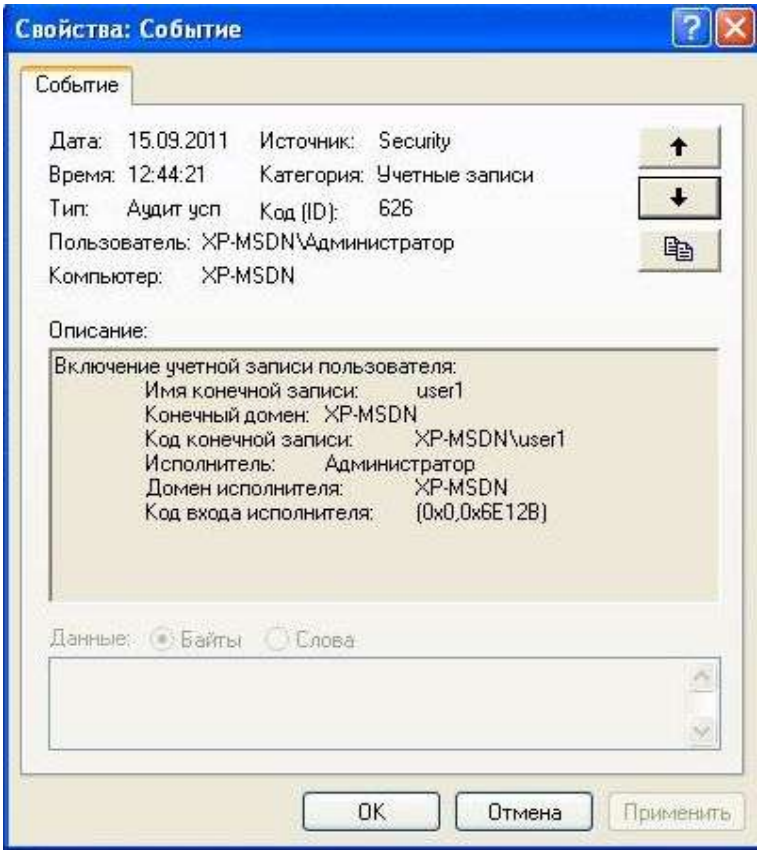


Рисунок 9 – Запись аудита о включении учётной записи

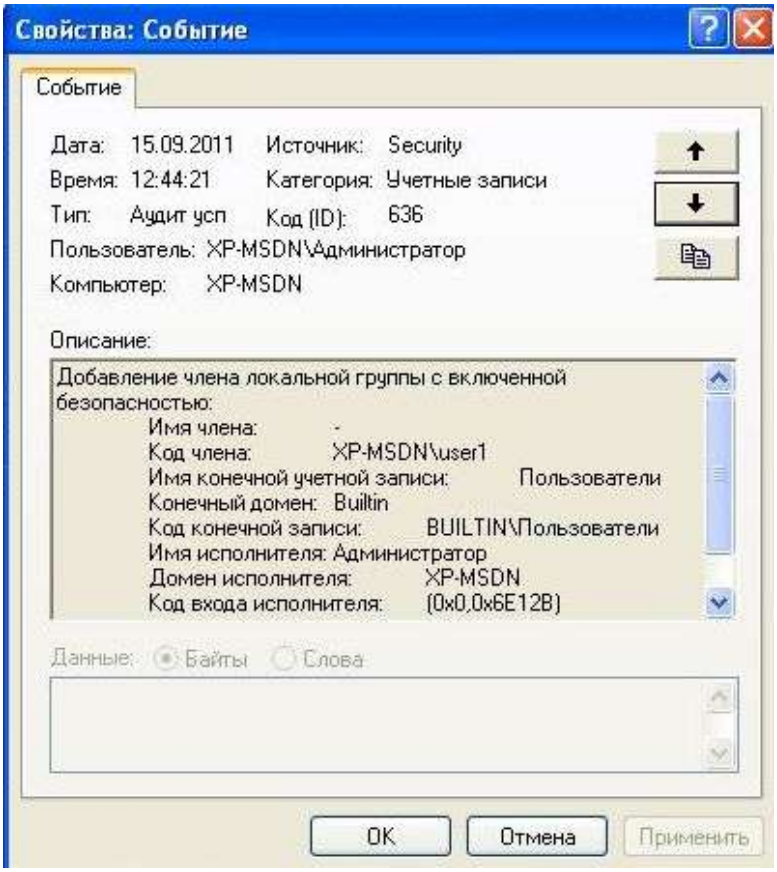


Рисунок 10 – Запись аудита о добавлении учётной записи в группу

Параметр «Аудит изменения политики» включает фиксацию событий, связанных с изменением политики аудита, назначения прав пользователям и т.д. Включите тип событий «Успех» для «Аудита изменения политики».

Откройте раздел «Локальные политики – Назначение прав пользователя» в «Локальной политике безопасности». Предоставьте пользователю «user» право «Архивирование файлов и каталогов», удалите право «Локальный вход в систему» у учётной записи «Гость».

Записи категории «Аудит изменения политики» содержат имя учётной записи, производившей изменение какой-либо политики, название изменяемой привилегии или настройки. Если происходило изменение привилегии учётной записи пользователя, то указывается имя этой учётной записи.

Откройте запись категории «Изменение политики» с кодом 608 (рис. 11). Данная запись содержит информацию о предоставлении пользователю права на резервное копирование информации (SeBackupPrivelege).

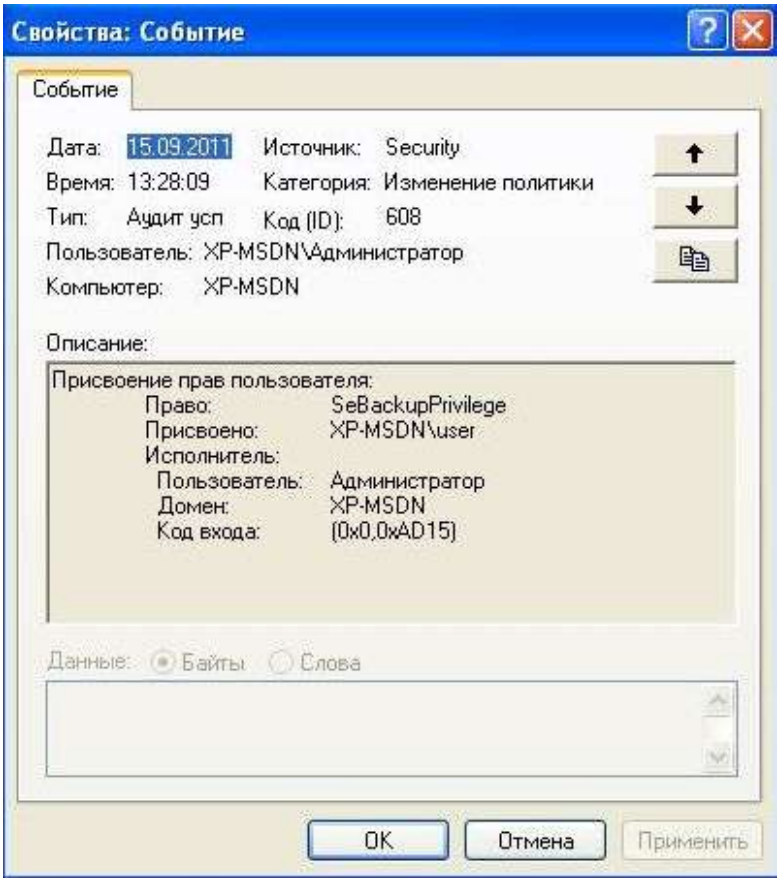


Рисунок 11 – Запись аудита о присвоении пользователю прав

Откройте запись категории «Изменение политики» с кодом 622 (рис. 12). Данная запись содержит информацию об удалении права локального входа пользователя в систему (SeInteractiveLogonRight).

Откройте запись категории «Изменение политики» с кодом 612 (рис. 13). Данная запись содержит информацию об изменении политики аудита. Зафиксировано включение аудита «Успехов» в категории «Изменение политики».

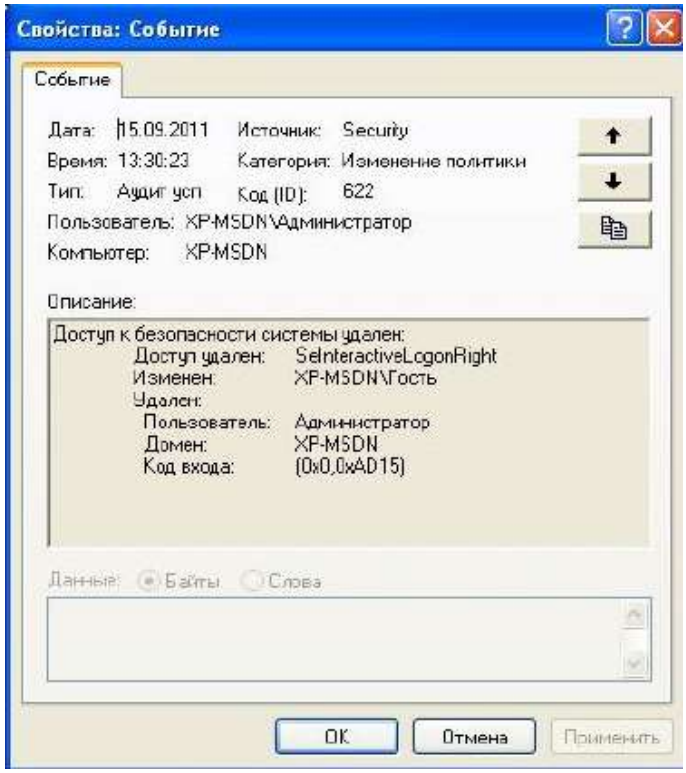


Рисунок 12 – Запись аудита об удалении прав у пользователя

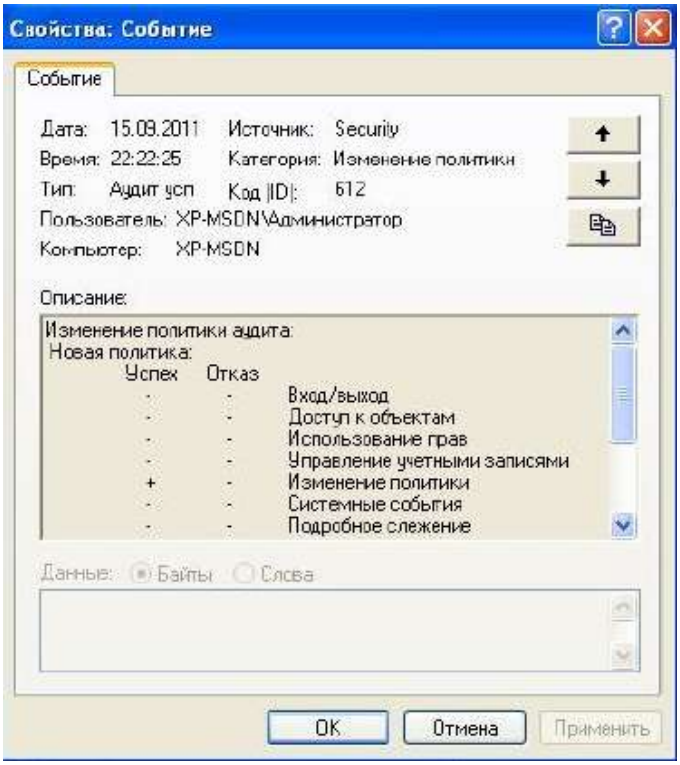


Рисунок 13 – Запись аудита об изменении политики безопасности

Параметр «Аудит использования привилегий» включает фиксацию событий, связанных с применением пользователем выданных ему привилегий. Включите тип событий «Успех» для «Аудита использования привилегий».

Измените системное время. Завершите сеанс пользователя. Войдите под учётной записью «Администратор».

Откройте запись категории «Использование прав» с кодом 577 (рис. 14). Данная запись содержит информацию об использовании привилегии изменения системного времени (SeSystemtimePrivelege) с указанием пользователя, применившего привилегию.

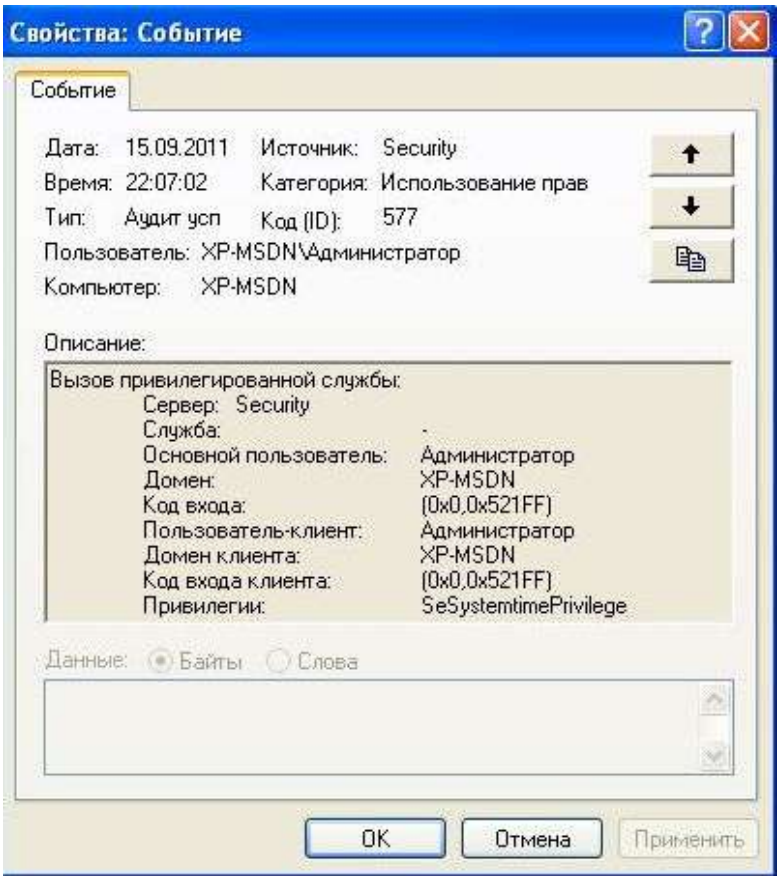


Рисунок 14 – Запись аудита о применении привилегии на изменение системного времени

Откройте запись категории «Использование прав» с кодом 576 (рис. 15). Данная запись содержит информацию о предоставлении пользователю набора привилегий при входе в операционную систему.

Откройте запись категории «Использование прав» с кодом 578 (рис. 16). Данная запись содержит информацию об операции с привилегированным объектом – открытие журнала аудита (EventLog).

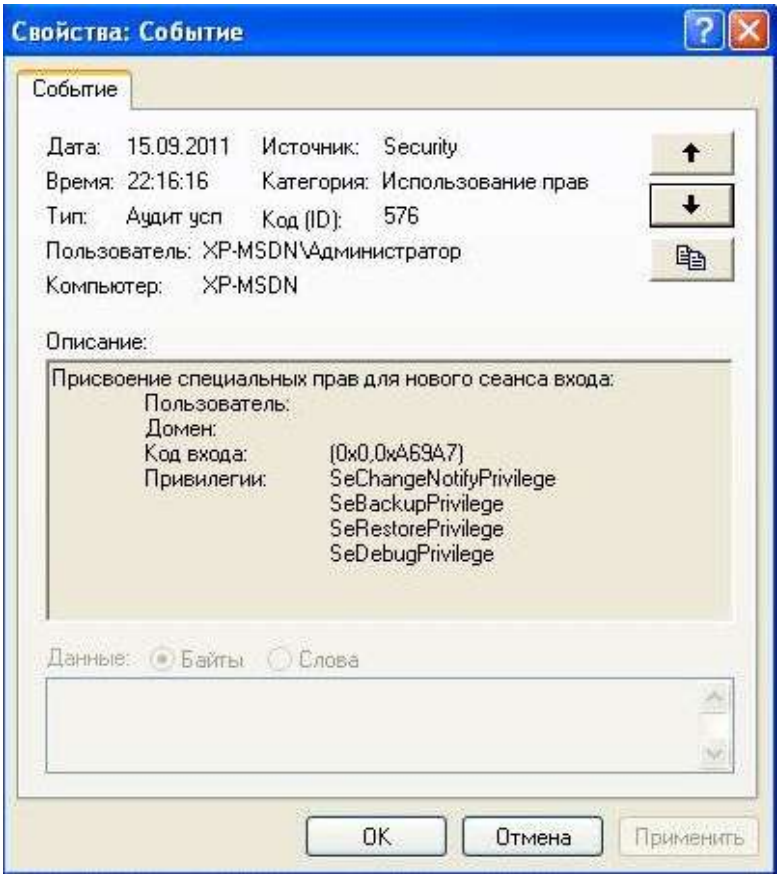


Рисунок 15 – Запись аудита о присвоении привилегий пользователю при входе в систему

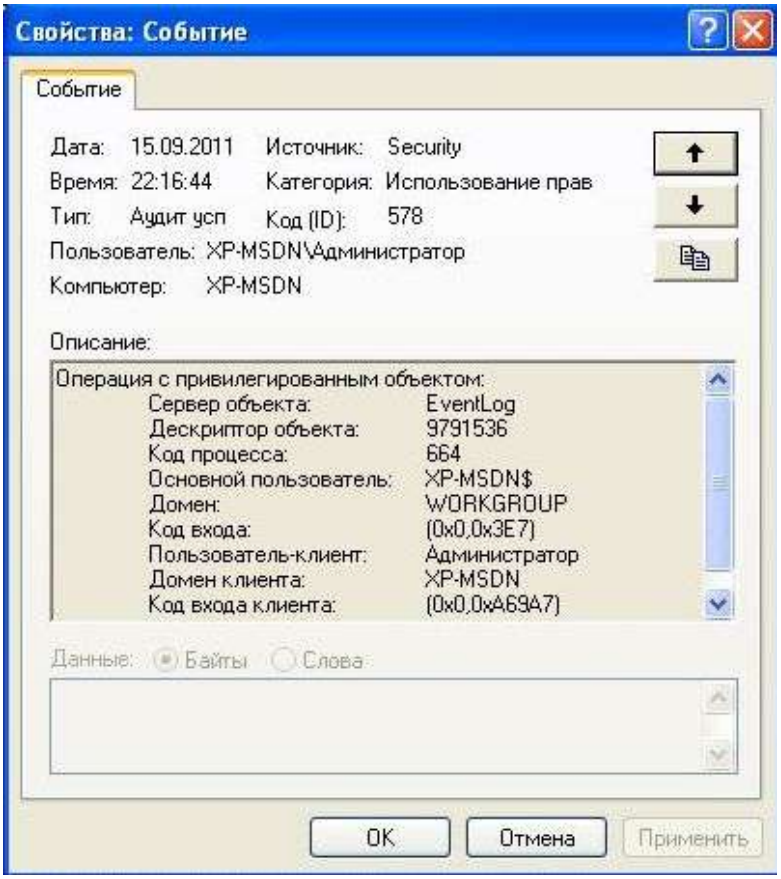


Рисунок 16 – Запись аудита о работе с журналом аудита

4. Аудит событий, связанных с работой операционной системы

Параметр «Аудит системных событий» включает фиксацию событий, связанных со следующими системными событиями: изменение системного времени; запуск и отключение элементов системы безопасности и др. Включите тип событий «Успех» для «Аудита системных событий».

Очистите журнал аудита (например, через контекстное меню журнала). Перезагрузите операционную систему.

Откройте запись категории «Системное событие» с кодом 517 (рис. 17). Данная запись содержит информацию о времени очистки журнала аудита и имя учётной записи пользователя, очистившего журнал.

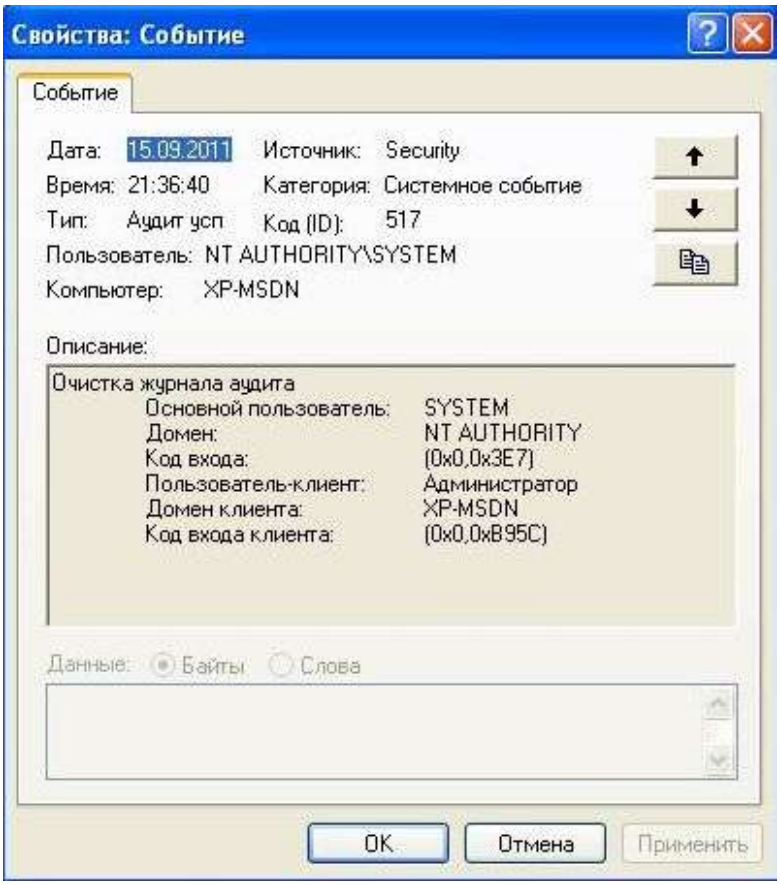


Рисунок 17 – Запись аудита об очистке журнала аудита

Откройте запись категории «Системное событие» с кодом 520 (рис. 18). Данная запись содержит информацию об изменении системного времени. Это событие может генерироваться как от имени учётной записи «System» при синхронизации времени с сервером, так и от имени пользователя. В записи указывается предыдущее и новое время.

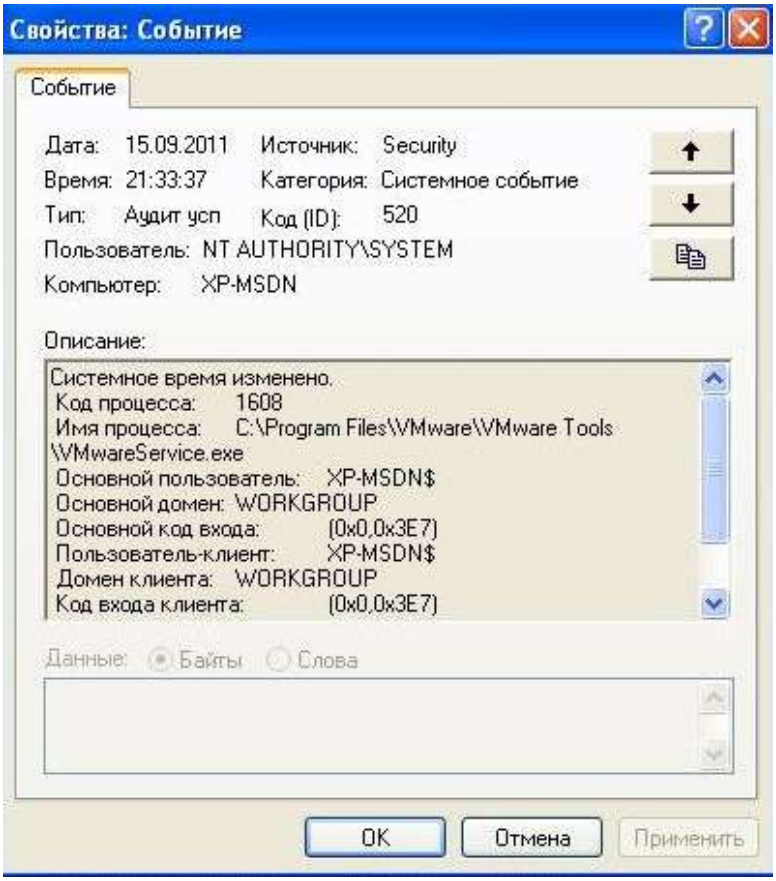


Рисунок 18 – Запись аудита об изменении системного времени

Параметр «Аудит отслеживания процессов» включает фиксацию событий, связанных с работой процессов (создание, завершение, дублирование и т.п.). Включите тип событий «Успех» для «Аудита отслеживания процессов».

Запустите какое-нибудь приложение и закройте его.

Откройте записи категории «Подробное отслеживание» с кодом 592 и 593 (рис. 19, 20). Эти записи содержат информацию о создании нового процесса и его завершении. В информацию о событии включается полное имя исполняемого файла, инициировавшего процесс.

5. Аудит доступа пользователей к ресурсам

Параметр «Аудит доступа к объектам» включает фиксацию событий, связанных с доступом к файлам, каталогам, ключам реестра, принтерам и т.д. Возможен аудит различных типов доступа: чтения, изменения, удаления, печати и др.

Включите оба типа событий («Успех» и «Отказ») для параметра «Аудит доступа к объектам».

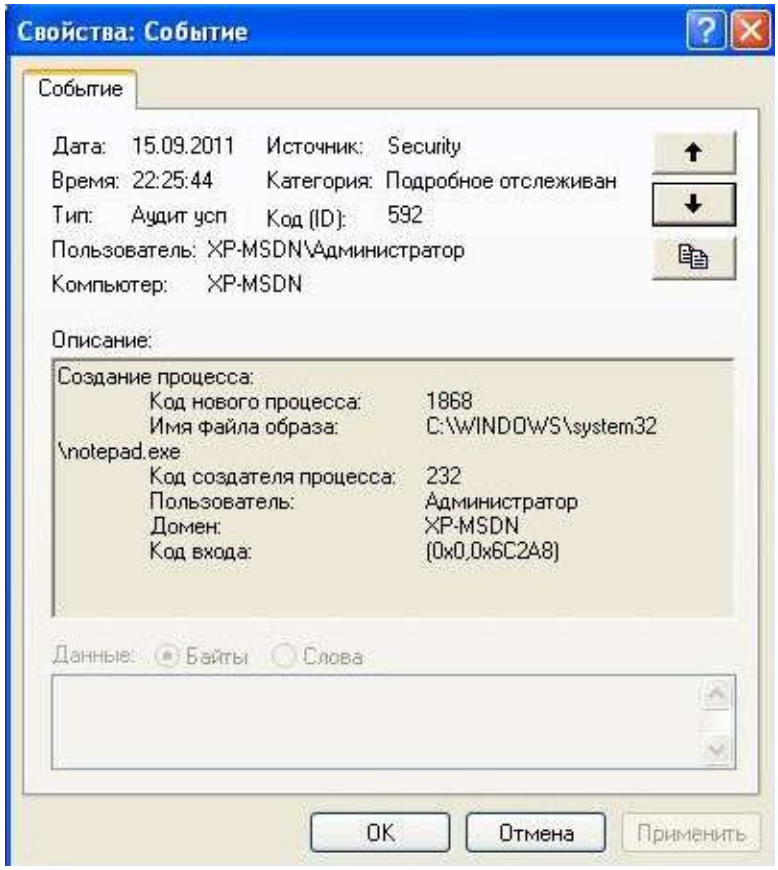


Рисунок 19 – Запись аудита о запуске приложения (создании процесса)

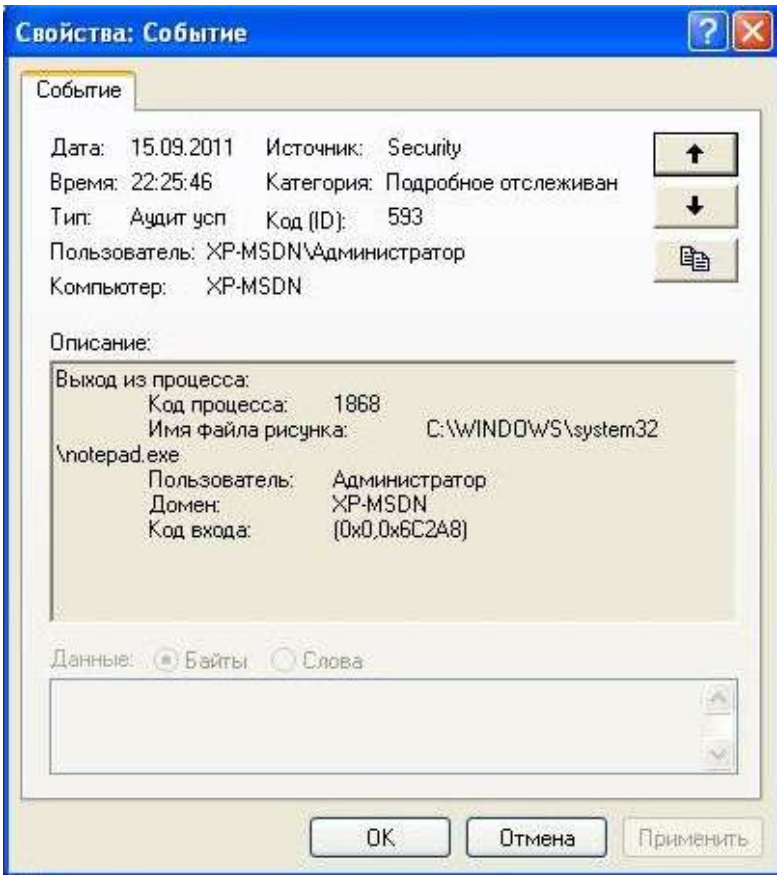


Рисунок 20 – Запись аудита о завершении приложения (выходе из процесса)

Аудит доступа к ресурсам возможен только на логических дисках с файловой системой NTFS. Аудиту подвергаются только те объекты, для которых явно указана необходимость фиксации событий. Таким образом, включение аудита доступа происходит в два этапа: включение «Аудита доступа к объектам» в политике аудита и включение аудита для каждого контролируемого объекта.

Создайте текстовый файл. Перейдите на вкладку «Аудит» в «Свойствах» созданного файла («Свойства – Безопасность – Дополнительно – Аудит»). Включите тип событий «Успех» на тип доступа «Изменение разрешений» для пользователя «Администратор» и тип событий «Отказ» на все типы доступа для пользователя «user» (рис. 21). Во вкладке «Безопасность» свойств созданного файла запретите пользователю «user» доступ на «Запись».

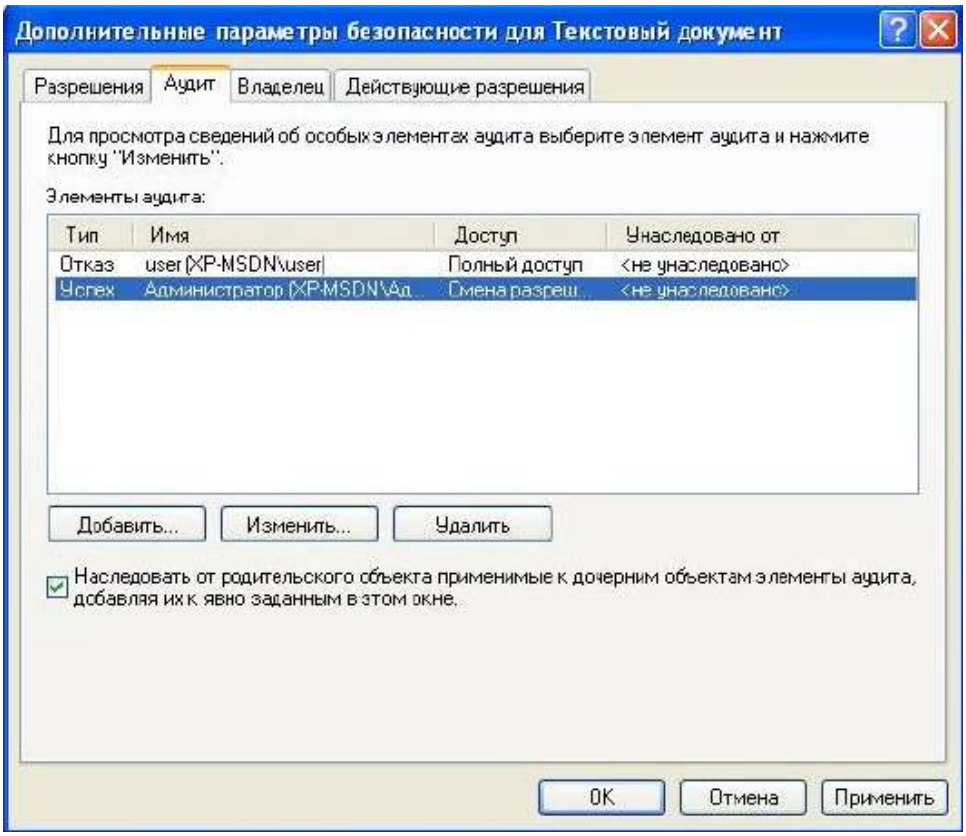


Рисунок 21 – Параметры аудита доступа к файлу

Откройте запись категории «Доступ к объекту» с кодом 560 (рис. 22, 23). Данная запись содержит информацию об успешной смене разрешений на доступ к объекту (тип доступа – WRITE_DAC). Кроме типа доступа, в записи указывается информация об объекте доступа: имя и тип (File). О субъекте доступа указывается следующая информация: имя учётной записи, осуществлявшей доступ, и полное имя исполняемого файла процесса, при помощи которого осуществлялся доступ.

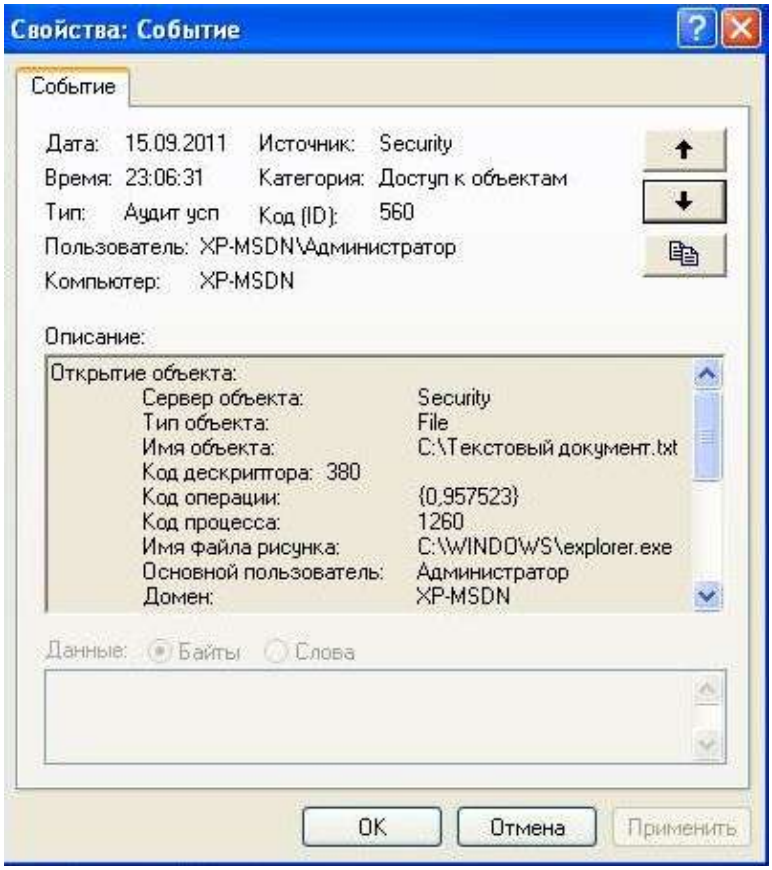


Рисунок 22 – Запись аудита о доступе к объекту для изменении прав доступа

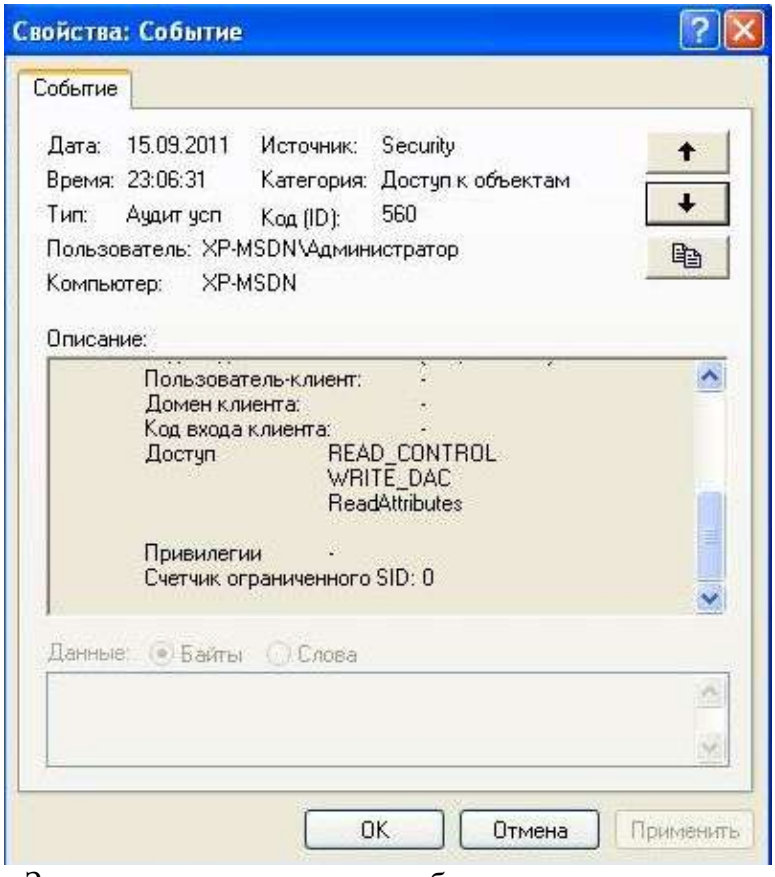


Рисунок 23 – Запись аудита о доступе к объекту для изменении прав доступа (окончание)

Войдите под учётной записью «user». Попытайтесь удалить созданный файл, попытайтесь изменить разрешения на доступ к файлу.

Войдите под учётной записью «Администратор». Откройте записи журнала «Безопасность» категории «Доступ к объекту» с кодом 560, произведённой от имени учётной записи «user». Одна из записей содержит информацию о неуспешной (Аудит отказов) попытке удаления файла (тип доступа – DELETE, рис. 24). Другая запись содержит информацию о неуспешной (Аудит отказов) попытке изменения разрешений на доступ к файлу (рис. 25).

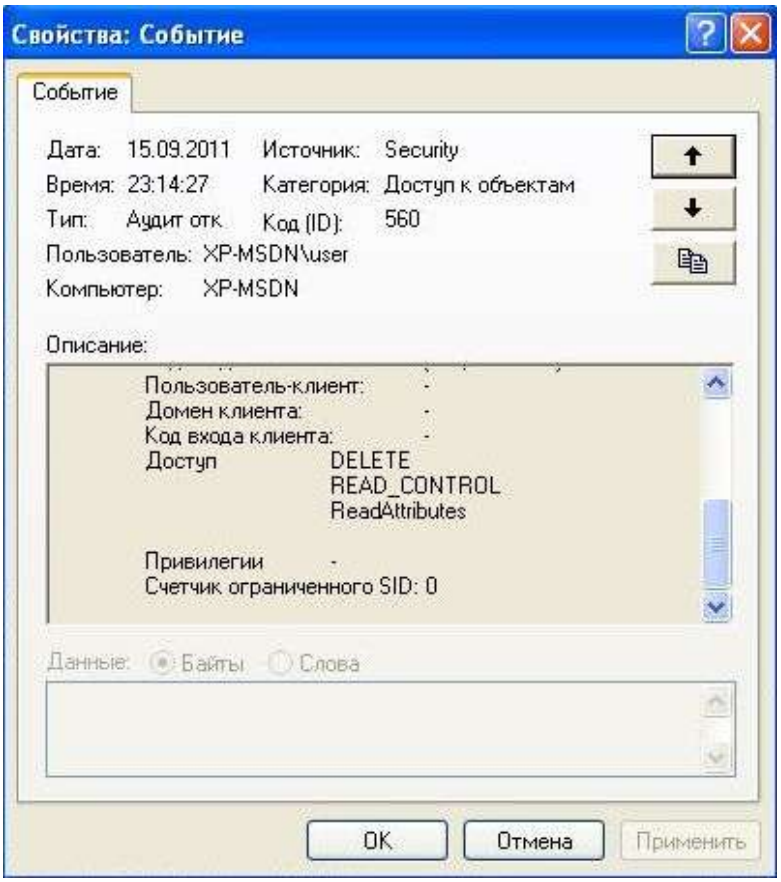


Рисунок 24 – Запись аудита о неуспешной попытке доступа к объекту для его удаления

Откройте «Свойства» принтера doPDF («Пуск – Настройка – Принтеры и факсы»). Для принтеров возможен аудит следующих специфичных действий: печать, управление принтерами, управление документами.

Включите тип аудита «Успех» типа доступа «Управление документами» принтера doPDF для пользователя «Администратор» (применить «Для этого принтера и докуентов», рис.26). Напечатайте текстовый документ.

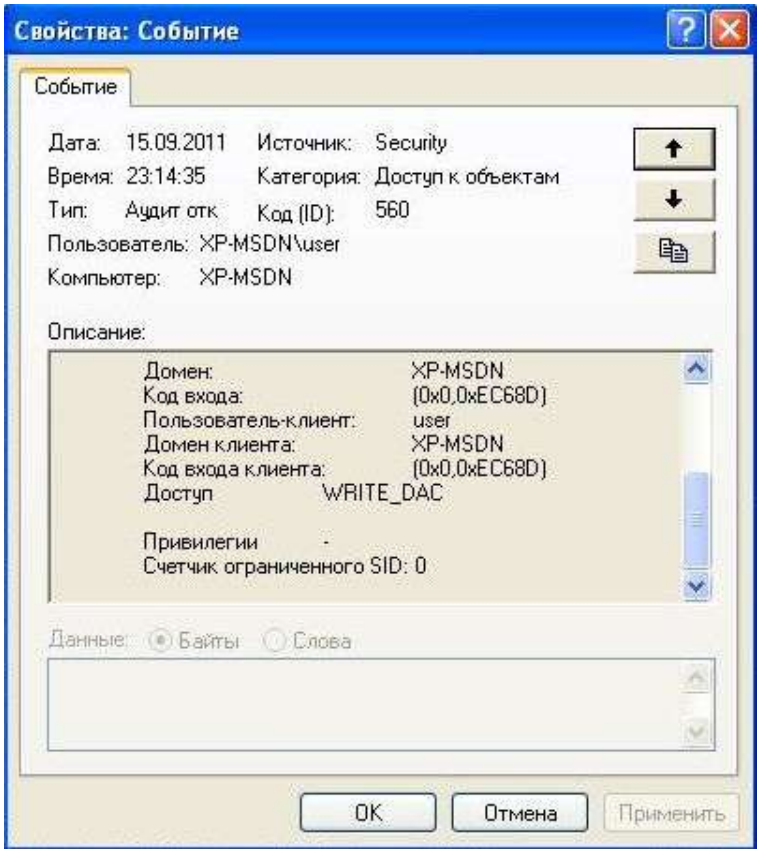


Рисунок 25 – Запись аудита о неуспешной попытке доступа к объекту для изменения прав доступа к нему

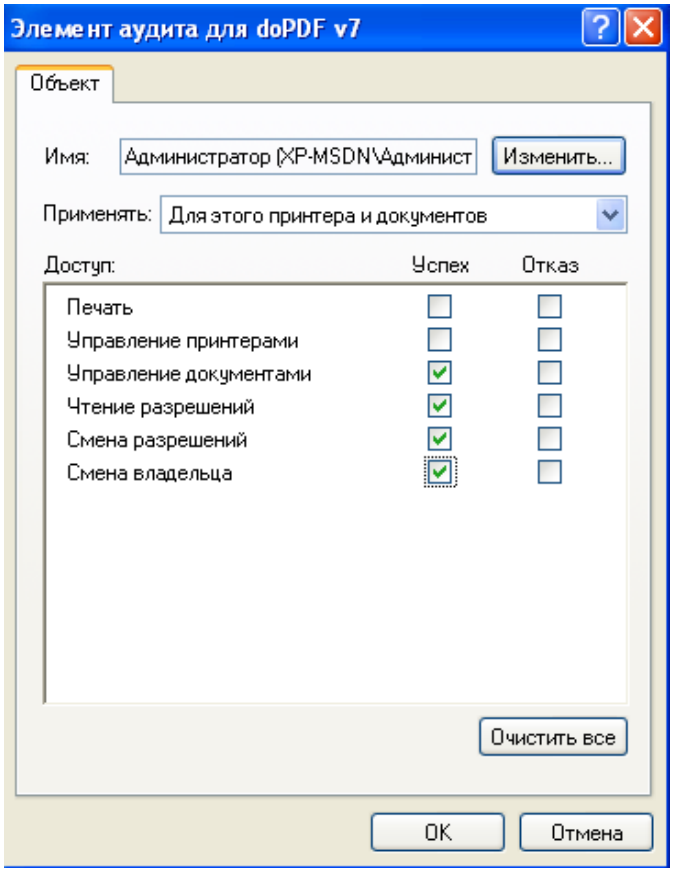


Рисунок 26 – Параметры аудита доступа к принтеру

Просмотрите записи категории «Доступ к объекту» с кодом 560. К печати документа имеют отношение записи с типом объекта Printer (рис. 27) и Document (рис. 28). В записи для принтера указан тип доступа «Печать». В записи для документа указано имя напечатанного документа.

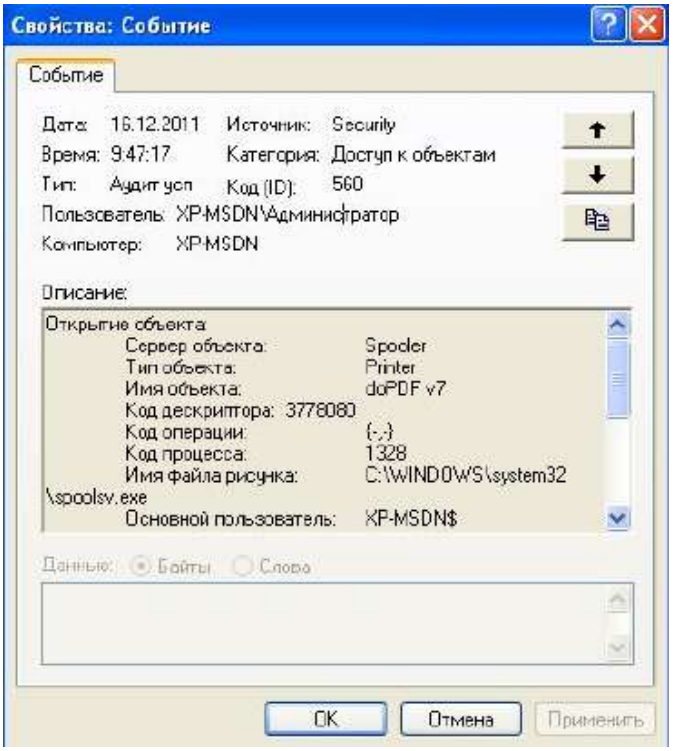


Рисунок 27 – Запись аудита об использовании принтера

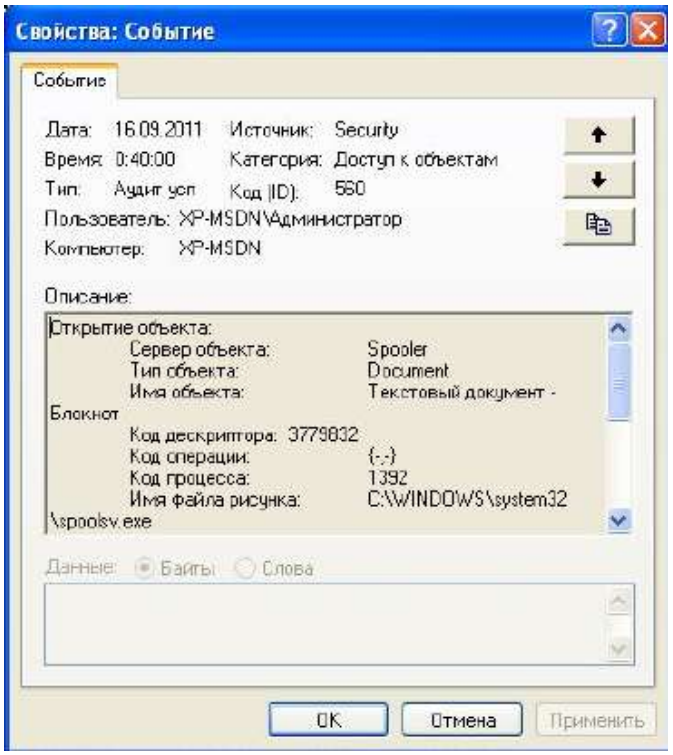


Рисунок 27 – Запись аудита об управлении документом

6. Управление журналом аудита

Войдите под учётной записью «user». Попытайтесь открыть журнал аудита. Группе «Пользователи», в которую входит «user», по умолчанию запрещена работа с журналом аудита, поэтому операционная система сгенерирует ошибку доступа (рис.29).

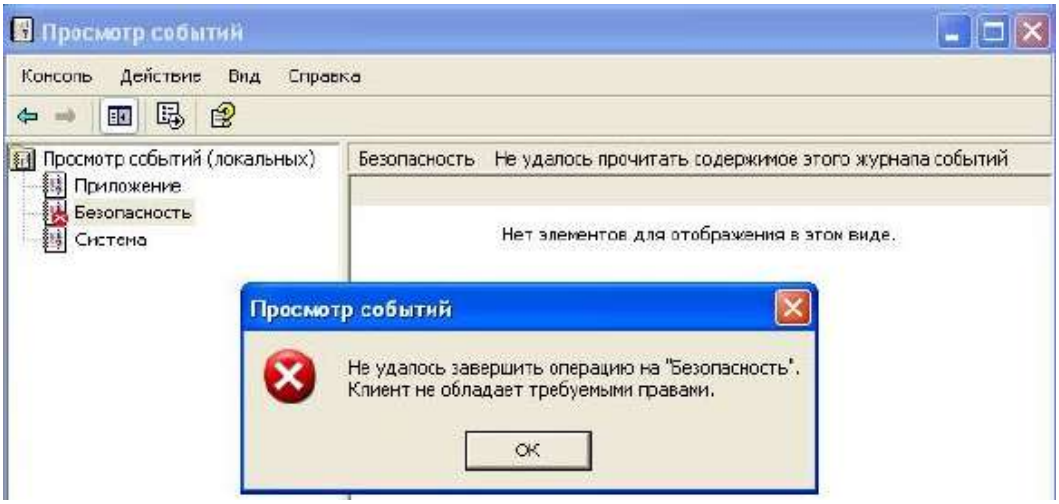


Рисунок 29 – Ошибка доступа к журналу аудита

Запустите от имени учётной записи «Администратор» оснастку «Локальная политика безопасности». Добавьте пользователя «user» в перечень учётных записей параметра «Управление аудитом и журналом безопасности» («Локальные политики – Назначение прав пользователей», рис. 30). Под учётной записью «user» проверьте наличие прав для работы с журналом аудита.

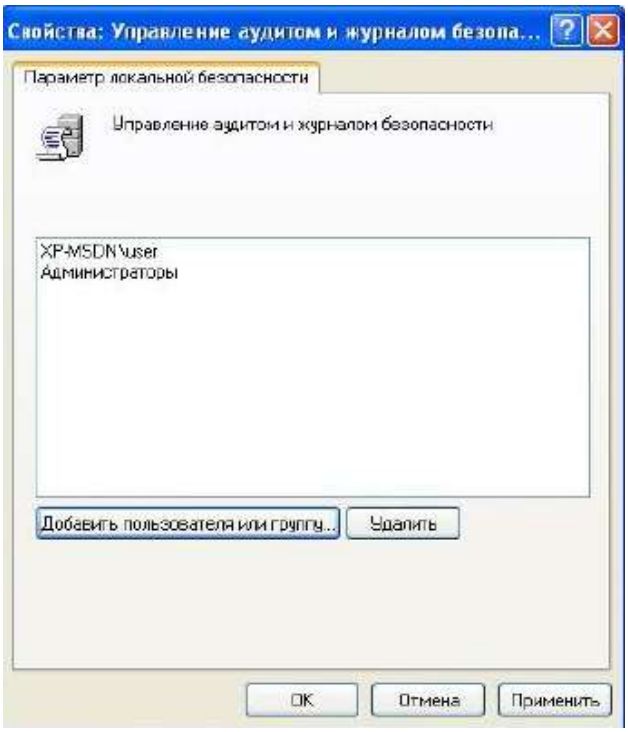


Рисунок 30 – Параметр управления доступом к журналу безопасности

Войдите под учётной записью «Администратор». В меню журнала аудита выберите «Вид» – «Фильтр». Настройте фильтр в соответствии с рис. 31. После применения фильтра в журнале останутся записи только об удачных и неудачных попытках входа под учётной записью «user».

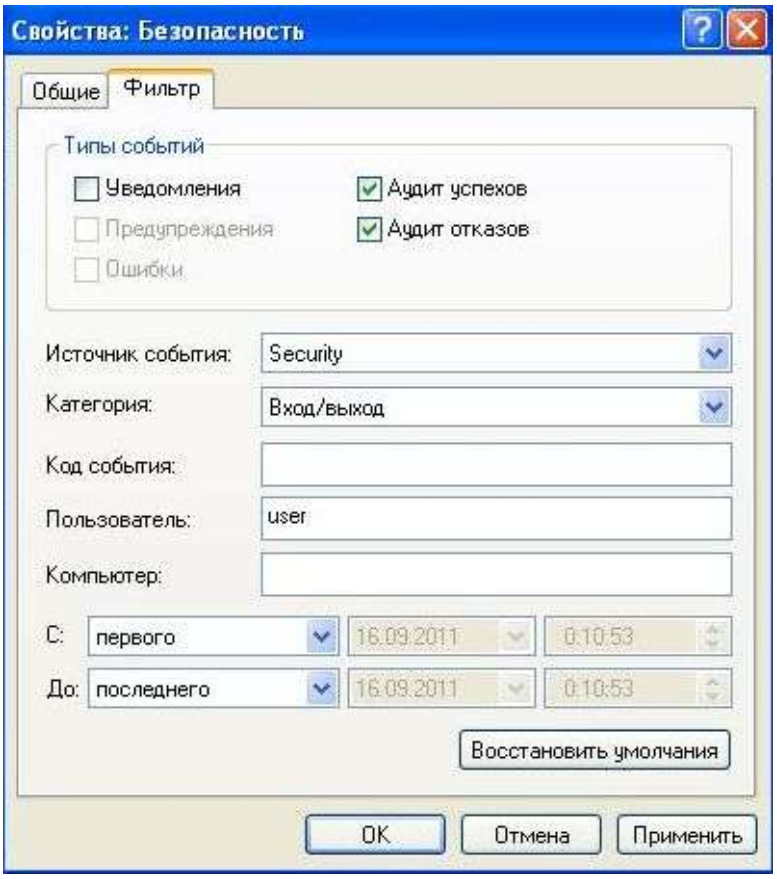


Рисунок 31 – Настройка фильтрации записей журнала безопасности

При поиске объекта с известным именем лучше использовать функцию поиска: «Вид» – «Найти» (рис. 32), введя имя (часть имени) файла.

В контекстном меню журнала «Безопасность» выберите «Свойства». В появившейся вкладке можно установить максимальный размер журнала и действия в случае его переполнения (рис. 33).

Установите размер журнала в минимально возможное значение – 64 КБ. Включите все возможные виды аудита.

Рисунок 32 – Настройка поиска записей журнала безопасности

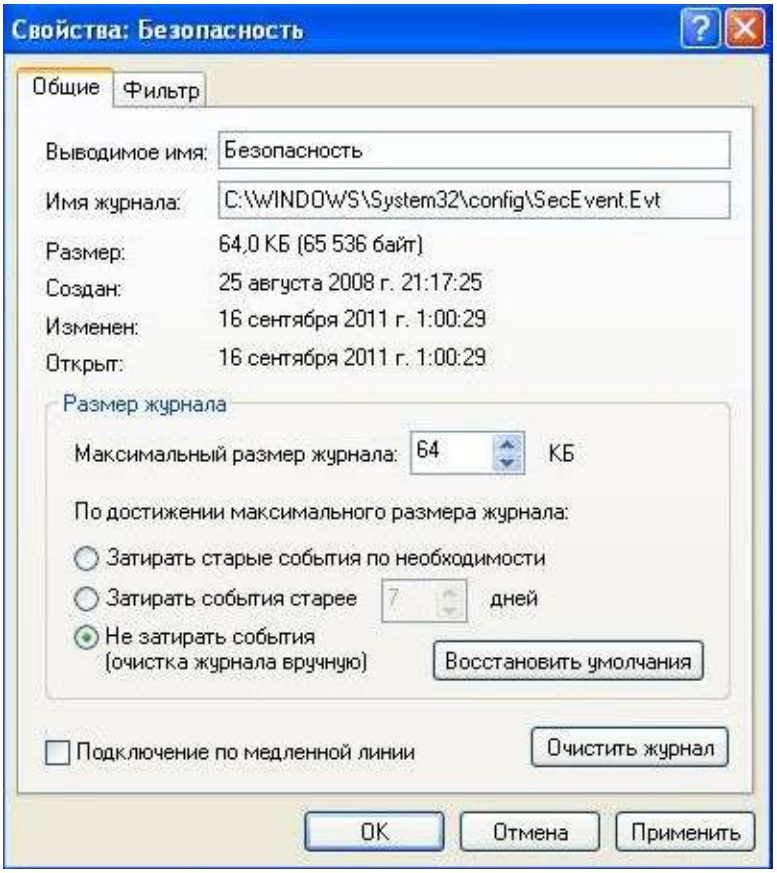


Рисунок 33 – Настройка работы журнала безопасности

Для установки запрета работы пользователя в случае переполнении журнала необходимо включить параметр «Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности» в разделе «Параметры безопасности» локальной групповой политики (рис. 34).

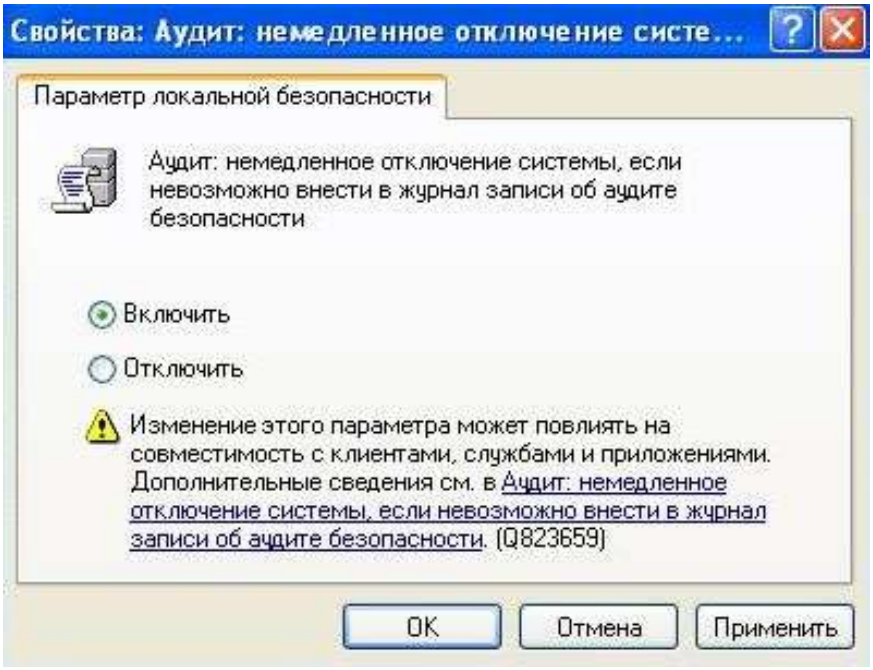


Рисунок 34 – Настройка действий при переполнении журнала безопасности

Перезагрузите операционную систему. Войдите под учётной записью «Администратор». Генерируйте новые записи аудита до тех пор, пока не произойдёт заполнение журнала и перезагрузка системы. После этого войдите в систему под учётной записью «Администратор» (рис. 35), сохраните журнал (рис. 36) и очистите его.

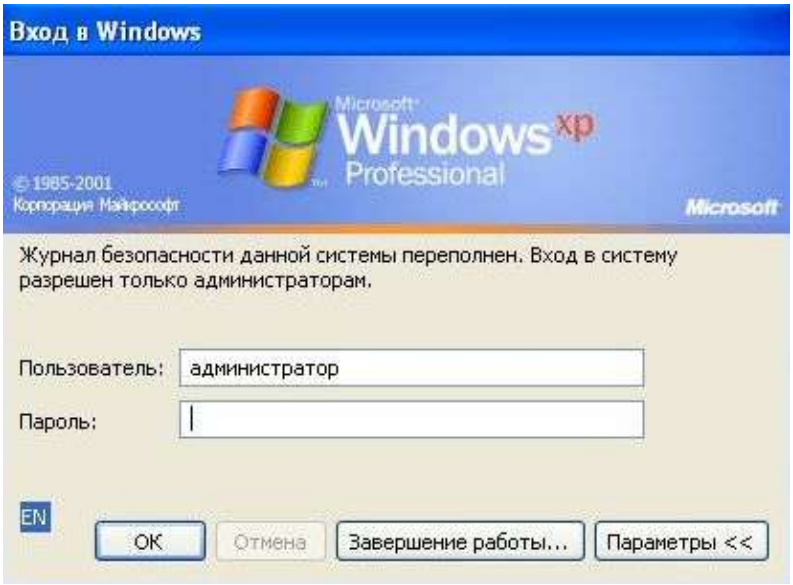


Рисунок 35 – Окно входа в систему при переполнении журнала безопасности

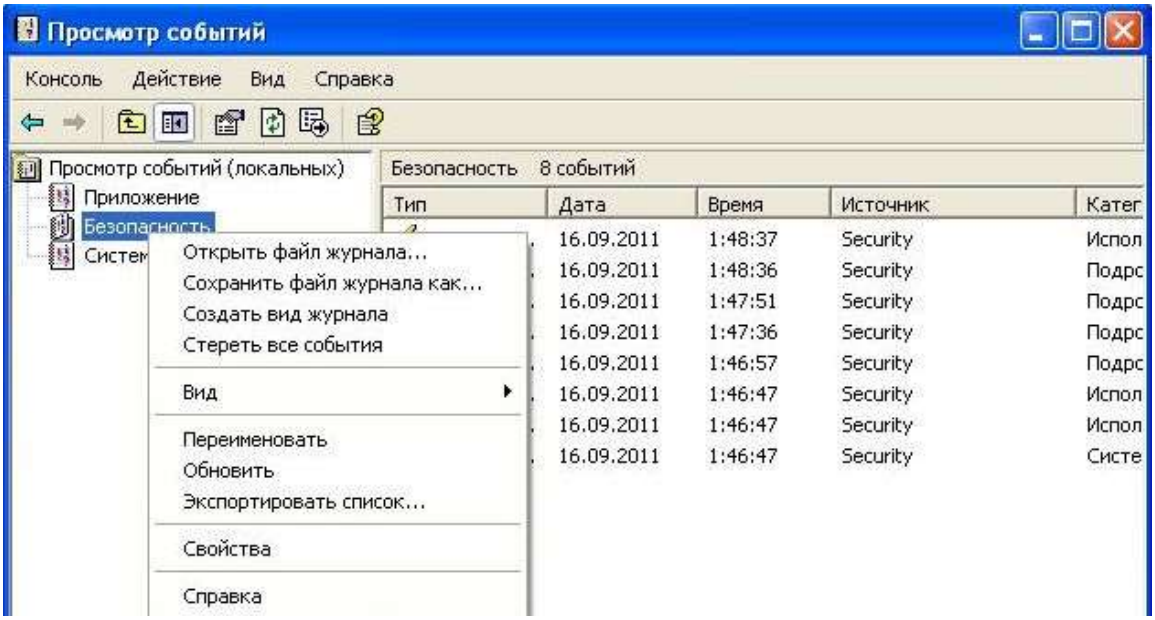


Рисунок 36 – Сохранение журнала безопасности

Просмотр сохранённых журналов безопасности осуществляется при помощи функции «Открыть файл журнала» контекстного меню журнала безопасности.

Задание

Импортируйте журнал безопасности в соответствии со своим вариантом. Проанализируйте журнал безопасности согласно распределению вариантов и определите виновных. Параметры аудита, использовавшиеся при фиксации событий, перечислены в табл. 2. Также включен параметр «Аудит прав на архивацию и восстановление». Правом управлять аудитом и журналом безопасности могут только «Администратор» и пользователь «Анатолий». Сведения об учётных записях перечислены в табл. 3.

Таблица 2 - Параметры политик аудита

Название параметра	Успех	Отказ
Аудит событий входа в систему	+	+
Аудит управления учётными записями	+	+
Аудит доступа к службе каталогов	-	-
Аудит входа в систему	+	+
Аудит доступа к объектам	+	+
Аудит изменения политики	+	+
Аудит использования привилегий	-	+
Аудит отслеживания процессов	-	-
Аудит системных событий	+	+

Таблица 3 - Учётные записи

Имя учетной записи	Должность, группа
Дмитрий	стажёр, пользователь
Геннадий	финансовый менеджер, пользователь
Василий	оператор пульта видеонаблюдения, пользователь
Администратор	технический консультант, администратор системы
Валерий	директор, оператор архива
Людмила	бухгалтер, пользователь
Татьяна	секретарь, пользователь
Артур	помощник технического консультанта, пользователь
Анатолий	администратор безопасности, администратор системы
ДАВЫДОВ	руководитель отдела разработки, пользователь

Вариант 1

Администратор безопасности Анатолий предоставил полный доступ к материалам по безопасности отдела только стажеру Дмитрий. Эти материалы были размещены на сетевом ресурсе «Ресурсы предприятия\Обмен\Дмитрию», к которому был заранее выставлен аудит чтения, записи, удаления, а также смены владельца. При утилизации документации Анатолий обнаружил распечатанные копии этих материалов. Стажер утверждает свою непричастность к распечатанным копиям важных документов. Докажите или опровергните причастность Дмитрия к распечатанным документам.

Вариант 2

На предприятии есть сетевой ресурс «Ресурсы предприятия\Конкурентоспособность основного продукта», в котором находились два документа «Продукты конкурентов.doc» и «Стратегия развития основного продукта.doc». Доступ на запись и чтение имели только следующие пользователи: «Геннадий» и «ДАВЫДОВ». Администратор безопасности Анатолий ранее настроил для этого ресурса аудит успехов и отказов удаления, чтения, записи, смены разрешений и смены владельца. Вскоре финансовый менеджер и руководитель отдела разработки сообщили об исчезновении этих документов. Выясните, кто причастен к удалению этих документов?

Вариант 3

Администратор системы неоднократно сообщал о действиях в системе, выполняемых кем-то под его учетной записью, включая смену паролей пользователей. Администратор безопасности посчитал необходимым настроить полный аудит ветви реестра, хранящий учетные записи и их пароли в неявном виде. Ветвь реестра, хранящая базу данных учетных записей, имеет следующий путь: «HKEY_LOCAL_MACHINE\SAM\SAM». Выясните, кто и какой программой получает доступ к базе данных учетных записей.

Вариант 4

Из организации, по собственному желанию, уволился системный администратор, не проработав и одной рабочей недели. По прошествии нескольких дней оператор пульта видеонаблюдения сообщил о странном поведении компьютера: «Компьютер самопроизвольно заблокировался, отобразив окно блокировки пользователем MS_Support_tech567». Выясните причину блокировки.

Вариант 5

В сетевых ресурсах предприятия дополнительной мерой защиты при обмене значимыми электронными документами между сотрудниками является установка пароля. Секретарь оповестила администратора безопасности о недейственности таких мер защиты, приведя в пример редактированный документ «Отчет деятельности сотрудников на апрель.doc» по сравнению с сохранившимся оригиналом. Администратор безопасности настроил аудит чтения на сетевой ресурс «C:\Ресурсы предприятия\Обмен» с применением наследования параметров аудита для создаваемых в нем файловых объектов. Проведите аудит файловых объектов этого ресурса на факт подбора пароля к ним.

Вариант 6

В предприятии имеется доступ к сети интернет, настроенный только для работы с почтовыми серверами. Приходящие счета за предоставления доступа к сети интернет не соизмеримы с объемом трафика, получаемого по почтовым протоколам. Директор потребовал администратора безопасности выяснить причину таких затрат. Проведите аудит запущенных пользователями программ, которые могли получать большой объем данных из сети интернет.

Вариант 7

Администратор безопасности ответственен за лицензионное ПО, используемое в компьютерах организации. Поэтому он должен отслеживать доступ к информации, приводящий к краже закрытой

информации лицензионного ПО, такой как 25-тизначный ключ продукта Windows. Большинство такой информации хранится в ветвях реестра, к которым применим аудит чтения. Проведите аудит журнала безопасности на факт чтения значений ветвей реестра лицензионных программ, а также используемые программы.

Вариант 8

Директор организации использует встроенные средства резервирования для файла «База данных заказов.doc», архив которого он сохраняет в папку «C:\АРХИВ\backup», к которому только он имеет доступ. Служба внутренней безопасности организации сообщила об отфильтрованном электронном письме с поддельным адресом отправителя, не значившимся в списке разрешенных отправителей. Текст письма содержал предложение о продаже информации и список электронных документов, в число которых входил архивируемый директором файл. Администратору безопасности было поручено разобраться проблемами утечки информации, в число которых входит вопрос выявления способа получения ограниченных в доступе файлов. Выясните, кто и как получил ограниченный в доступе файл.

Вариант 9

Администратор безопасности посчитал необходимым провести аудит неблагонадежных сотрудников организации. Для этого он открыл доступ к документу «зарплата сотрудников на 30.04.09.doc», назначив аудит чтения и записи. Выявите неблагонадежных пользователей, которые редактировали этот файл.

Вариант 10

Администратор пожаловался на наличие в компьютерах организации нежелательного ПО (компьютерные игры), которое регулярно появляются вновь, включая то, которые требуют для установки права локального администратора. Проведите аудит, чтобы выяснить пользователей, обладающих паролем локального администратора.

Контрольные вопросы

1. Какие данные фиксируются при аудите входа/выхода в систему?
2. Чем отличается аудит входа в систему от аудита событий входа в систему?
3. Какие данные фиксируются при аудите управления учётными записями?
4. Какие данные фиксируются при аудите изменения политики?
5. Какие данные фиксируются при аудите использования прав?
6. Какие данные фиксируются при аудите системных событий?

7. Какие данные фиксируются при аудите отслеживания процессов?

8. Какие типы объектов могут подвергаться фиксации при аудите доступа к объектам? Какие при этом фиксируются данные?

9. Каким образом происходит настройка аудита доступа к объектам?

10. Какие существуют настройки политики безопасности, связанные с аудитом?

Лабораторная работа № 5
Анализ, настройка и контроль целостности параметров безопасности подсистем защиты

Целью данной работы является ознакомление с встроенными в операционную систему Windows XP возможностями по оценке текущего состояния подсистемы безопасности и контролю целостности настроек безопасности.

Оценка текущего состояния проводится на основе сравнения текущих значений параметров безопасности с эталонными. Применение эталона позволяет автоматизировать настройку безопасности операционной системы и дальнейший контроль установленного уровня безопасности.

В операционной системе Windows XP для работы с текущими и эталонными настройками безопасности предназначены оснастки «Шаблоны безопасности» и «Анализ и настройка безопасности».

Ход работы

Войдите в операционную систему под учётной записью «Администратор». Откройте Microsoft Management Console («Пуск – Выполнить» и введите команду «mmc») и добавьте оснастки «Анализ и настройка безопасности» и «Шаблоны безопасности».

1. Структура шаблона безопасности

Шаблон безопасности – набор эталонных настроек операционной системы, влияющих на информационную безопасность. В Windows XP существует набор встроенных шаблонов безопасности. По умолчанию встроенные шаблоны безопасности расположены в каталоге C:\Windows\security\templates\. Просмотр и редактирование настроек, входящих в шаблон, осуществляется через оснастку «Шаблоны безопасности» (рис. 1).

Ниже приведён перечень встроенных шаблонов безопасности и их краткое описание.

а). Безопасность по умолчанию (Setup security.inf) – содержит параметры безопасности, которые применяются по умолчанию во время установки операционной системы, включая разрешения для файлов корневого каталога системного диска. Этот шаблон можно использовать полностью или частично в целях аварийного восстановления.

б). Совместимый (Compatws.inf) – содержит разрешения по умолчанию для рабочих станций и серверов (не контроллеров домена). Учитывается иерархия прав локальных групп: "Администраторы", "Опытные пользователи" и "Пользователи".

в). Защита (Securews.inf и Securedc.inf) – шаблоны для настройки рабочих станций (ws – workstations) и контроллеров домена (dc – domain controllers). В них определяются параметры повышенной безопасности: определяются параметры надёжных паролей, блокировки и аудита; правила работы с протоколом NTLM; определяются дополнительные ограничения для анонимных пользователей.

г). Повышенная защита (Hisecws.inf и Hisecdc.inf) – шаблоны повышенной защиты для рабочих станций и контроллеров домена, налагающие дополнительные ограничения на уровни кодировки и подписи, необходимые для проверки подлинности и для данных, передаваемых по безопасным каналам между клиентами SMB и серверами.

д). Безопасность системного корневого каталога (Rootsec.inf) – включает разрешения, по умолчанию применяемые для корневого каталога системного диска.

Каждый шаблон состоит из следующих разделов (рис. 1):

– Политики учётных записей;
– Локальные политики;
– Журнал событий;
– Группы с ограниченным доступом;
– Системные службы;
– Реестр;
– Файловая система.

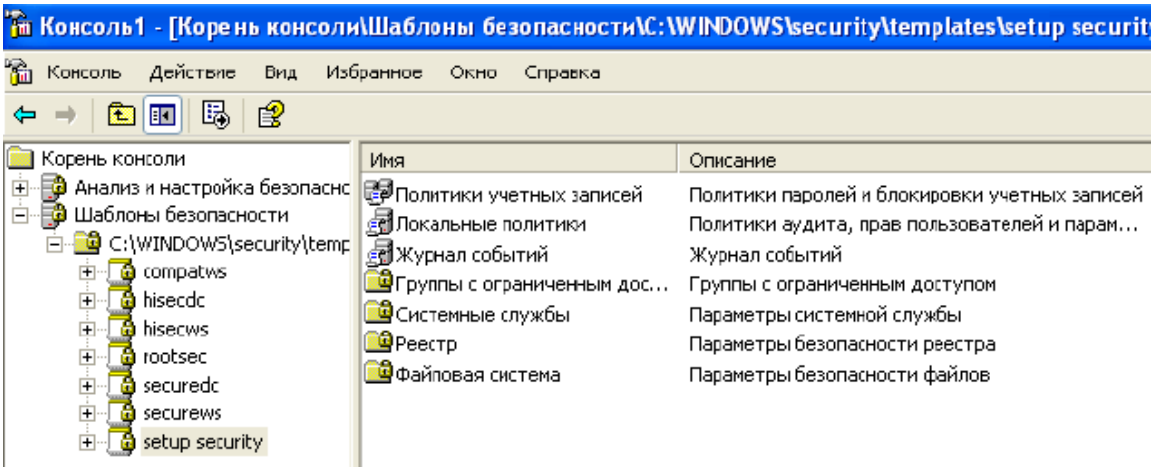


Рисунок 1 – Структура шаблона безопасности

Дальнейшее рассмотрение структуры шаблона и изменение его настроек осуществляется на основе встроенного шаблона «setup security».

Разделы «Политики учётных записей» и «Локальные политики» включают в себя все параметры аналогичных разделов «Групповой политики». Измените значение минимальной длины пароля на 6

символов в разделе «Политики учётных записей» – «Политика паролей» (рис. 2). Добавьте группу «Пользователи» в параметре «Управление аудитом и журналом безопасности» раздела «Локальные политики» – «Назначение прав пользователя» (рис. 3).

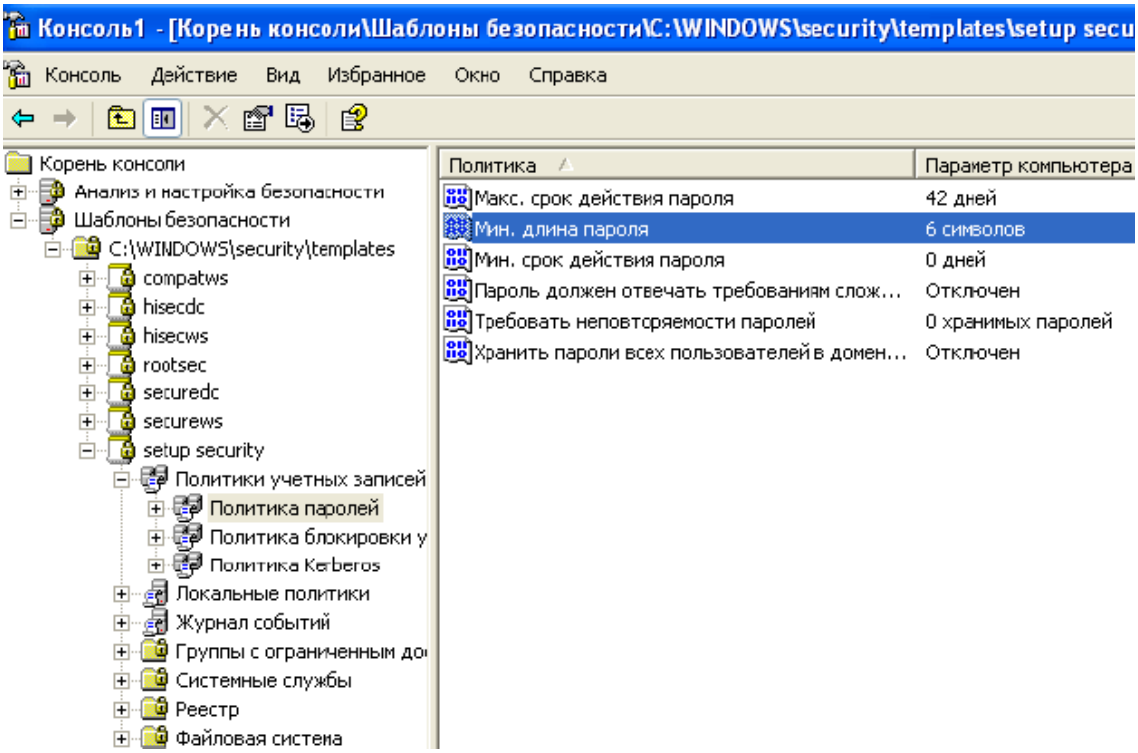


Рисунок 2 – Изменение параметра в разделе «Политики учётных записей»

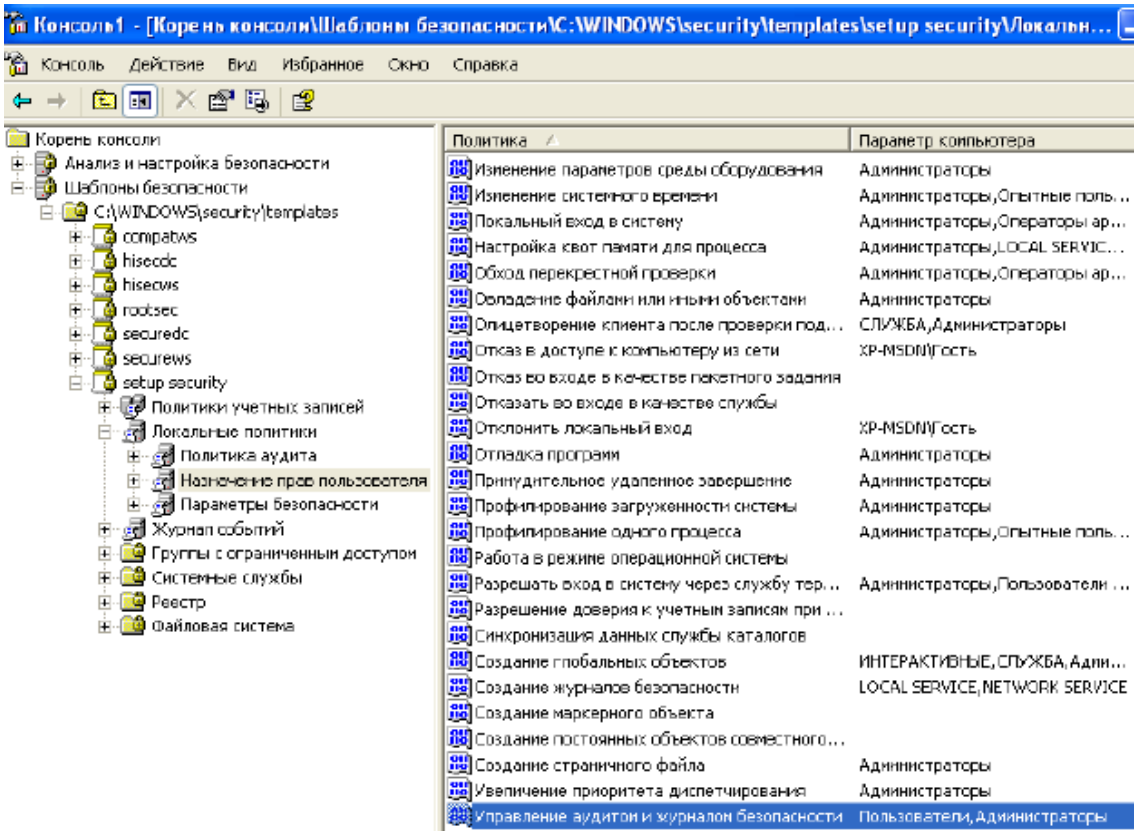


Рисунок 3 – Изменение параметра в разделе «Локальные политики»

Раздел «Журнал событий» включает настройки правил работы с журналами аудита. Разрешите доступ локальной группе гостей к журналу безопасности (рис. 4).

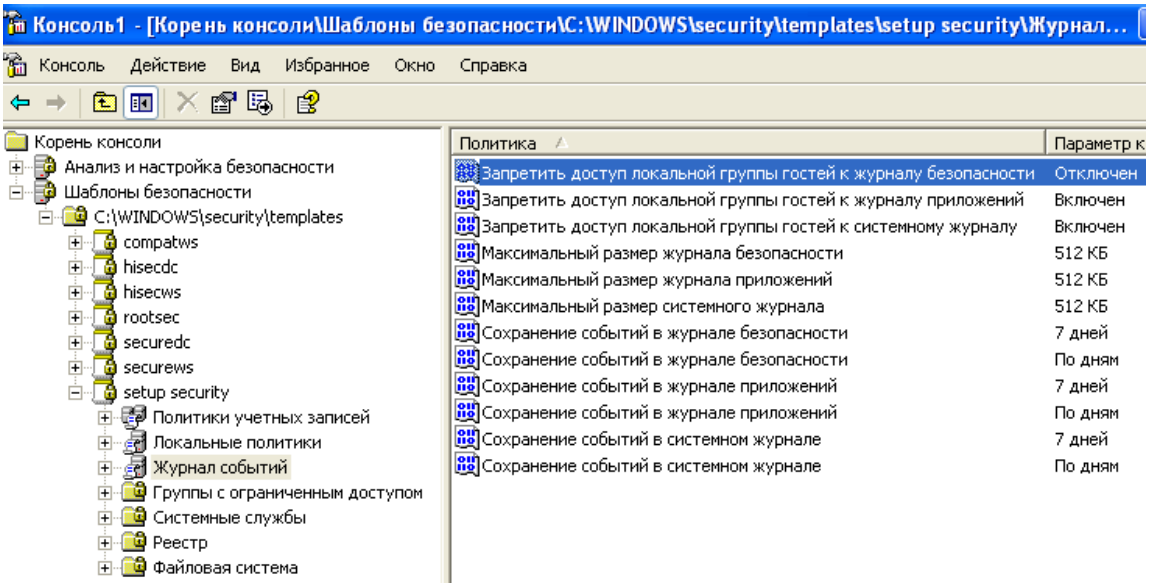


Рисунок 4 – Изменение параметра в разделе «Журнал событий»

Раздел «Группы с ограниченным доступом» позволяет настраивать состав групп пользователей. При помощи контекстного меню добавьте в список группу «Администраторы» и в качестве члена группы добавьте пользователя «user» (рис. 5).

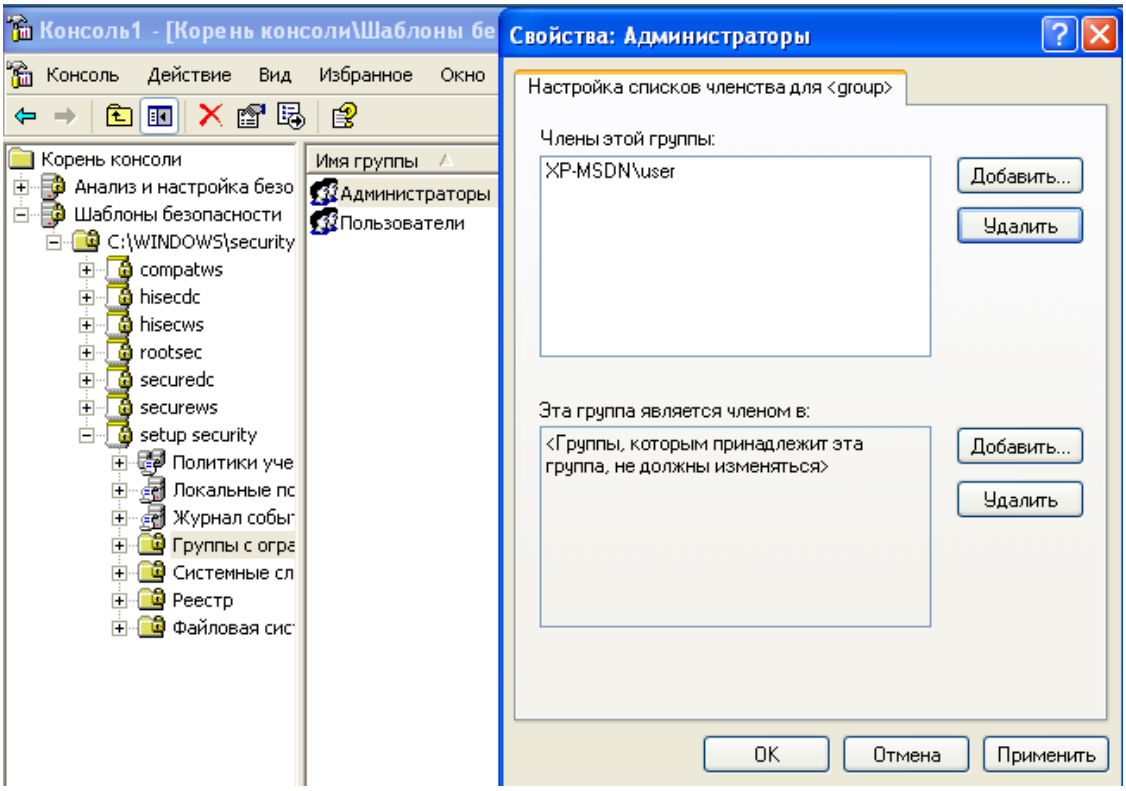


Рисунок 5 – Изменение параметра в разделе «Группы с ограниченным доступом»

Раздел «Системные службы» содержит настройки по запуску служб и разграничению доступа к управлению ими. Запретите запуск службы «Диспетчер очереди печати» (рис. 6). Эта служба запускается как процесс с именем spoolsv.exe.

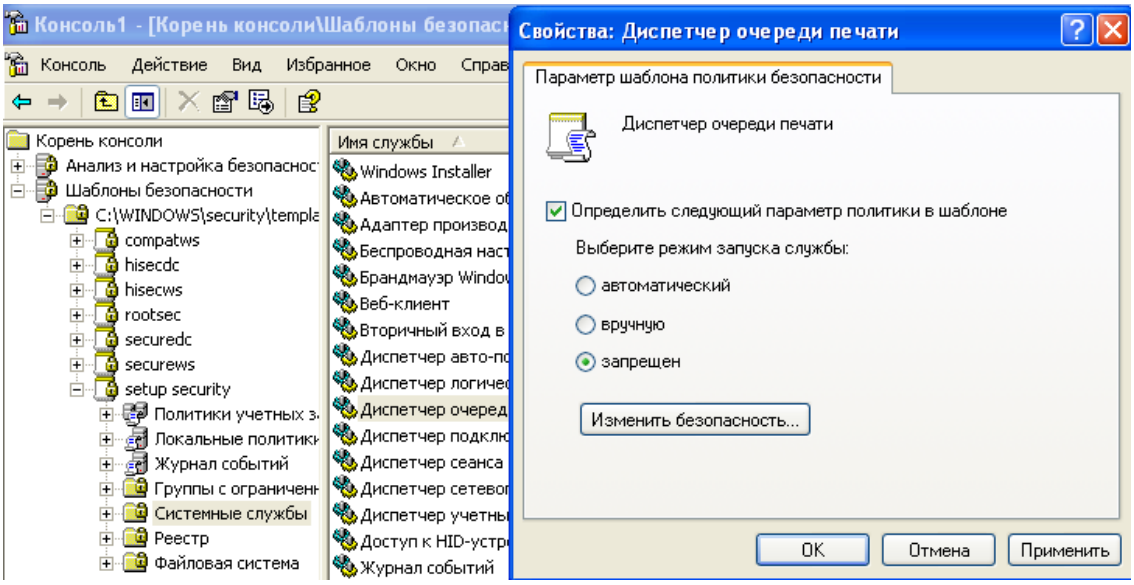


Рисунок 6 – Изменение параметра в разделе «Системные службы»

Раздел «Реестр» содержит правила разграничения доступа к основным ветвям реестра: software, system, users. Настройте доступ к разделу HKEY_LOCAL_MACHINE\SOFTWARE (рис. 7), разрешив полный доступ к нему группе «Опытные пользователи» (рис. 8).

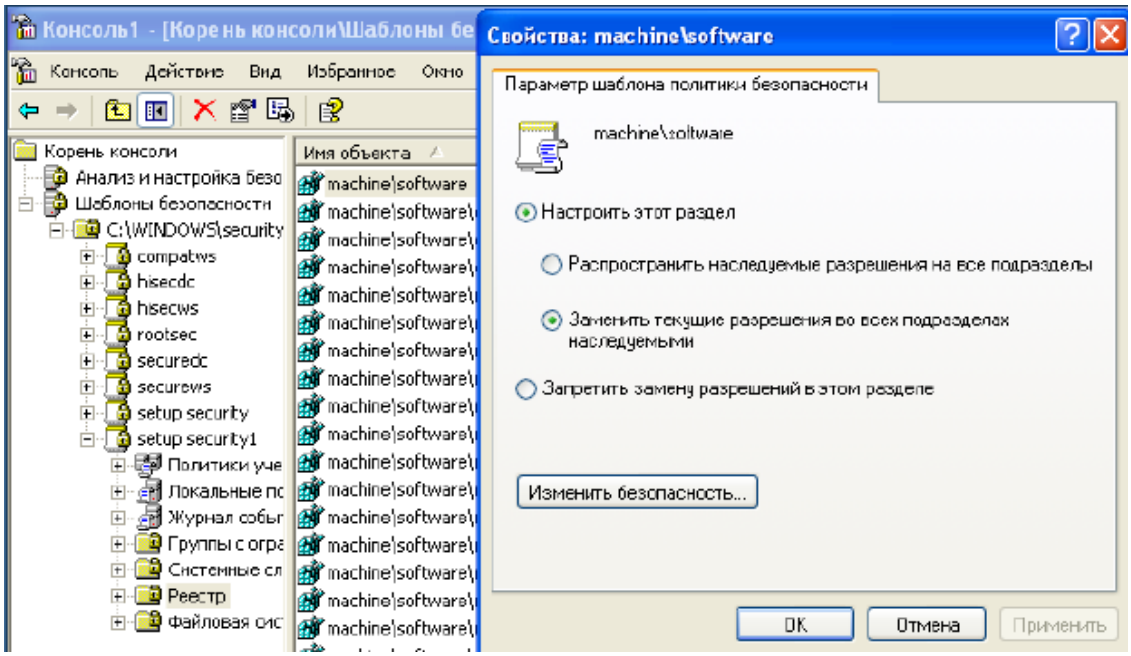


Рисунок 7 – Изменение параметра в разделе «Реестр»

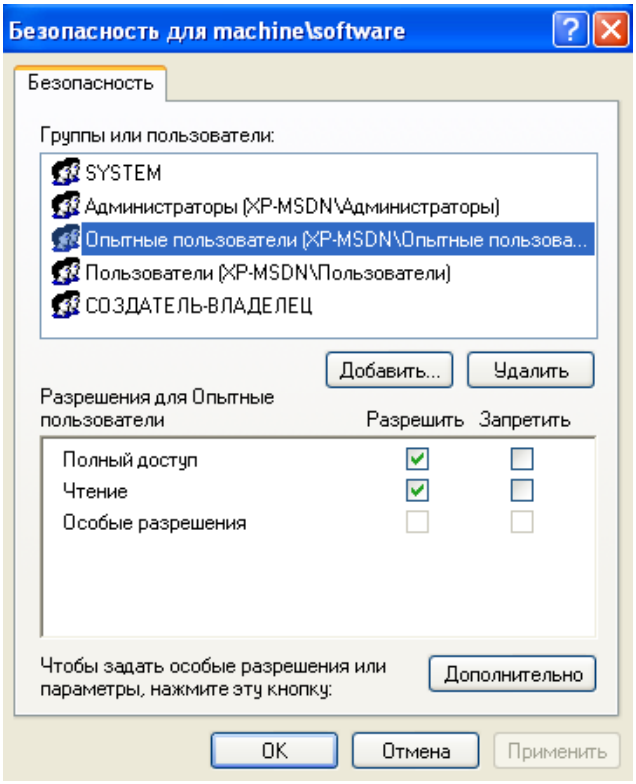


Рисунок 8 – Установка прав доступа к разделу реестра

Раздел «Файловая система» содержит правила разграничения доступа к каталогам на системном диске. Запретите всем пользователям доступ к «Косынке» («C:\WINDOWS\system32\sol.exe», рис. 9-10).

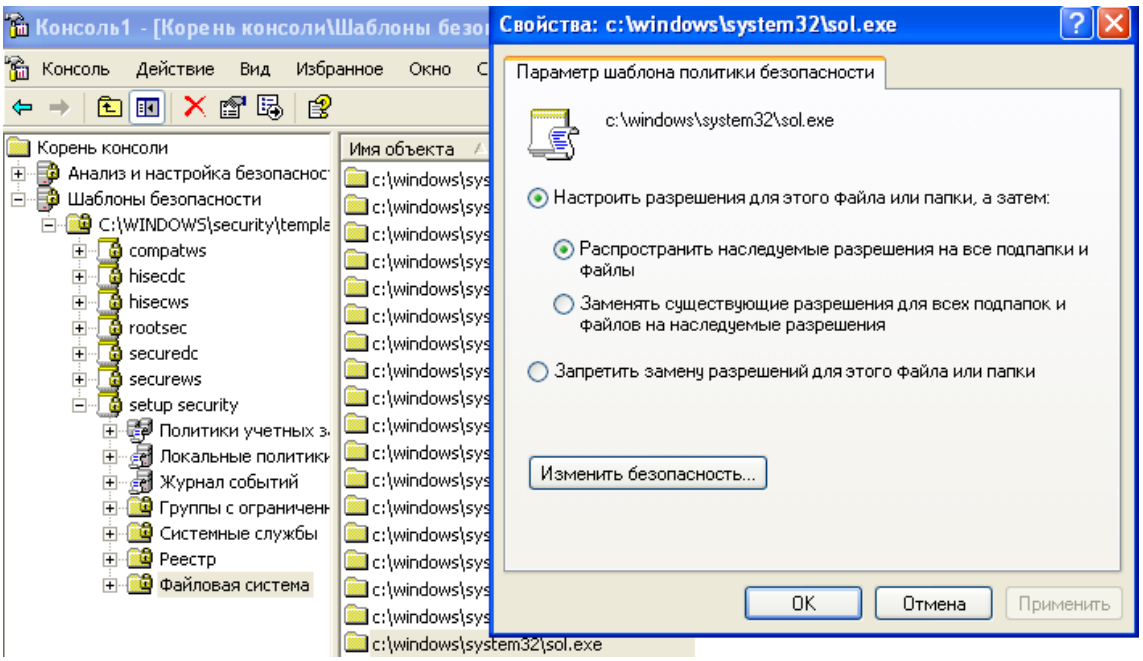


Рисунок 9 – Изменение параметра в разделе «Файловая система»

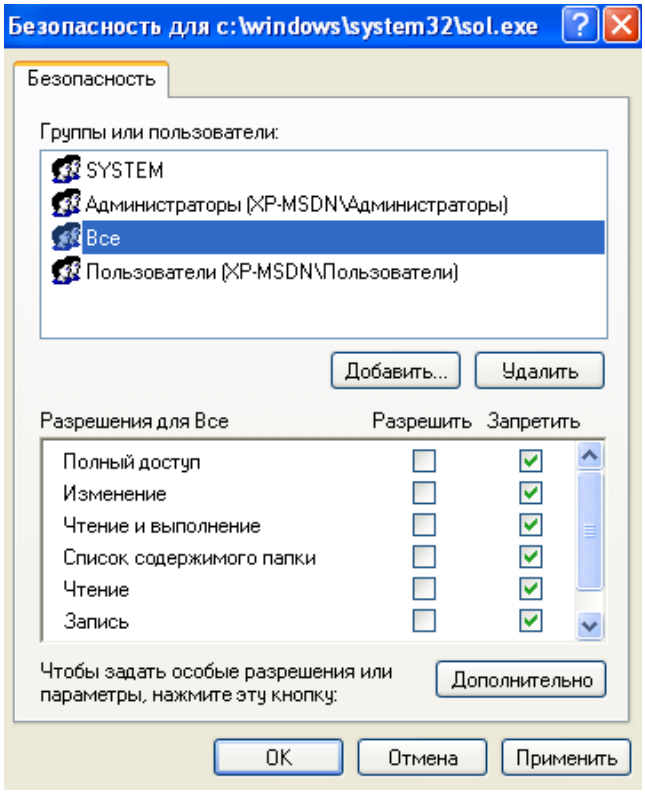


Рисунок 10 – Установка прав доступа к файлу

2. Управление шаблонами безопасности

В оснастке «Шаблоны безопасности» существует возможность создавать собственные шаблоны. Создать новый шаблон можно через контекстное меню каталога, содержащего шаблоны (рис. 11). При этом будет создан шаблон, у которого все параметры будут иметь значение «Не определено».

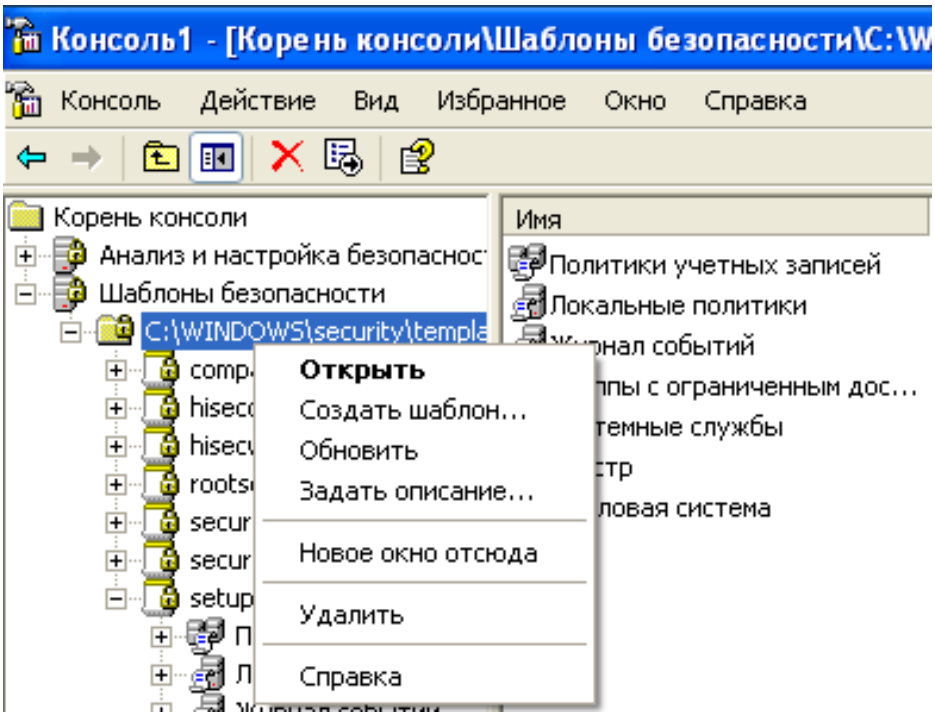


Рисунок 11 – Создание нового шаблона безопасности

Кроме того, собственный шаблон можно создать на основе существующего. Вызовите контекстное меню шаблона «setup security», выберите «Сохранить как…» (рис. 12) и сохраните шаблон под новым именем (например, «test»). При этом будет создан новый шаблон, включающий все сделанные ранее изменения значений параметров.

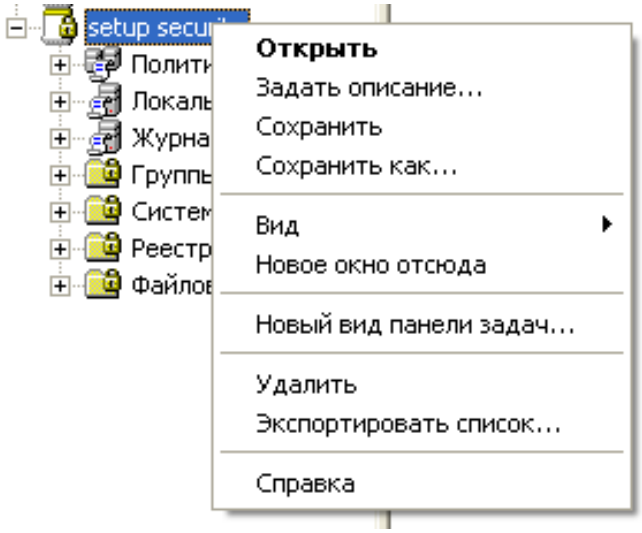


Рисунок 12 – Сохранение изменённого шаблона

3. Анализ параметров безопасности операционной системы

Вызовите контекстное меню оснастки «Анализ и настройка безопасности» (рис. 13), выберите пункт «Открыть базу данных…». Задайте имя для создаваемой базы данных эталонных настроек. После этого необходимо занести в базу значения параметров из интересующего шаблона. Выберите созданный шаблон (рис. 14).

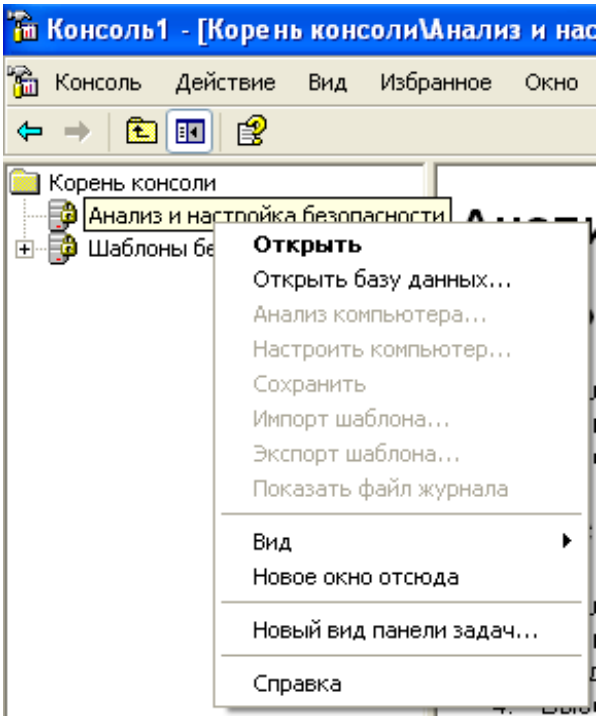


Рисунок 13 – Создание базы данных настроек безопасности

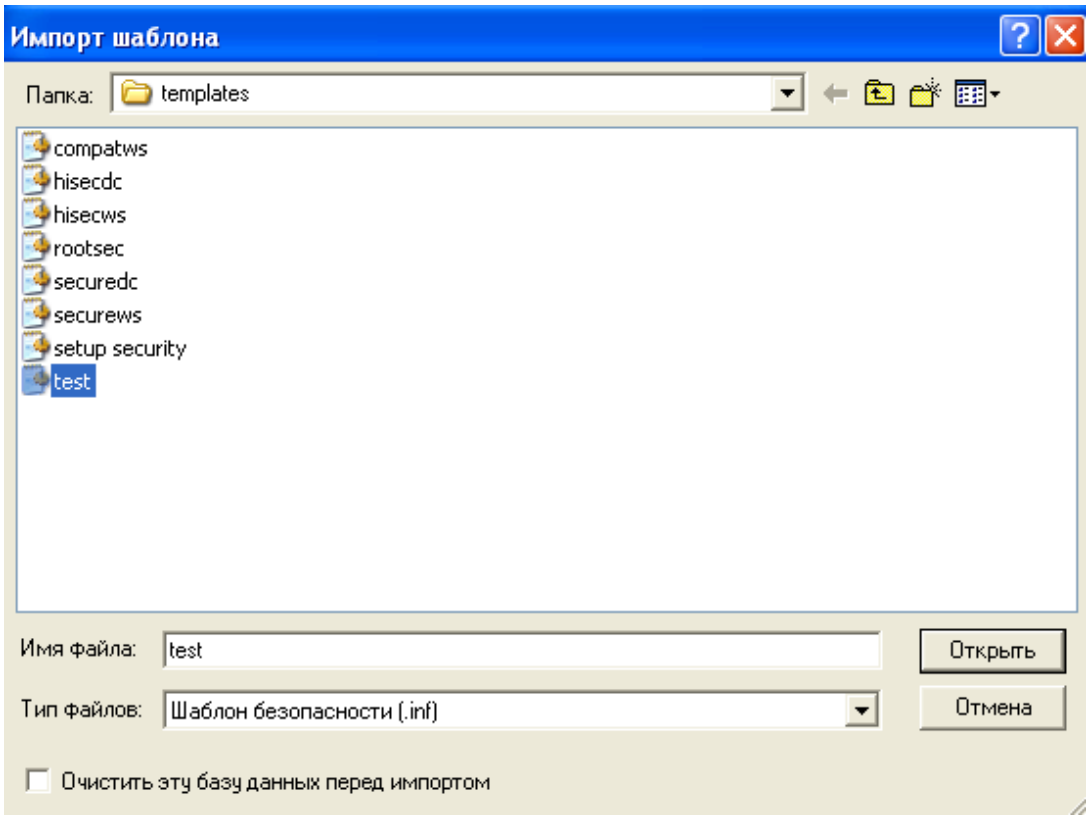


Рисунок 14 – Выбор шаблона для импорта в базу данных

Занесение в базу настроек из другого шаблона возможно через команду контекстного меню «Импорт шаблона» (рис. 15).

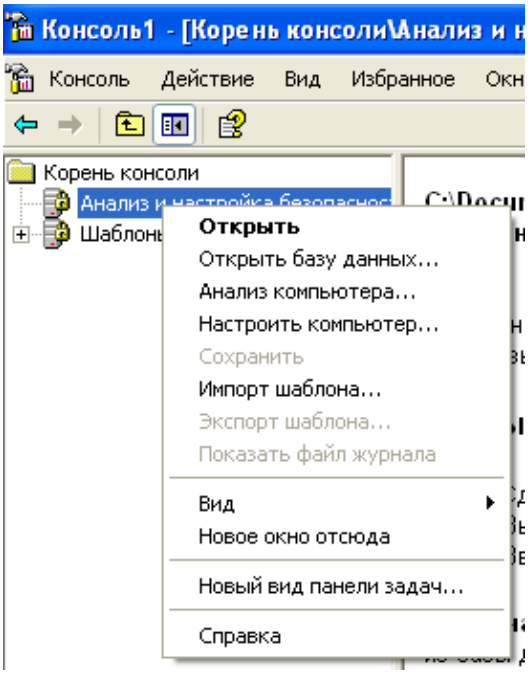


Рисунок 15 – Импорт шаблона

Выберите в контекстном меню оснастки пункт «Анализ компьютера…» и подтвердите предложенный путь к лог-файлу. После

этого начнётся анализ текущих настроек безопасности операционной системы (рис. 16). Результатом анализа является сравнение текущих (Параметр компьютера) и эталонных (Параметр базы данных) значений параметров безопасности. Структура представления результатов совпадает со структурой шаблона (рис. 17).

Результаты сравнения значений параметров представляются в виде специальных пиктограмм, находящихся рядом с названием каждого параметра (табл. 1).

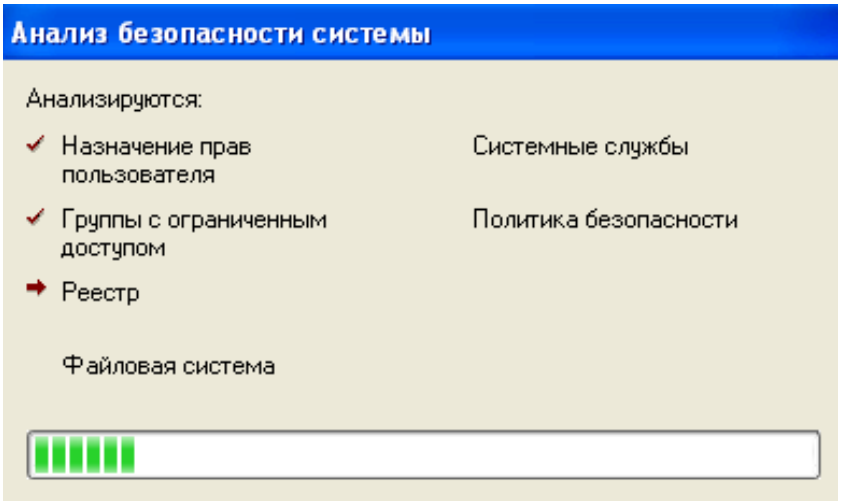


Рисунок 16 – Анализ настроек безопасности операционной системы

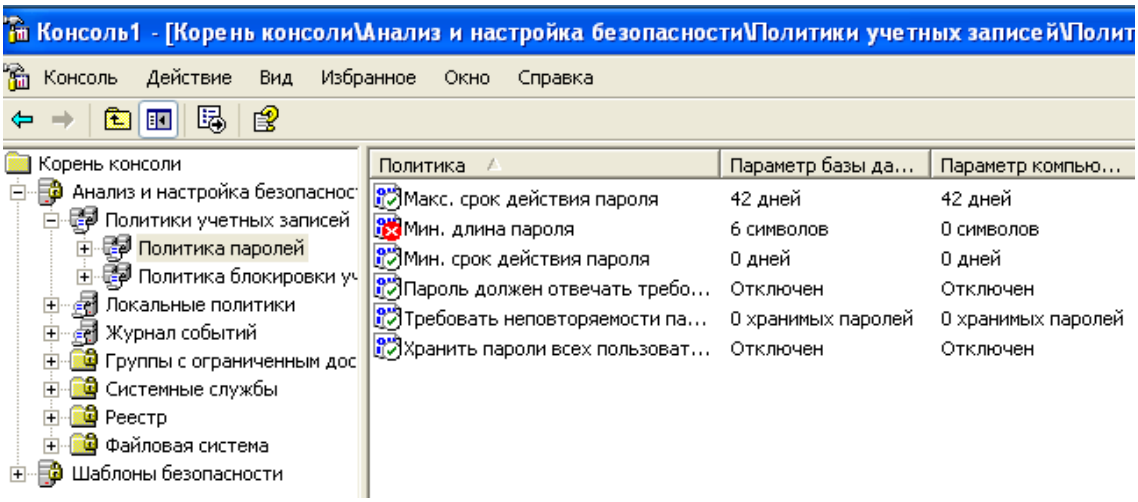


Рисунок 17 – Результат анализа безопасности операционной системы

Таблица 1 – Описание пиктограмм результатов анализа

Пиктограмма	Описание
	Элемент определён в базе данных анализа и в системе, но значения параметров безопасности не совпадают.
	Элемент определён в базе данных анализа и в системе; значения параметров безопасности совпадают.

	Элемент не анализировался. Возможно, он не был определён в базе данных анализа или пользователь, выполняющий анализ, не имеет достаточных разрешений на анализ данного объекта или области
	Элемент определён в базе данных анализа, однако, не существует в текущей конфигурации системы. Например, может существовать группа с ограниченным доступом, определённая в базе данных анализа и не существующая в анализируемой системе
	Элемент не определён в базе данных анализа или в системе

Удостоверьтесь, что в результате проведенного анализа изменённые параметры безопасности отмечены как несовпадающие.

Если какая-нибудь из текущих настроек системы предпочтительнее эталонной, то её можно занести в базу (рис. 18). Изменённую базу можно сохранить в качестве шаблона из контекстного меню оснастки, сохранив базу и выбрав пункт «Экспорт шаблона».

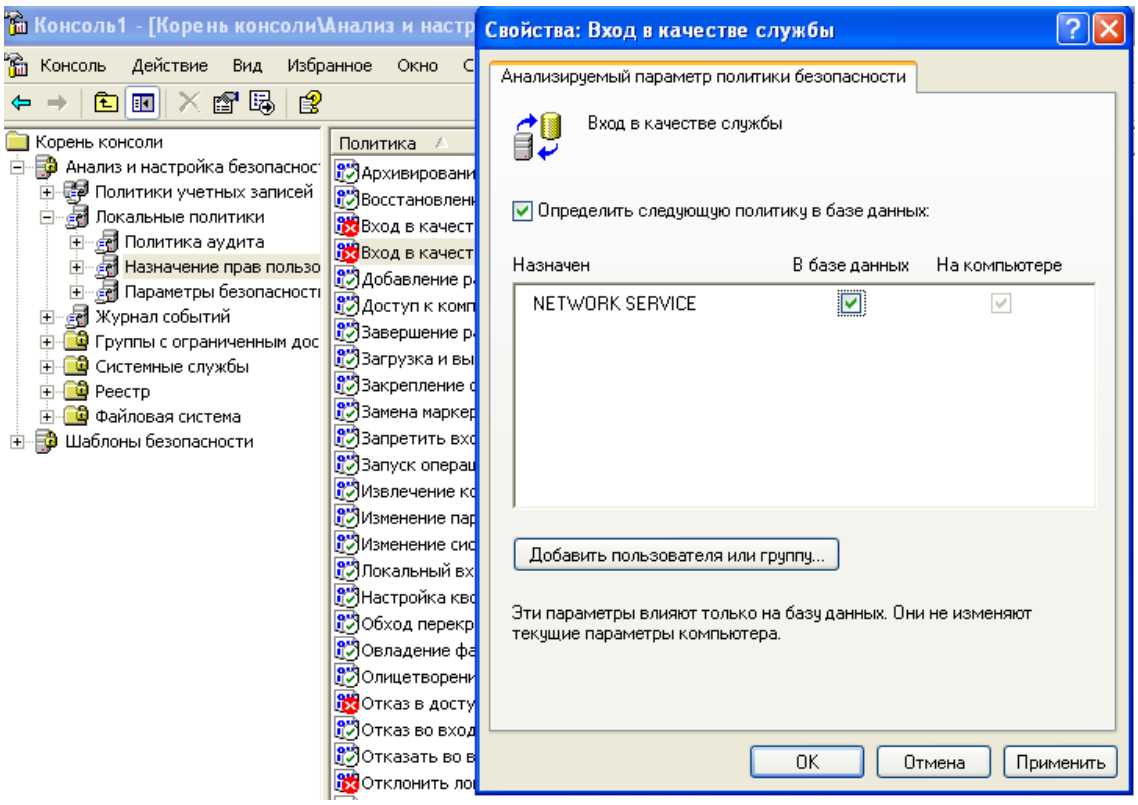


Рисунок 18 – Изменение настроек в базе данных

В итоге, был создан шаблон, в котором запрещён доступ к «Косынке», запрещён запуск службы «Диспетчер очереди печати» и пользователь с учётной записью «user» является членом группы «Администраторы». Проверьте текущее состояние этих настроек:

возможность запуска «Косынки», наличие запущенного процесса spoolsv.exe в «Диспетчере задач» и отсутствие пользователя «user» в группе «Администраторы».

4. Настройка параметров безопасности операционной системы

Вызовите контекстное меню оснастки «Анализ и настройка безопасности» и выберите пункт «Настроить компьютер…». После подтверждения пути к лог-файлу начнётся настройка операционной системы в соответствии со значениями параметров, указанных в базе данных (рис. 19).

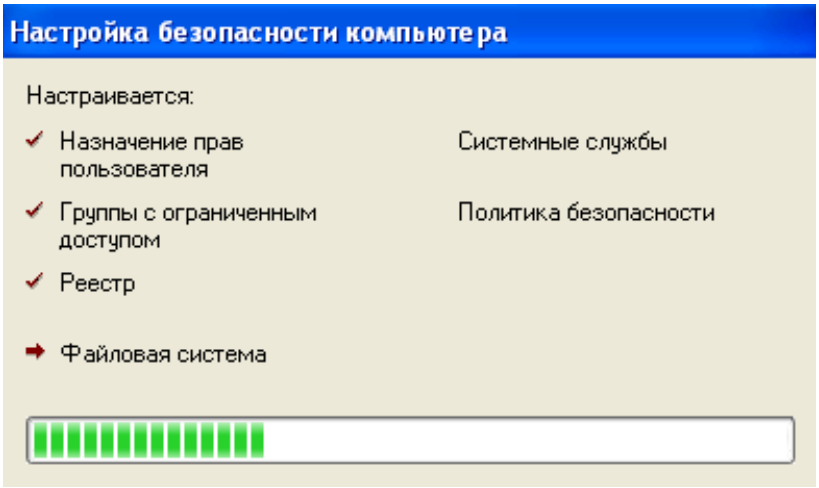


Рисунок 19 – Настройка параметров безопасности операционной системы

Проведите повторный анализ системы для проверки изменения несовпадавших параметров (рис. 20).

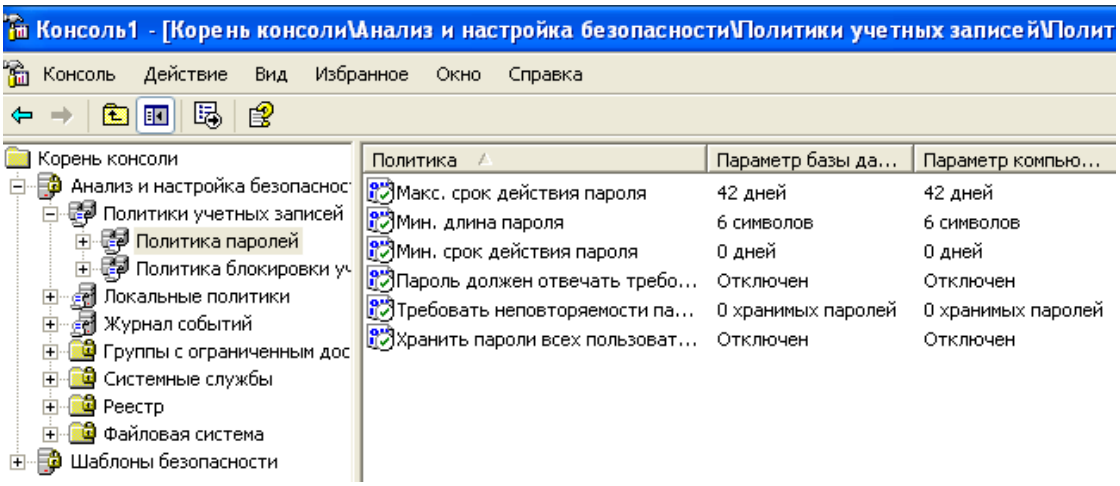


Рисунок 20 – Результат настройки параметров операционной системы

Удостоверьтесь в применении настроек, установленных в изменённом шаблоне: попытайтесь запустить «Косынку», проверьте отсутствие процесса spoolsv.exe в «Диспетчере задач» и наличие учётной записи «user» в группе «Администраторы».

Задание

Создайте шаблон безопасности в соответствии с Вашим вариантом и настройте операционную систему, используя созданный шаблон.

Вариант 1

Политики учётных записей	Политики учётных записей	Локальные политики
Минимальная длина пароля – 10 символов	Пороговое значение блокировки – 3 ошибки входа	Включите аудит отказов входа в систему

Вариант 2

Локальные политики	Журнал событий	Группы с ограниченным доступом
Запретите группе «Операторы архива» восстановление архивных файлов	Сохранение событий в журнале безопасности – вручную	Включите учётную запись «user» в группу «Операторы архива»

Вариант 3

Локальные политики	Журнал событий	Файловая система
Включите аудит доступа к объектам (успех и отказ)	Сохранение событий в журнале безопасности – 30 дней	Аудит создания файлов и записи данных (успех и отказ) на каталог C:\Windows и дочерние для учётной записи «user»

Вариант 4

Локальные политики	Локальные политики	Системные службы
Запретите отображение имени последнего пользователя при входе в систему	Включите обязательное нажатие Ctrl-Alt-Del при входе в систему	Автозапуск службы «Центр обеспечения безопасности»

Вариант 5

Локальные политики	Журнал событий	Группы с ограниченным доступом
Разрешите учётной записи «user» работу с журналом аудита	Максимальный размер журнала безопасности – 2 МБ	Включите учётную запись «user» в группу «Опытные пользователи»

Вариант 6

Политики учётных записей	Локальные политики	Системные службы
Включите применение требований к сложности паролей	Включите аудит управления учётными записями	Автозапуск службы «Автоматическое обновление»

Вариант 7

Локальные политики	Группы с ограниченным доступом	Файловая система
Запретите группе «Пользователи» завершение работы системы	В группу «Пользователи» добавьте пользователя «user» и исключите из неё группы «Интерактивные» и «Прошедшие проверку»	Запретите доступ к редактору реестра группе «Пользователи»

Вариант 8

Политики учётных записей	Локальные политики	Системные службы
Срок действия пароля – 90 дней	Запретите учётной записи «user» доступ к компьютеру из сети	Запретить запуск службы «Диспетчер сеанса справки для удалённого рабочего стола»

Вариант 9

Локальные политики	Группы с ограниченным доступом	Файловая система
Включите очистку файла подкачки при завершении работы системы	В группу «Пользователи» добавьте учётную запись «user» и исключите из неё группы «Интерактивные» и «Прошедшие проверку»	Запретите доступ к оснастке «Службы» (services.msc) группе «Пользователи»

Вариант 10

Локальные политики	Локальные политики	Файловая система
Запретите изменение системного времени группе «Опытные пользователи»	Включите аудит системных событий (успех и отказ)	Запретите учётной записи «user» доступ к оснастке «Просмотр событий» (eventvwr.msc)

Контрольные вопросы

1. Каким образом при помощи встроенных средств операционной системы Windows XP можно осуществлять контроль целостности настроек, связанных с информационной безопасностью?
2. Каким образом при помощи встроенных средств Windows XP можно автоматизировать настройку операционной системы в соответствии с требуемыми параметрами безопасности?
3. Что такое «Шаблон безопасности»?
4. Для чего предназначена оснастка «Шаблоны безопасности»?
5. Какие группы настроек входят в шаблон безопасности?
6. Для чего предназначена оснастка «Анализ и настройка безопасности»?
7. Опишите последовательность действий администратора при проведении анализа настроек безопасности операционной системы.
8. Опишите последовательность действий администратора при настройке безопасности операционной системы.
9. Приведите возможные типы результатов анализа параметров безопасности операционной системы.
10. Каким образом можно внести в шаблон текущие настройки безопасности операционной системы?

Лабораторная работа № 6
Криптографическая защита объектов файловой системы в ОС Windows

Цель работы

Целью данной работы является изучение штатного средства шифрования информации в операционных системах Microsoft Windows.

Краткие теоретические сведения

Наиболее действенный способ защиты файлов и содержащих их каталогов от несанкционированного доступа — это шифрование. В операционных системах Microsoft Windows штатным средством, служащим для этой цели, является шифрованная файловая система (Encrypting File System — EFS). Данное средство присутствует в операционных системах Microsoft Windows, начиная с Microsoft Windows 2000, за исключением базовых (домашних) версий (EFS присутствует в выпусках Professional, Enterprise, Ultimate).

EFS фактически представляет собой надстройку файловой системы NTFS, и является недоступной для разделов жесткого диска с файловой системой FAT32. Все этапы шифрования производятся при сохранении и открытии файла и проходят незаметно для пользователя.

Симметричный алгоритм шифрования, используемый EFS, зависит от версии операционной системы и выбранных настроек. Возможные варианты: 3DES, DESX, AES. Для шифрования каждого файла должен быть сгенерирован случайный ключ, называемый File Encryption Key (FEK). Секретность данного ключа, в свою очередь, обеспечивается с помощью асимметричного шифрования по алгоритму RSA, для чего используется открытый ключ пользователя, содержащийся в цифровом сертификате (рис. 1.1).

Когда пользователю необходимо получить доступ к содержимому зашифрованного файла, драйвер шифрованной файловой системы прозрачно для него расшифровывает FEK, используя закрытый ключ пользователя, а затем с помощью соответствующего симметричного алгоритма на расшифрованном ключе — сам файл (рис. 1.2).

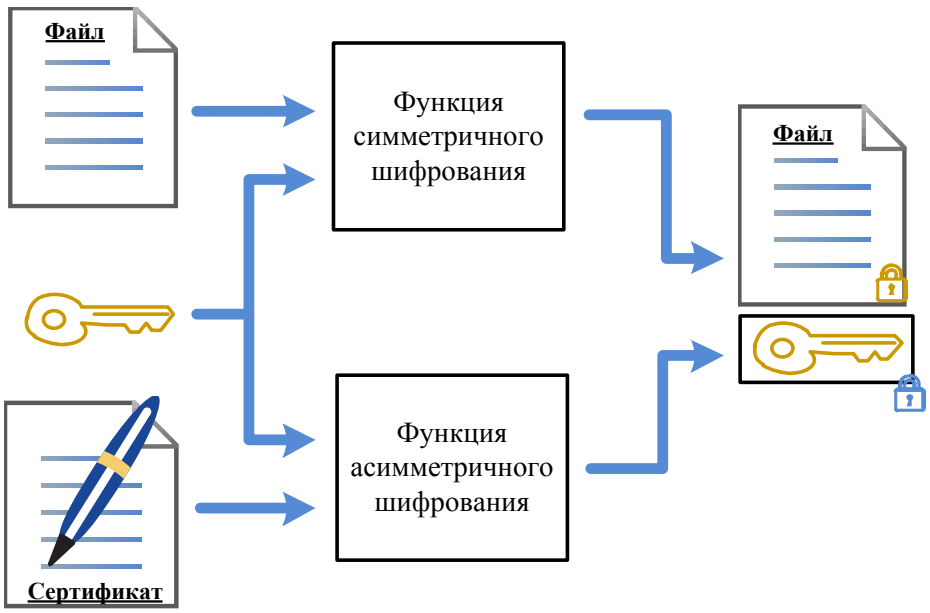


Рис. 1.1. Схема зашифрования файла

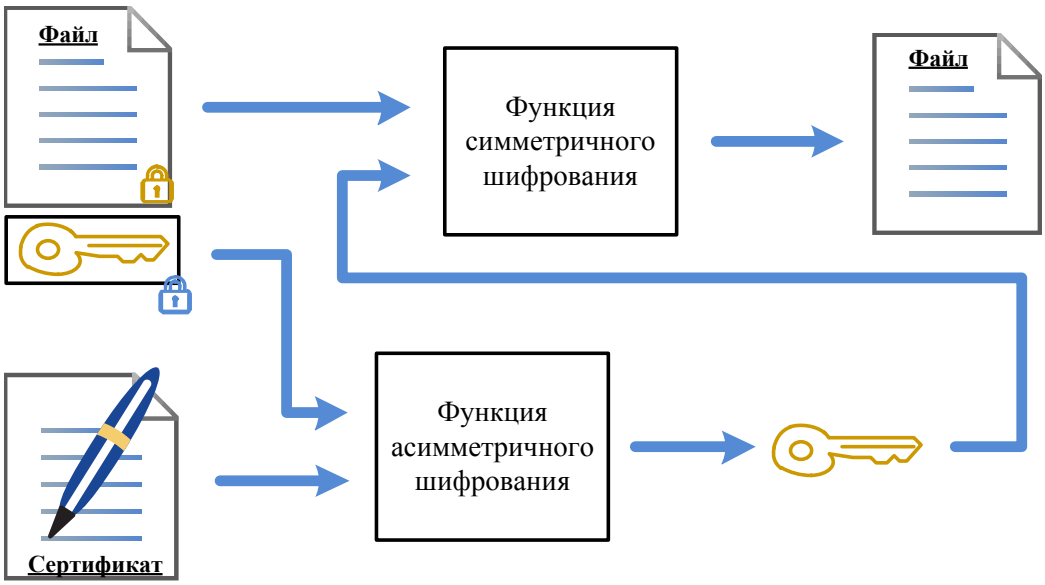


Рис. 1.2. Схема расшифрования файла

Войдя в систему под своей учетной записью, пользователь может работать с зашифрованными ранее файлами: просматривать их содержимое и редактировать. При добавлении новых файлов в зашифрованный каталог они также шифруются. Перемещение или копирование файла из зашифрованного каталога не приводит к автоматическому расшифрованию, при условии, что файл перемещается в раздел NTFS. Остальные пользователи не могут получить доступ к содержимому файлов.

При шифровании каталога, шифруются все находящиеся в нем файлы.

Порядок выполнения работы

Работа выполняется на виртуальной машине с установленной операционной системой Windows 7 Ultimate, для запуска которой используется программа VMware Player.

Прежде чем приступить к изучению шифрованной файловой системы Windows, необходимо выбрать файлы, с которыми будет вестись дальнейшая работа. Для этого на локальном диске виртуальной машины создайте два произвольных файла, например, два текстовых файла Файл№1.txt и Файл №2.txt (рис. 1.3). Каждому из них затем будут назначены свои параметры шифрования.

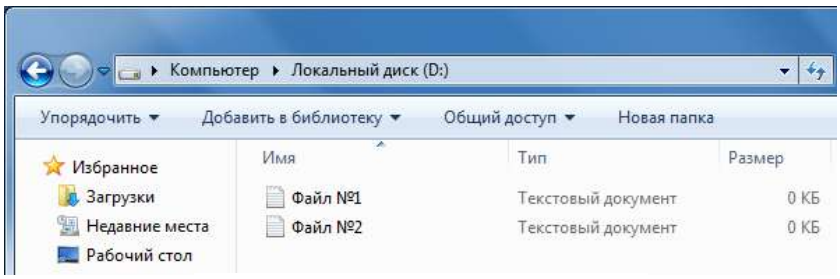


Рис. 1.3. Файлы для шифрования

Теперь зашифруем первый файл. Для этого необходимо выполнить следующие действия:

1) Вызвать контекстное меню нужного объекта (файла или папки) и выбрать пункт «Свойства».

2) Перейти на вкладку «Общие» и нажать кнопку «Другие», что приведет к открытию окна «Дополнительные атрибуты».

3) Активировать параметр «Шифровать содержимое для защиты данных» (рис. 1.4).

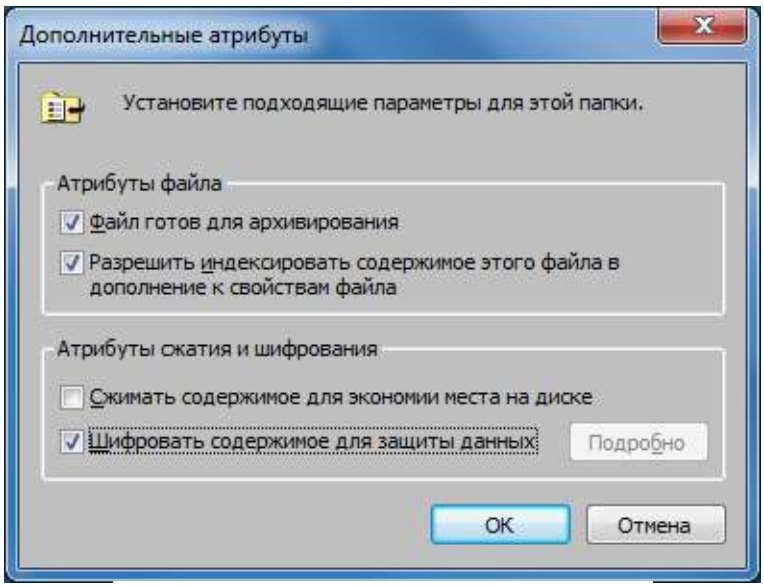


Рис. 1.4. Настройка шифрования файла

4) Закрыть оба окна при помощи кнопки «ОК».

Если шифрование было применено к отдельному файлу, который расположен не в корне локального диска, а в какой-либо папке, то система выдаст дополнительный запрос на запуск шифрования только данного файла или всей папки, в которой этот файл расположен (рис. 1.5).

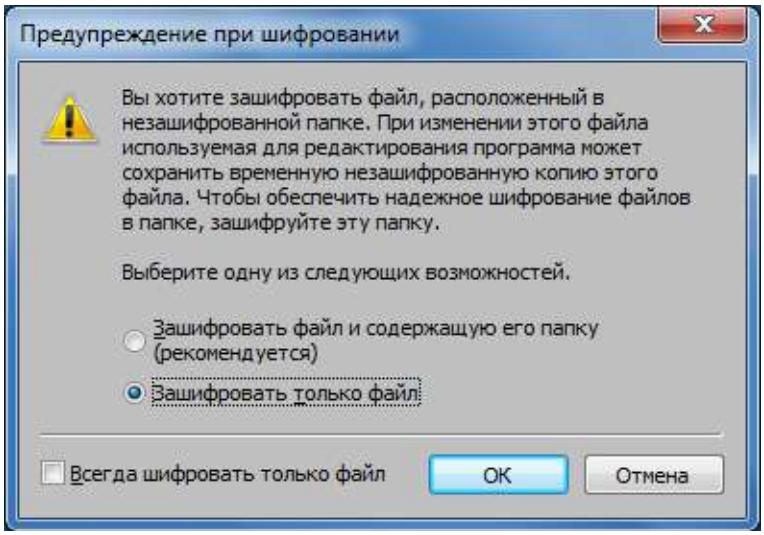


Рис. 1.5. Дополнительный запрос при шифровании файла

Если шифрование было применено к папке, то система выдаст дополнительный запрос на запуск шифрования всего каталога (рис. 1.6).

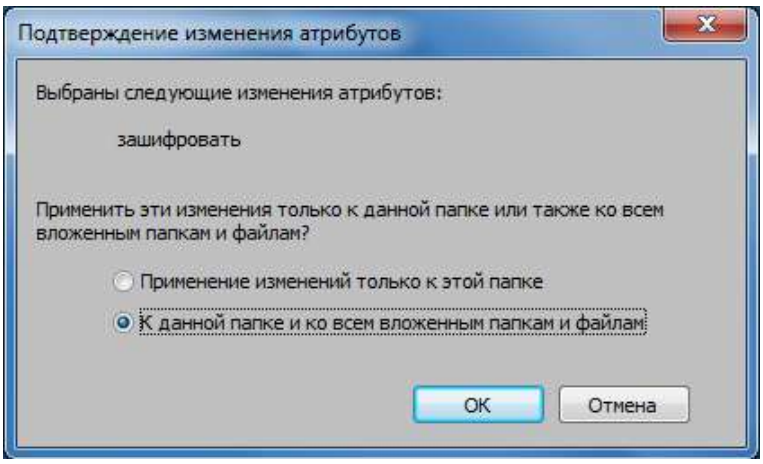


Рис. 1.6. Дополнительный запрос при шифровании папки

После этого файл (папка с файлами) будет зашифрован, а название файла станет отображаться зелёным цветом (рис. 1.7). Если нужно отключить шифрование, то необходимо снова открыть панель «Дополнительные атрибуты» и отключить параметр «Шифровать содержимое для защиты данных».

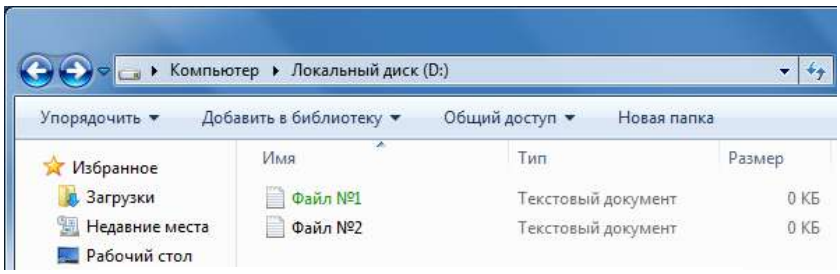


Рис.7. Вид файла с включенным шифрованием

При первой настройке функции шифрования отобразится предложение о создании архивной копии сертификата и ключа шифрования (рис. 1.8). Данную процедуру обязательно необходимо произвести, поскольку есть шанс потерять зашифрованные файлы, например, после переустановки системы или удаления учетной записи.

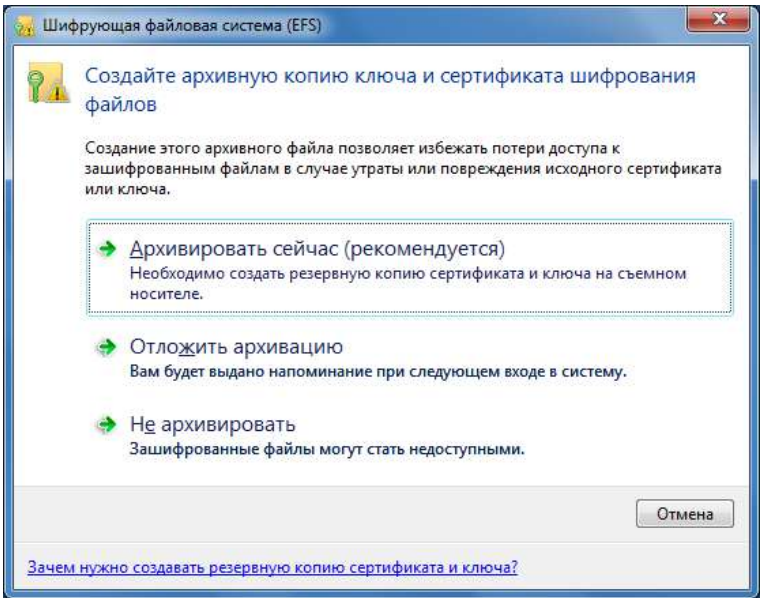


Рис. 1.8. Предложение о создании архивной копии ключа и сертификата

Для этого выберите пункт «*Архивировать сейчас (рекомендуется)*», после чего появится окно мастера экспорта сертификатов (рис. 1.9).

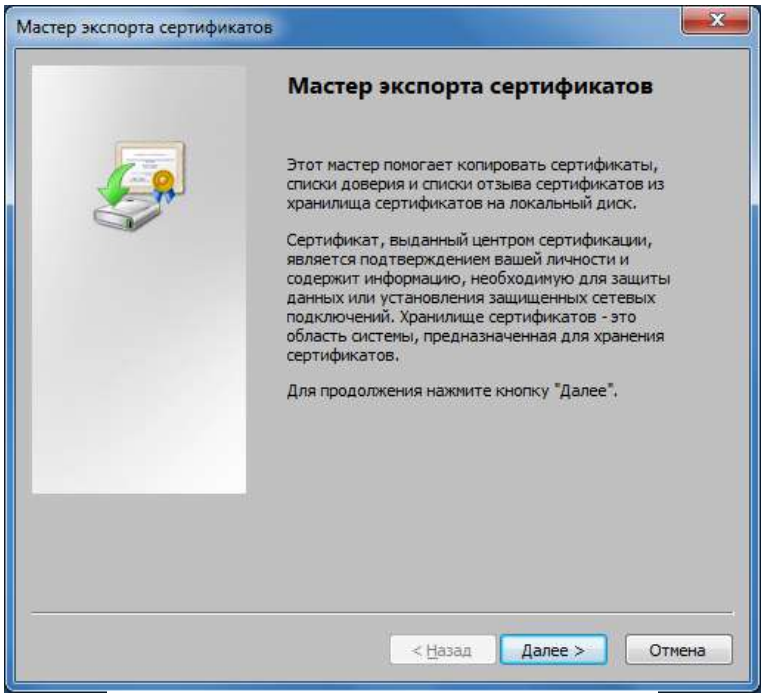


Рис. 1.9. Мастер экспорта сертификатов

Нажмите «Далее», в следующем окне также нажмите «Далее», не изменяя никаких параметров (рисунок 1.10).

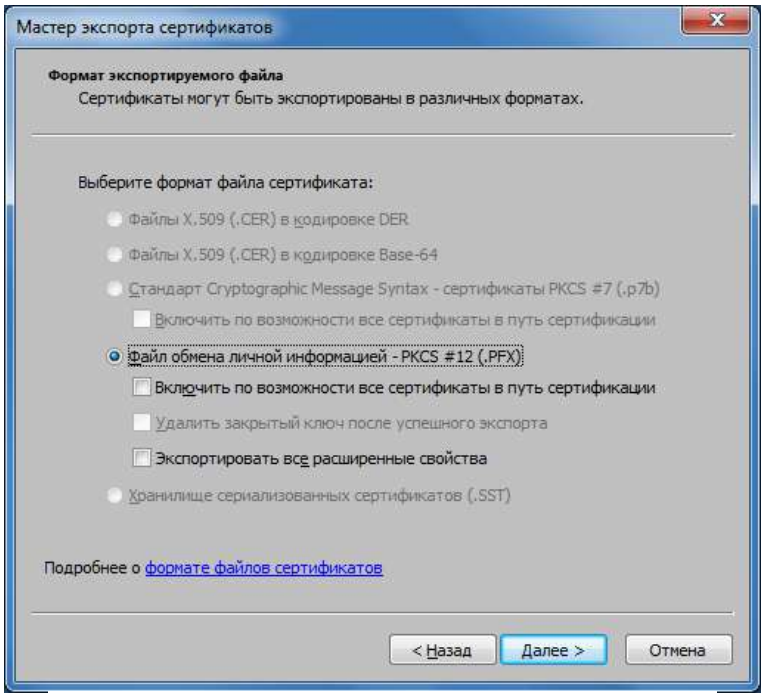


Рис. 1.10. Формат экспортируемого сертификата

Затем необходимо ввести пароль, являющийся защитой закрытого ключа пользователя (рис. 1.11). Введите произвольный пароль, который обязательно необходимо запомнить, и нажмите «Далее».

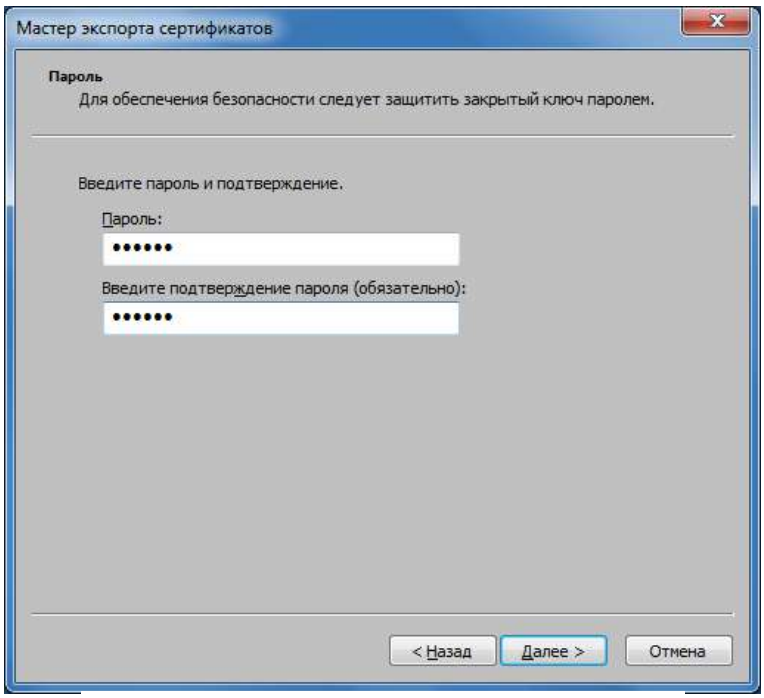


Рис. 1.11. Защита закрытого ключа паролем

Выберите расположение экспортирования файла, содержащего сертификат и закрытый ключ (рисунок 1.12).

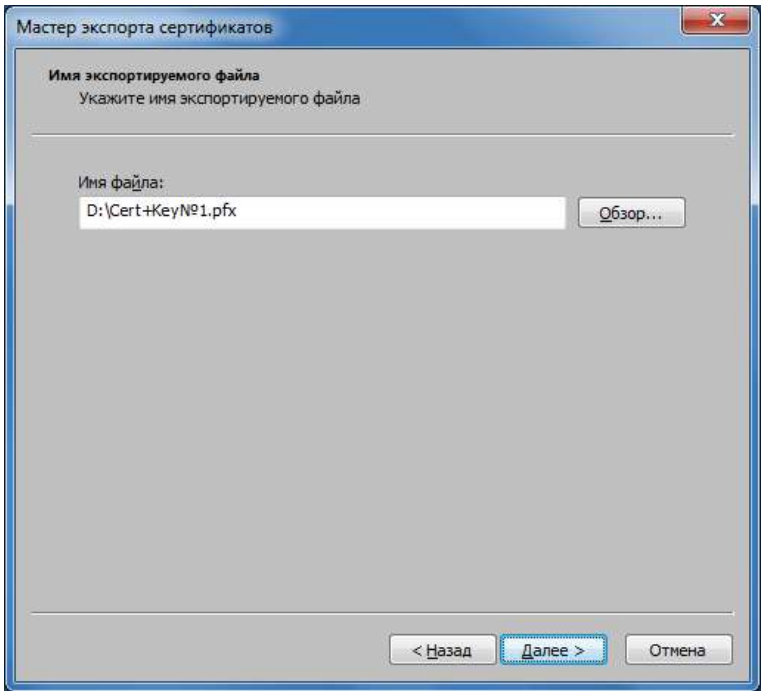


Рис. 1.12. Выбор места сохранения сертификата с ключом

В случае успешного завершения операции будет выведено соответствующее сообщение (рис. 1.13).

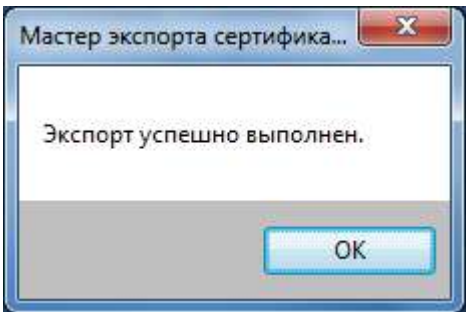


Рис. 1.13. Создание архивной копии

Чтобы проверить, что данный файл зашифрован, создайте учетную запись второго пользователя.

Откройте «Пуск», затем «Панель управления» и в режиме просмотра по категориям откройте «Добавление и удаление учетных записей пользователей» в категории «Учетные записи пользователей и семейная безопасность». Создайте новую учетную запись с обычным доступом и войдите в систему под данной учетной записью. Попробуйте открыть файл, зашифрованный первым пользователем. Будет выведено сообщение об отказе доступа к файлу (рис. 1.14).

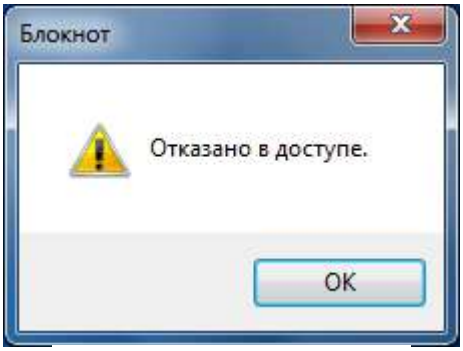


Рис. 1.14. Отказ в доступе

Теперь зашифруйте второй файл из-под учетной записи второго пользователя, а также создайте архивную копию сертификата и закрытого ключа второго пользователя. Перейдите на учетную запись первого пользователя и попробуйте открыть файл, зашифрованный вторым пользователем. Также отобразится сообщение об отказе доступа к файлу.

Если по какой-либо причине будут потеряны данные о сертификате и закрытом ключе пользователя, то и сам пользователь не сможет получить доступ к зашифрованным им файлам и папкам. Удалим данный сертификат вручную у первого пользователя:

1) Откройте меню «Пуск», в поле поиска введите название утилиты «certmgr.msc» и нажмите Enter (рис. 1.15).

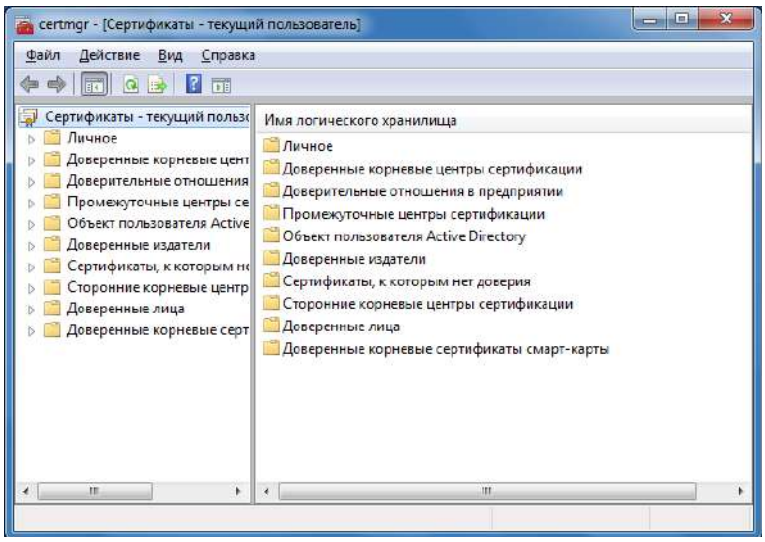


Рис. 1.15. Программа управления хранилищем сертификатов

2) В открывшемся окне управления хранилищем сертификатов откройте сертификаты раздела «Личное».

3) Удалите сертификат первого пользователя (рис. 1.16).

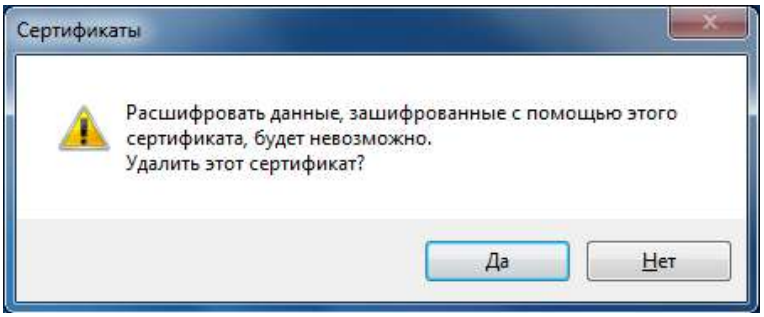


Рис. 1.16. Удаление вручную сертификата первого пользователя

Чтобы изменения вступили в силу, завершите сеанс первого пользователя и снова зайдите под учетной записью первого пользователя. Теперь доступ от первого пользователя к файлам, зашифрованным первым пользователем не доступен.

Чтобы вернуть доступ, необходимо восстановить сертификат и закрытый ключ пользователя. Для этого снова откройте хранилище сертификатов, перейдите в сертификаты раздела «Личное» и, вызвав правой кнопкой контекстное меню, выберите «Все задачи/Импорт…». Запустится мастер импорта сертификатов, нажмите «Далее» (рис. 1.17).

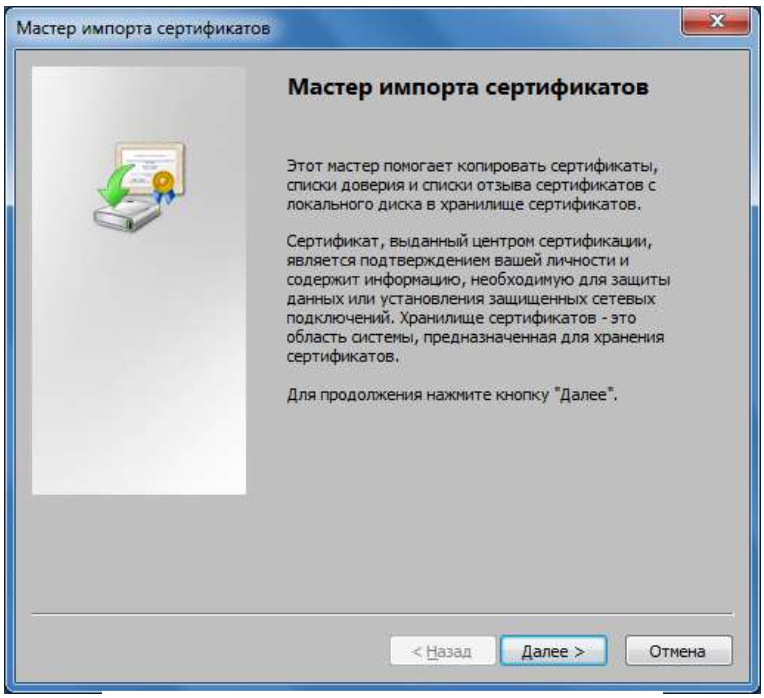


Рис. 1.17. Мастер импорта сертификатов

Укажите нужный сертификат, при этом нужно сменить указанный тип файлов с .cer и .crt на .pfx, так как по умолчанию в программе задаются сертификаты без закрытого ключа, нажмите «Далее» (рис. 1.18).

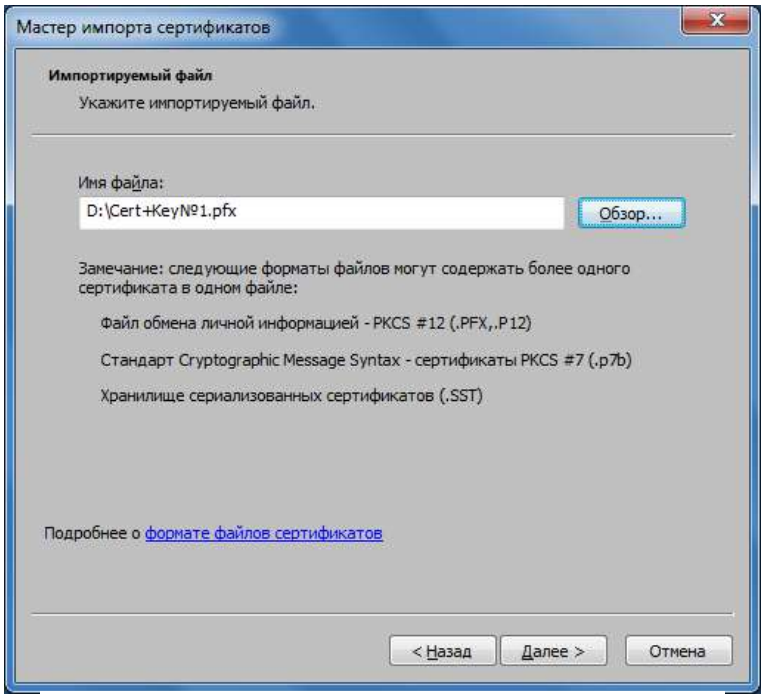


Рис. 1.18. Указание импортируемого сертификата

В следующем окне необходимо ввести пароль, указанный при архивировании сертификата первого пользователя. Введите пароль и нажмите «Далее» (рис. 1.19).

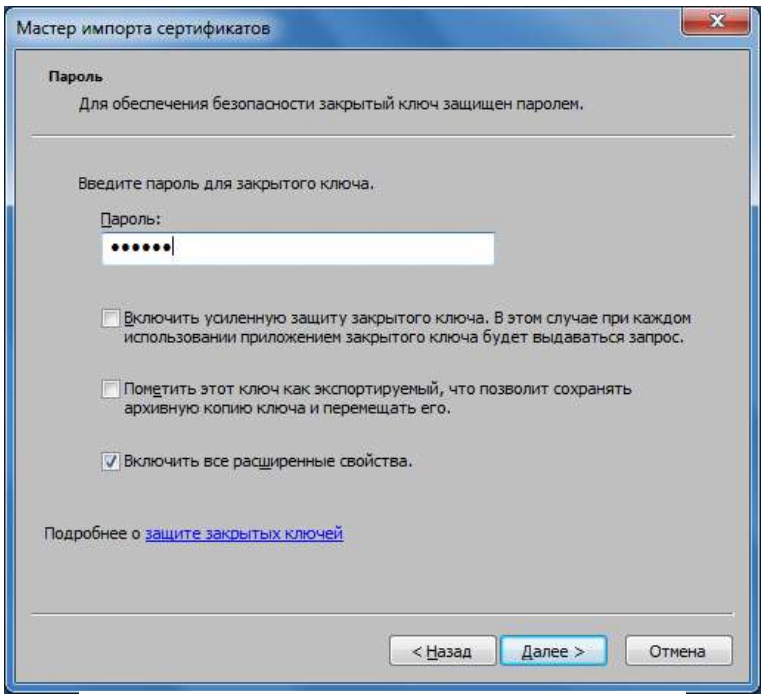


Рис. 1.19. Ввод пароля для закрытого ключа

Поместите сертификат в хранилище сертификатов «Личное», нажмите «Далее» (рис. 1.20).

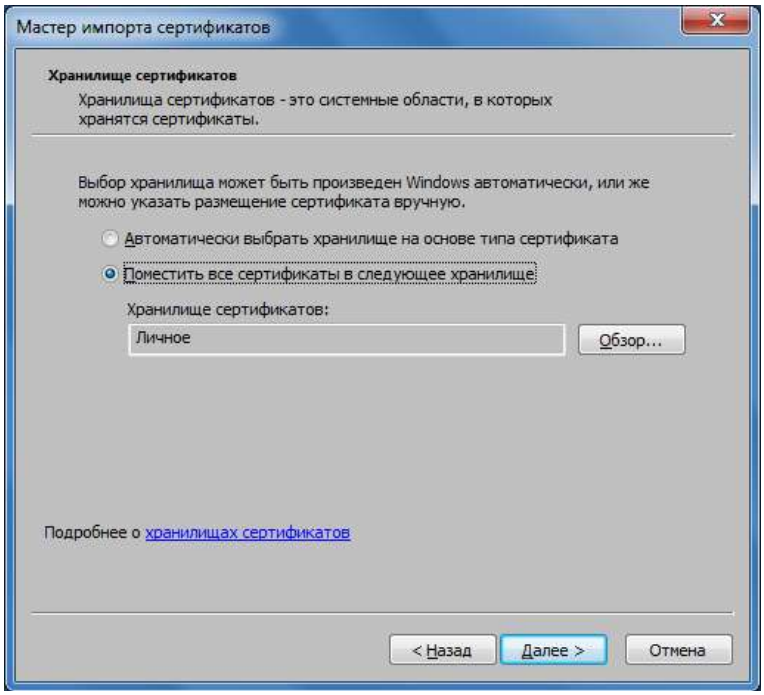


Рис. 1.20. Помещение сертификата в хранилище «Личное»

Восстановление сертификата с закрытым ключом завершено (рис. 1.21). Теперь доступ к файлам восстановлен.

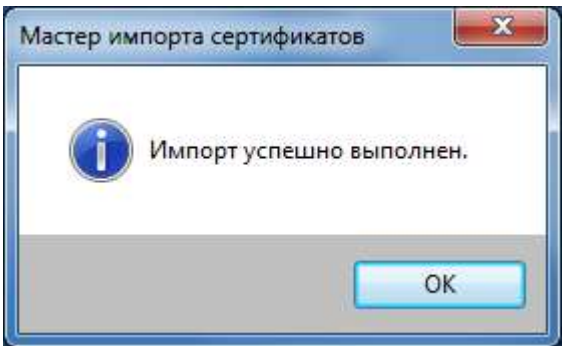


Рис. 1.21. Сертификат успешно восстановлен

Использовать шифрование файлов можно и при совместном использовании одного файла несколькими пользователями. Общий доступ для папок не устанавливается. Сделаем доступным второй файл первому пользователю. Для этого откройте личное хранилище сертификатов первого пользователя, выделите восстановленный сертификат, вызовите контекстное меню и выполните команду «Все задачи/Экспорт…» (рисунок 1.22).

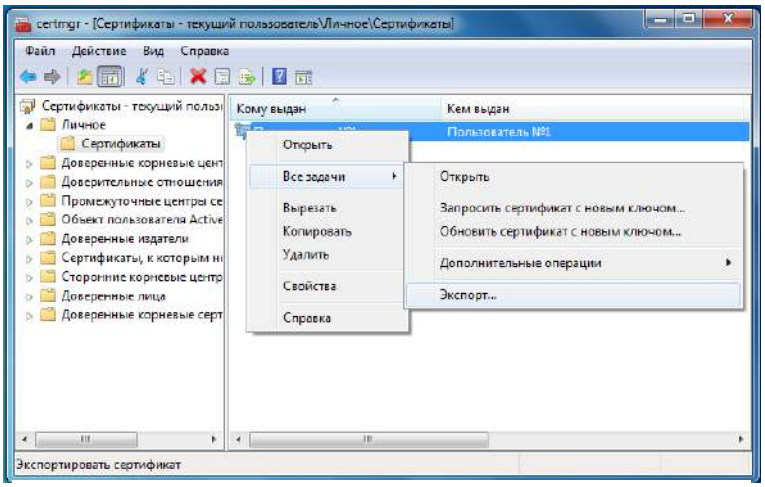


Рис. 1.22. Экспорт сертификата первого пользователя

При этом выполнится экспорт сертификата без закрытого ключа первого пользователя (рисунок 1.23).

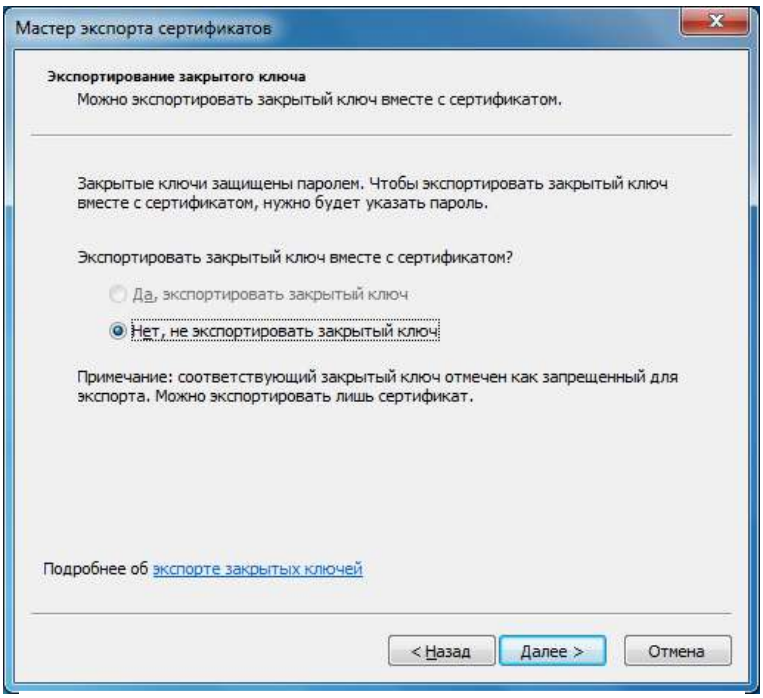


Рис. 1.23. Экспорт сертификата без закрытого ключа

Представим, что данный сертификат был передан второму пользователю.

Перейдите на учетную запись второго пользователя и откройте хранилище сертификатов второго пользователя. Перейдите в раздел сертификатов «Личное», вызовите контекстное меню и выполните команду «Все задачи/Импорт…». Импортируйте сертификат первого пользователя без закрытого ключа в раздел «Доверенные лица».

Откройте свойства второго файла, перейдите на вкладку «Общие» и нажмите кнопку «Другие». В окне «Дополнительные атрибуты» нажмите кнопку «Подробно», откроется окно доступа к файлу (рисунок 1.24).

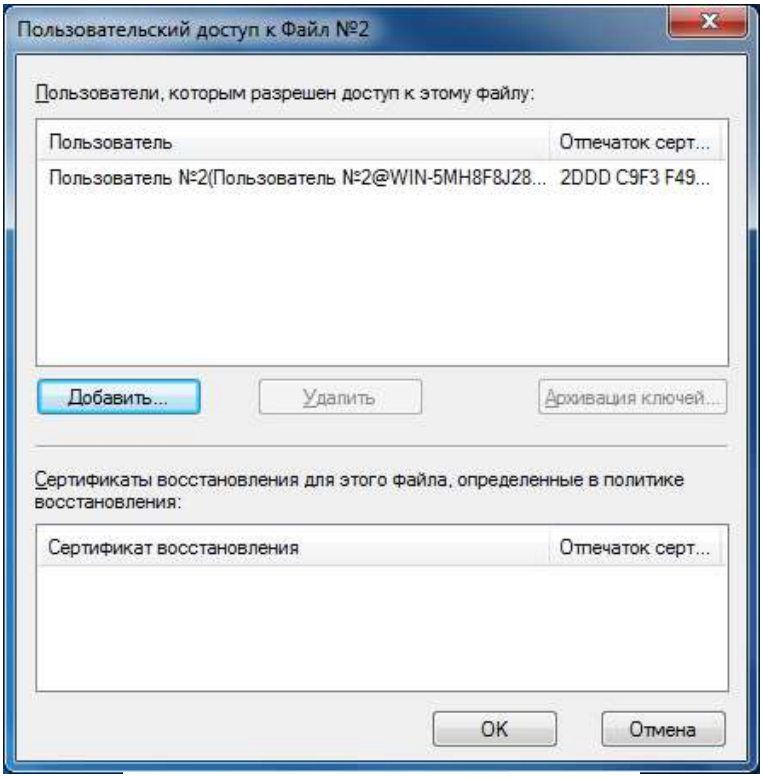


Рис. 1.24. Настройка доступа к файлу

Нажмите кнопку «Добавить…» и выберите сертификат первого пользователя (рис. 1.25).

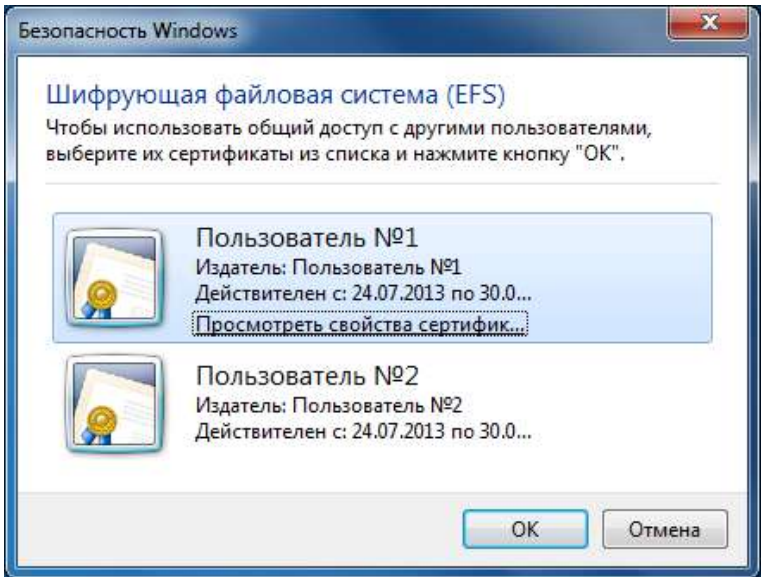


Рис. 1.25. Добавление доступа через сертификат первого пользователя

Проверьте доступ к данному файлу для первого пользователя. Чтобы убедиться, что данный файл доступен только первому и второму пользователю – создайте третьего пользователя и попробуйте через его учетную запись открыть второй файл.

Контрольные вопросы:

1) В каких выпусках операционных систем Windows присутствует шифрованная файловая система?

2) Для каких файловых систем применима шифрованная файловая система?

3) Для чего в шифрованной файловой системе используется симметричное шифрование? Асимметричное?

4) Опишите алгоритм работы шифрованной файловой системы Windows.

5) Для чего нужно архивировать закрытый ключ и сертификат пользователя?

Работа № 2.

Шифрование диска BitLocker.

Цель работы

Целью данной работы является изучение штатного средства шифрования информации в операционных системах Microsoft Windows — технологии шифрования диска BitLocker.

Краткие теоретические сведения

Обеспечение конфиденциальности данных, хранимых на носителях информации, посредством организации аутентифицированного доступа к ним является действенным до тех пор, пока носитель информации не попадет в руки злоумышленника, который в этом случае сможет работать с ним напрямую в обход всех механизмов разграничения прав доступа. В такой ситуации обеспечить конфиденциальность можно лишь с помощью шифрования содержимого носителя информации.

В операционных системах Microsoft Windows, начиная с Windows Vista (только в выпусках Enterprise, Ultimate), для этой цели служит технология шифрования диска BitLocker (BitLocker Drive Encryption), позволяющая шифровать информацию как на стационарных, так и на съемных носителях. Для шифрования используется алгоритм AES со 128-битовым ключом.

В отличие от шифрованной файловой системы (Encrypting File System – EFS), позволяющей шифровать отдельные файлы и каталоги, BitLocker шифрует носитель информации полностью. Такое шифрование является прозрачным для пользователей, которые после входа в систему могут работать с файлами как обычно, не испытывая затруднений от наличия данного защитного механизма. Однако злоумышленник, получивший физический доступ к диску, не сможет считать его содержимое.

BitLocker автоматически шифрует все файлы, добавляемые на зашифрованный диск. Если к файлам на зашифрованном диске предоставляется общий доступ, то храниться они будут в зашифрованном виде, но авторизованные пользователи смогут получать к ним доступ обычным образом.

Технология BitLocker предназначена для работы с носителями информации, на которых используются файловые системы exFAT, FAT16, FAT32 или NTFS. Для шифрования диска с операционной системой на нем должна использоваться файловая система NTFS.

Существуют некоторые различия между реализациями технологии BitLocker в операционных системах Windows Vista и Windows 7. Основное различие заключается в том, что в Windows 7 не нужно выполнять специальную разметку дисков. Ранее пользователь должен был для этого использовать утилиту Microsoft BitLocker Disk Preparation Tool, сейчас же достаточно просто указать, какой именно диск должен быть защищен, и система автоматически создаст на диске скрытый загрузочный раздел, используемый BitLocker. Этот загрузочный раздел будет использоваться для запуска компьютера, он хранится в незашифрованном виде (в противном случае загрузка была бы невозможна), раздел же с операционной системой будет зашифрован. По сравнению с Windows Vista, размер загрузочного раздела занимает примерно в десять раз меньше дискового пространства. Дополнительному разделу не присваивается отдельная буква, и он не отображается в списке разделов файлового менеджера.

BitLocker может работать в различных режимах, каждый из которых имеет свои особенности, а также обеспечивает свой уровень безопасности:

— режим с использованием доверенного платформенного модуля;
— режим с использованием доверенного платформенного модуля и USB-устройства;

— режим с использованием доверенного платформенного модуля и персонального идентификационного номера (ПИН-кода);
— режим с использованием USB-устройства, содержащего ключ.

Доверенный платформенный модуль (Trusted Platform Module — TPM) — это специальный криптографический чип, также называемый криптопроцессором, предназначенный для хранения ключевой информации и реализации некоторых криптографических функций. Такая микросхема может быть интегрирована, например, в некоторых моделях ноутбуков, настольных ПК, различных мобильных устройствах и т. д.

Когда защита выполняется исключительно с помощью доверенного платформенного модуля, в процессе включения компьютера на аппаратном уровне происходит сбор данных, которые позволят установить подлинность аппаратного обеспечения. Данная проверка является «прозрачной» и не требует от пользователя никаких действий, в случае успешного прохождения, выполняется загрузка операционной системы в штатном режиме. При обнаружении угрозы BitLocker заблокирует диск с операционной системой. Чтобы разблокировать его, потребуется специальный ключ восстановления BitLocker, который необходимо создать при первом запуске BitLocker. В противном случае доступ к файлам может быть потерян.

Порядок выполнения работы

Работа выполняется на виртуальной машине с установленной операционной системой Windows 7 Ultimate, для запуска которой используется программа VMware Player. Чтобы выполнить все действия, предусмотренные в данной работе, необходимо подготовить виртуальную машину не менее чем с двумя локальными дисками.

BitLocker To Go

Для шифрования локальных дисков, не являющихся системными, а также съемных дисков, предназначена функция BitLocker To Go. Чтобы воспользоваться данной функцией, необходимо открыть инструмент «Шифрование диска BitLocker» на «Панели управления» (рис. 2.1).

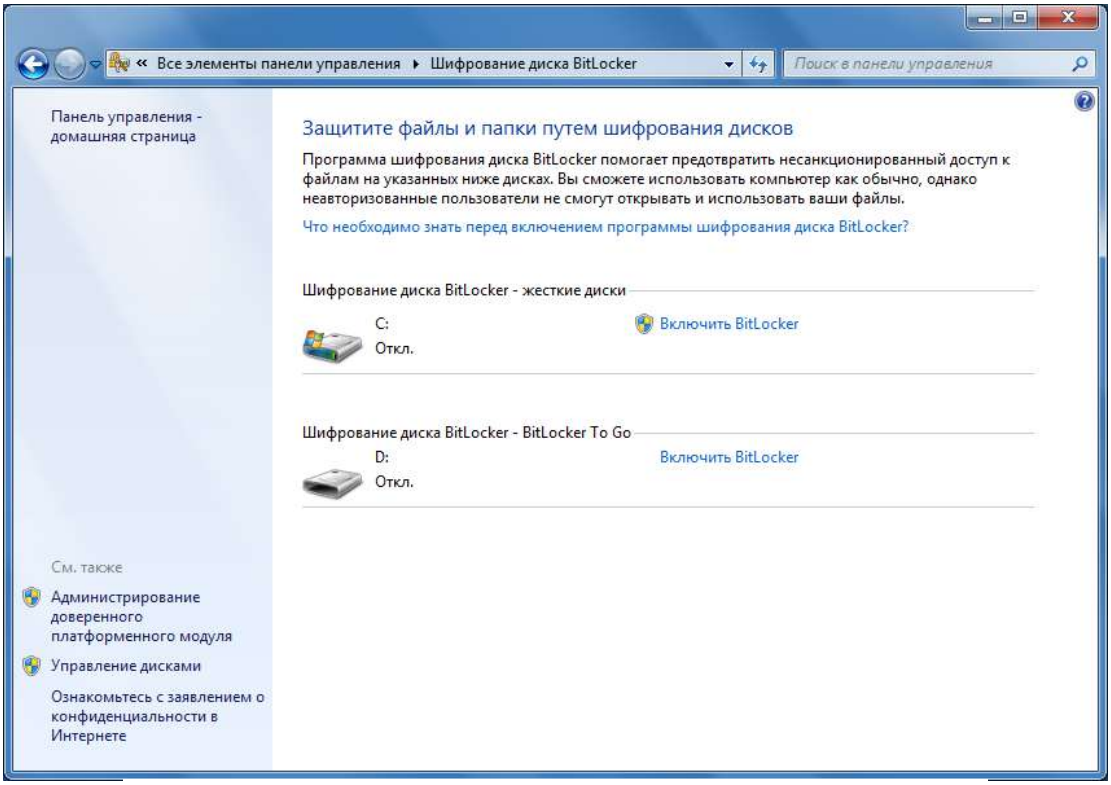


Рис. 2.1. Инструмент Windows «Шифрование диска BitLocker»

Чтобы запустить процедуру шифрования диска D (рис. 2.1), выполните команду «Включить BitLocker». Выберите способ шифрования с использованием пароля, введите произвольный пароль, содержащий не менее 8-ми символов, и нажмите «Далее» (рис. 2.2).

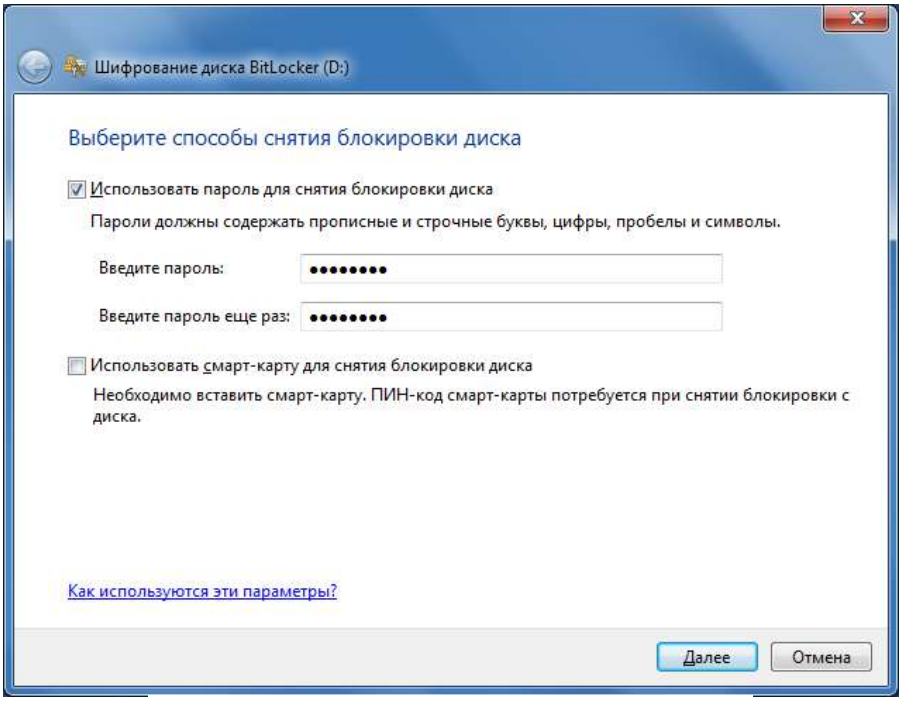


Рис. 2.2. Ввод пароля для блокировки диска

В следующем окне выберите пункт «Сохранить ключ восстановления в файле» (рис. 2.3) и указав место сохранения файла, нажмите «Далее».

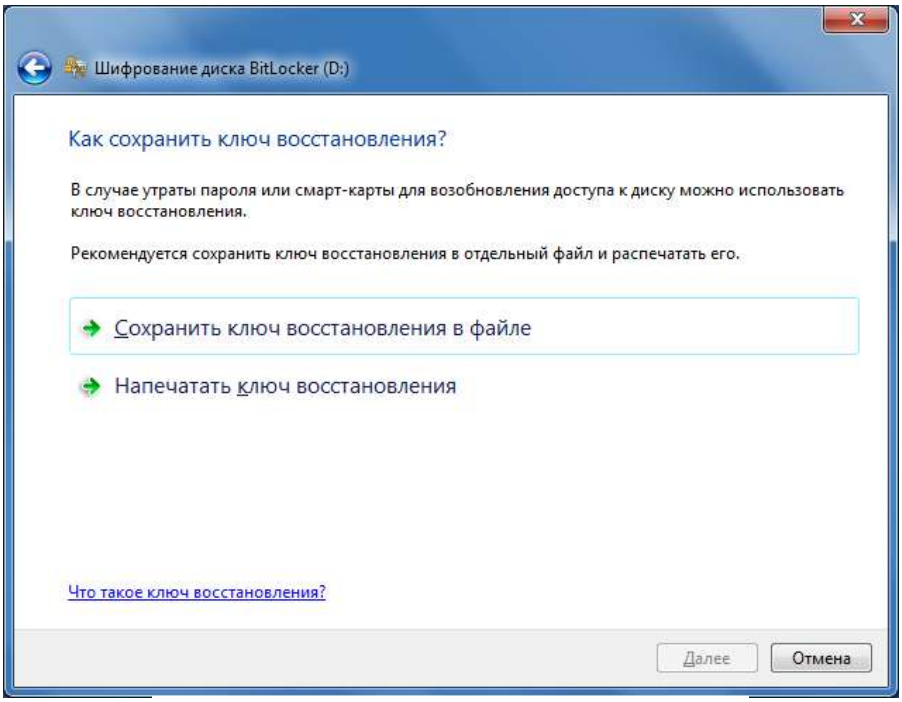


Рис. 2.3 Сохранение ключа восстановления

Затем запустите процедуру шифрования диска нажатием кнопки «Начать шифрование» (рис. 2.4) и дождитесь, когда диск будет полностью зашифрован (рис. 2.5).

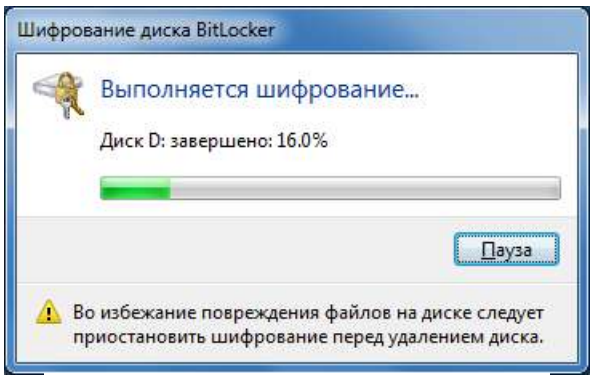


Рис. 2.4. Процесс шифрования диска

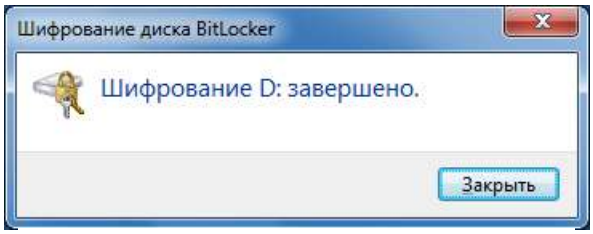


Рис. 2.5. Процесс шифрования завершен

Чтобы заблокировать диск, выполните перезагрузку. Теперь значок локального диска D в зашифрованном состоянии отображается с закрытым замком (рис. 2.6).

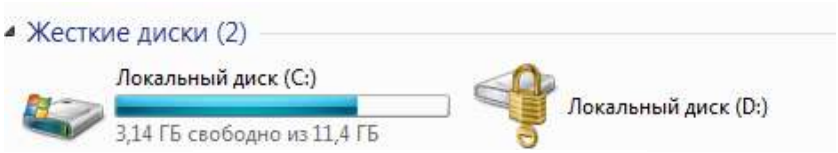


Рис. 2.6. Зашифрованный диск D

При попытке открыть данный диск, появится окно с запросом пароля для разблокировки диска (рис. 2.7).

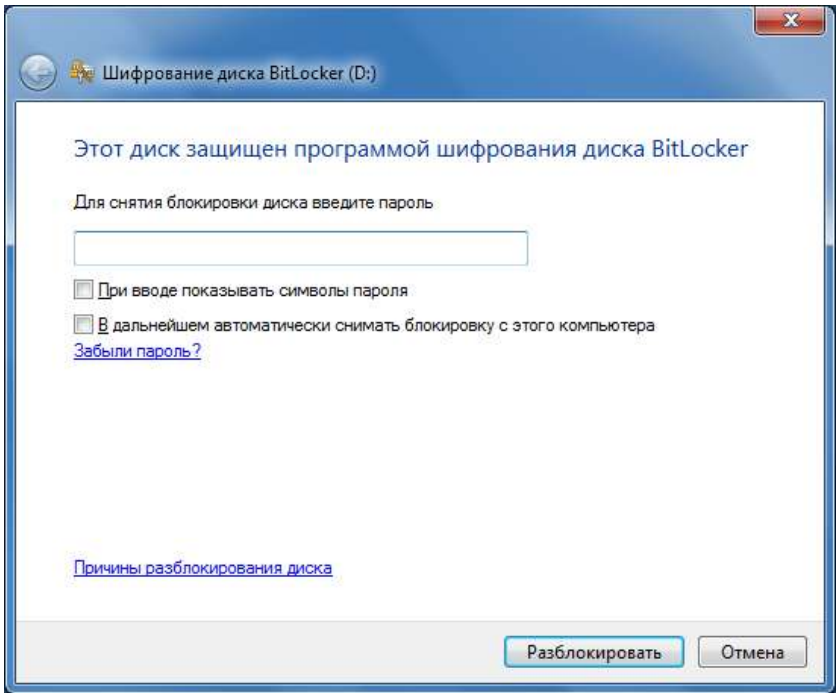


Рис. 2.7. Запрос на ввод пароля для снятия блокировки диска

После ввода верного пароля диск становится доступным, а значок диска изменяется на открытый замок (рисунок 8).

Рисунок 8 – Разблокированный диск D

Таким же способом, применяя функцию «BitLocker To Go», можно зашифровать USB-флеш-накопитель. Прочитать информацию, хранящуюся на зашифрованном USB-флеш-накопителе, можно только при подключении к компьютеру с операционной системой не ниже Windows XP с установленным обновлением KB970401, содержащим программу «BitLocker To Go Reader». При этом отобразится запрос на ввод пароля, установленного при зашифровании, и только после ввода верного пароля информация на USB-флеш-накопителе будет расшифрована.

Использование BitLocker на компьютере без TPM

Прежде чем выполнить шифрование системного диска, необходимо внести некоторые изменения в групповую политику, потому что BitLocker изначально использует систему TPM, и при его отсутствии Windows с настройками по умолчанию для системного диска не позволит включить BitLocker. Чтобы использовать BitLocker на компьютере без TPM, выполните следующие действия:

1) откройте меню «Пуск», введите в поле поиска «gpedit.msc» и нажмите Enter;

2) в появившемся окне «Редактор локальной групповой политики» зайдите в раздел «Конфигурация компьютера», затем в «Административные шаблоны» и в «Компоненты Windows» найдите «Шифрование диска BitLocker» (рис. 2.9);

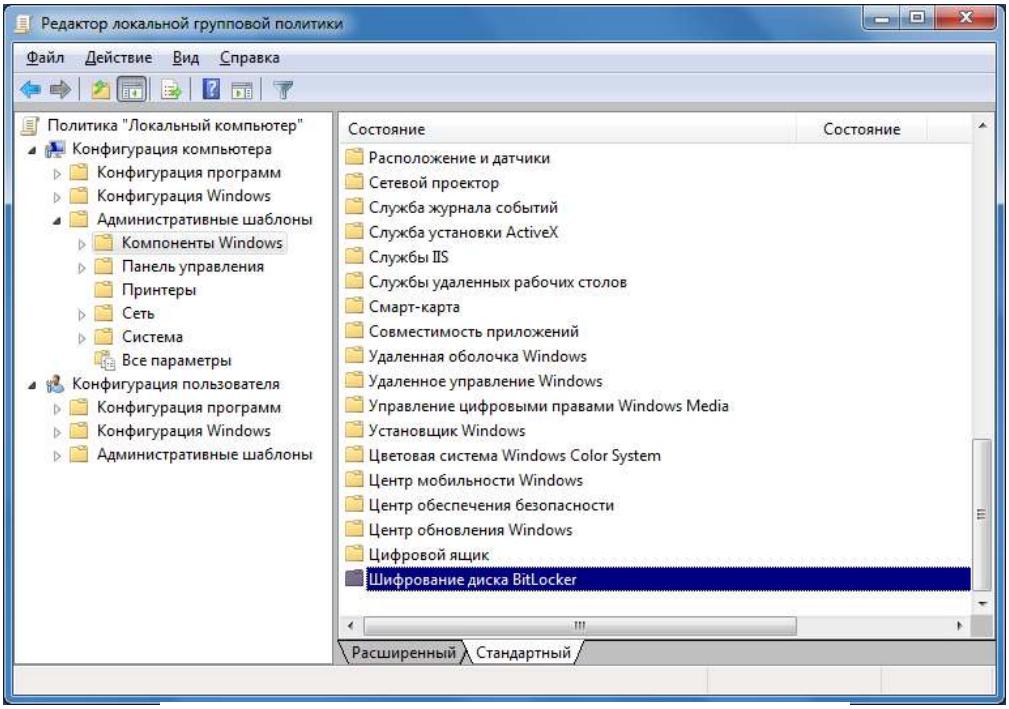


Рис. 2.9. Редактор локальной групповой политики

3) в данном компоненте зайдите в «Диски операционной системы» и откройте настройку «Обязательная дополнительная проверка подлинности при запуске» (рис. 2.10);

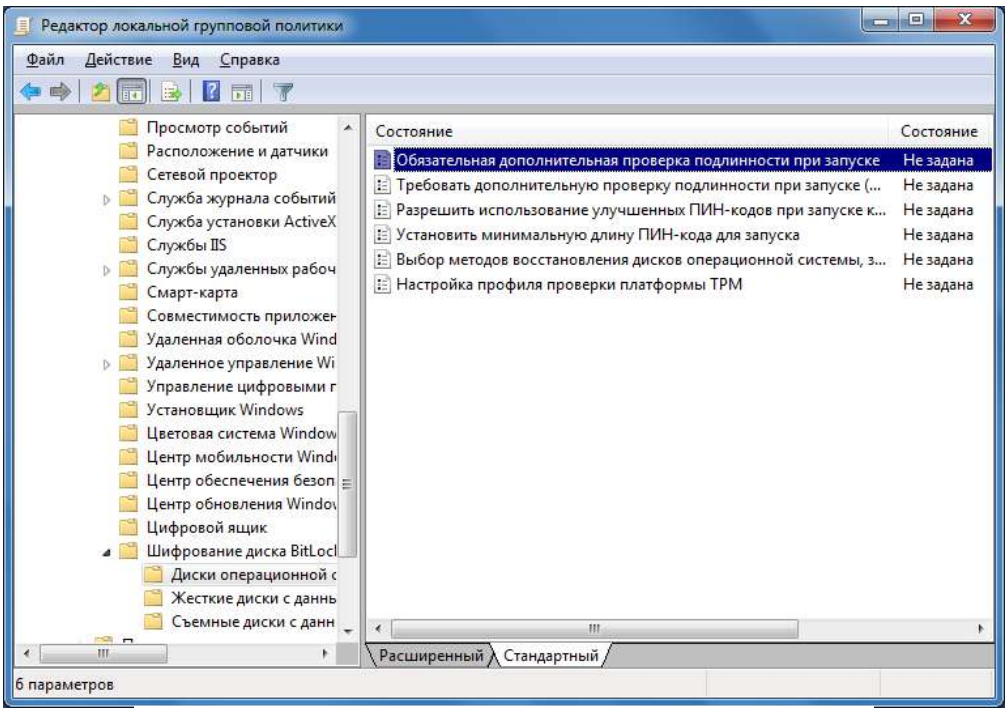


Рис. 2.10. Настройки BitLocker для системных дисков

4) в появившемся окне выберите вариант «Включить», установите флажок «Разрешить использование BitLocker без совместимого TPM» и нажмите кнопку «ОК» (рис. 2.11). Теперь вместо TPM можно использовать ключ запуска;

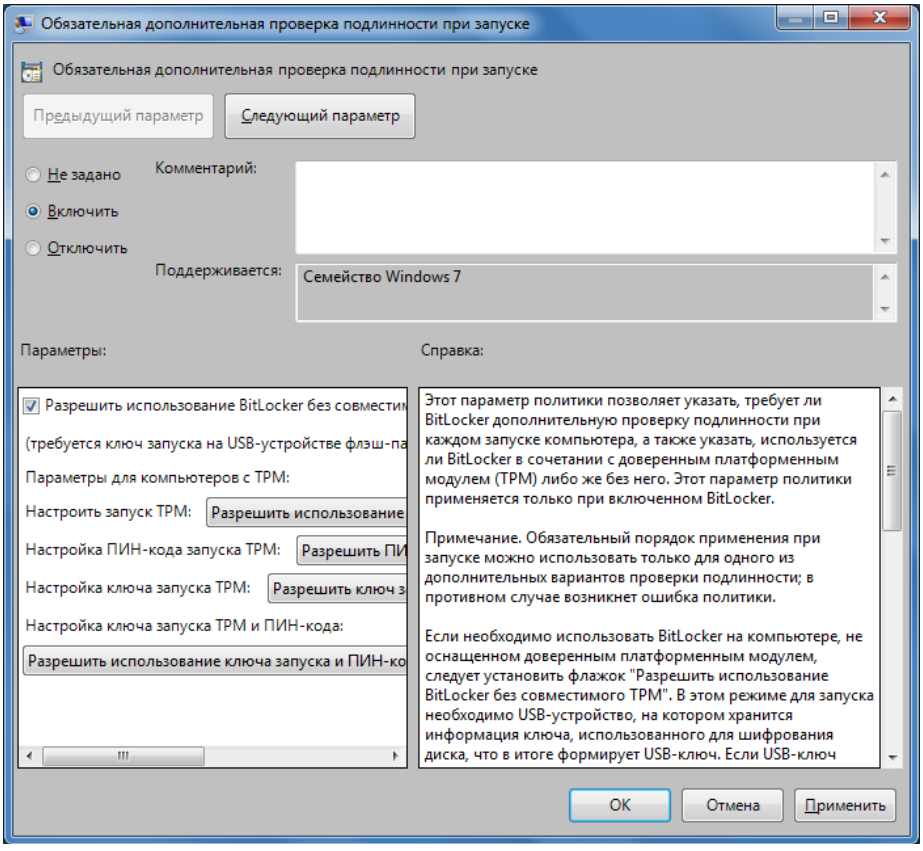


Рис. 2.11. Включение использования BitLocker без совместимого TPM

5) закройте редактор локальной групповой политики;

6) чтобы новые настройки групповых политик вступили в силу немедленно, нажмите кнопку «Пуск», введите «gpupdate.exe /force» в поле поиска и нажмите Enter. Дождитесь завершения процесса (рис. 2.12).

Рис. 2.12. Применение новых настроек групповых политик

Теперь можно приступить к шифрованию системного диска без TPM, а с использованием USB-флеш-накопителя.

Подготовка системного диска для BitLocker

Откройте инструмент «Шифрование диска BitLocker» и выполните команду «Включить BitLocker» для системного диска C. Запустится проверка конфигурации компьютера, время выполнения которой занимает несколько минут (рис. 2.13).

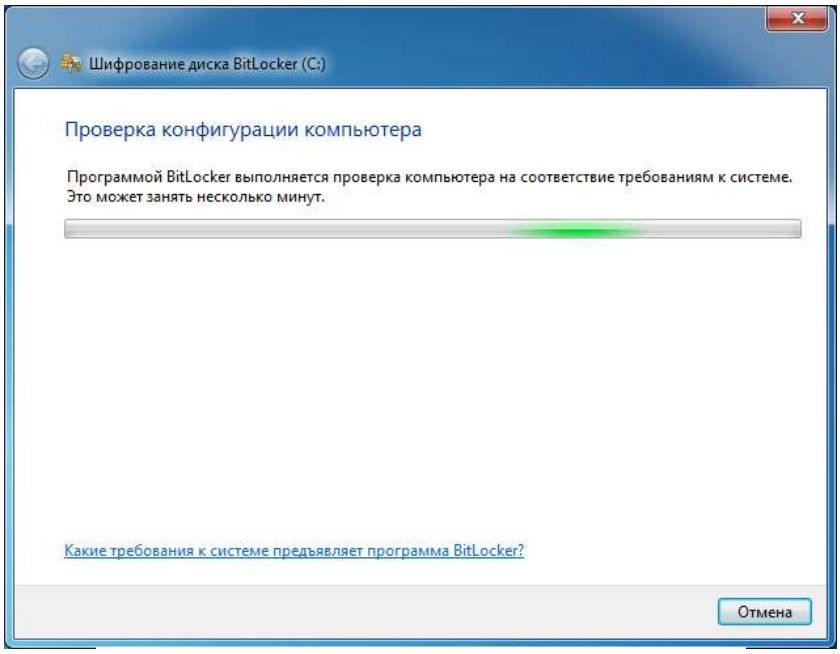


Рис. 2.13. Проверка конфигурации компьютера

После выполненной проверки конфигурации компьютера отобразится окно с перечнем действий, которые необходимо выполнить для шифрования системного диска (рис. 2.14).

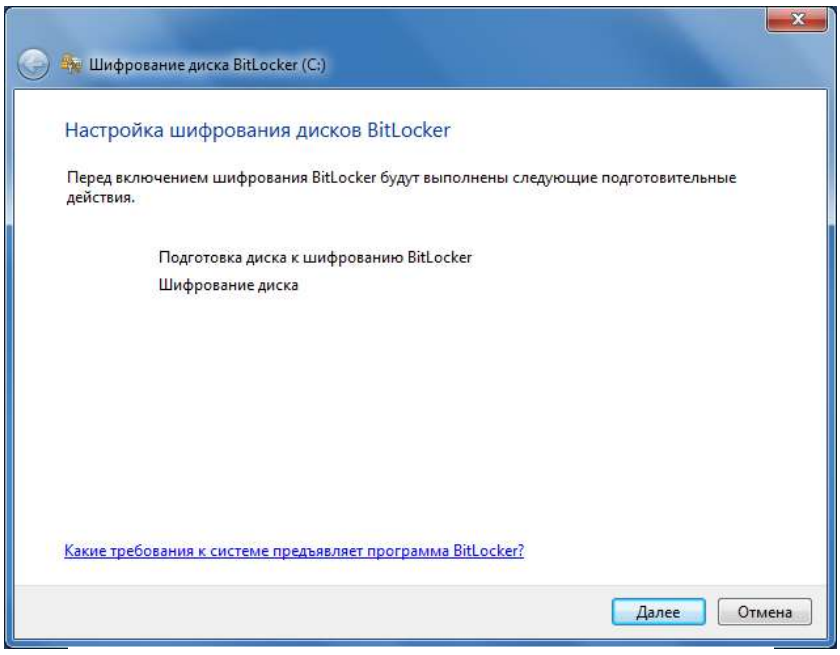


Рис. 2.14. Настройка шифрования дисков BitLocker

Нажмите два раза «Далее», начнется подготовка диска для BitLocker (рис. 2.15).

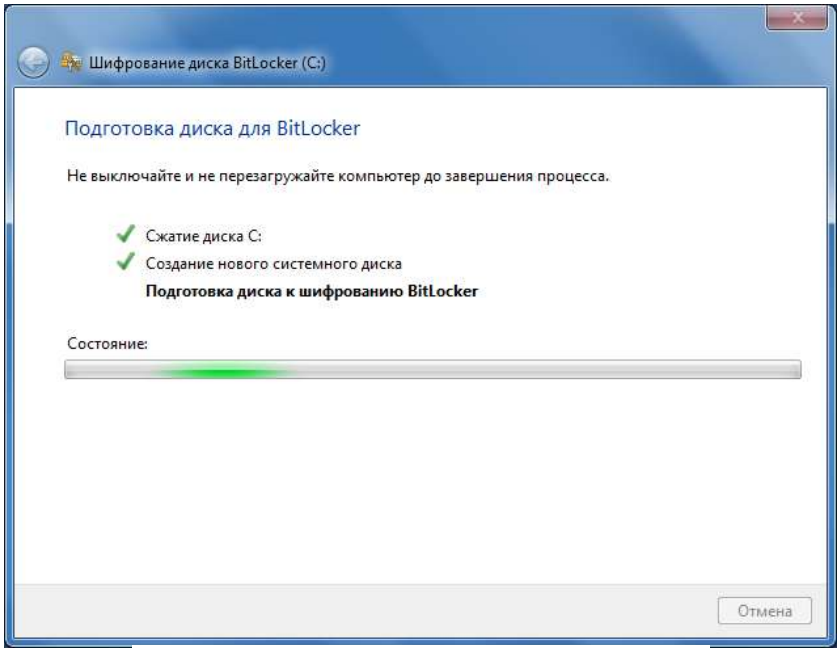


Рис. 2.15. Подготовка диска для BitLocker

После подготовки диска для BitLocker отобразится запрос на перезагрузку (рис. 2.16), выполните перезагрузку системы.

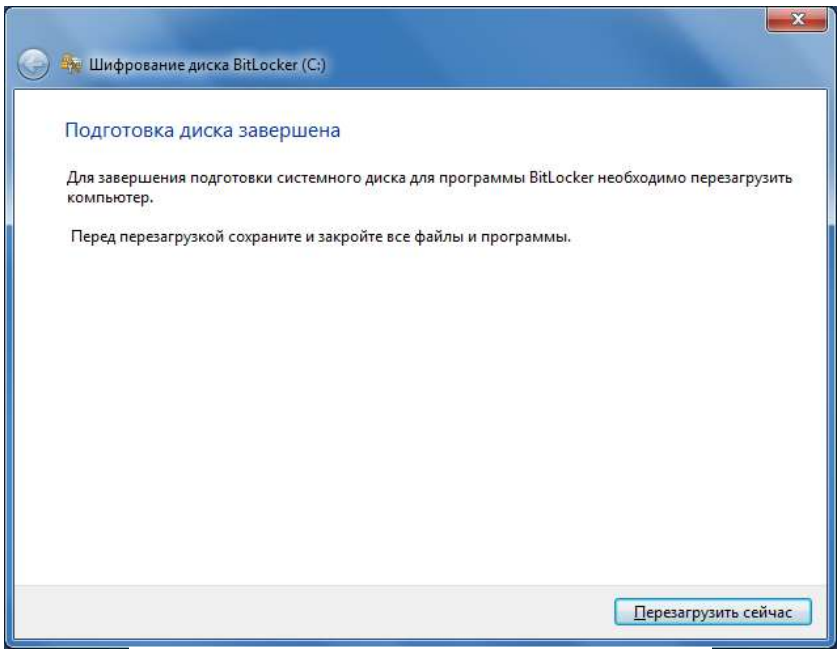


Рис. 2.16. Запрос на перезагрузку системы

После перезагрузки возобновится процедура шифрования системного диска с сообщением о том, что подготовка диска к BitLocker завершена и можно приступить к самому шифрованию (рис. 2.17).

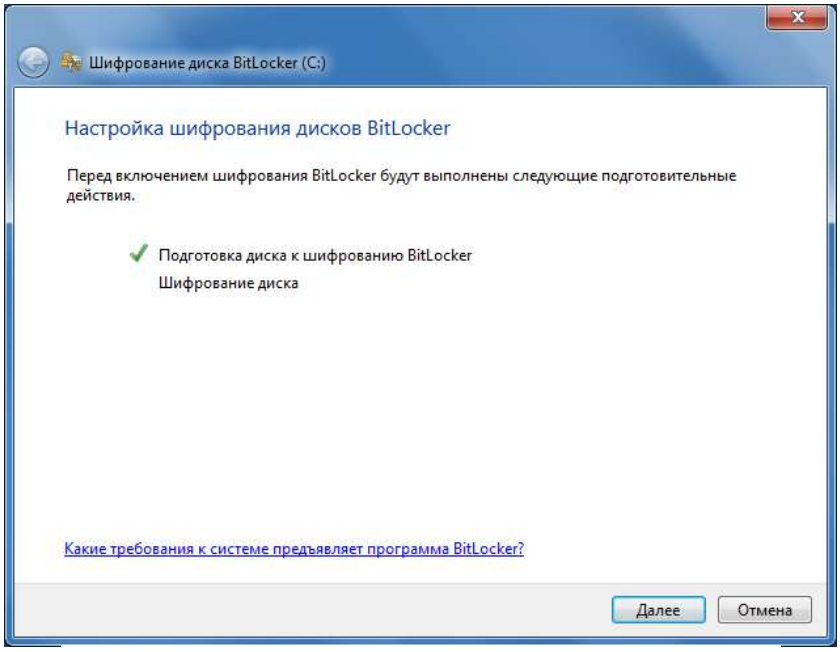


Рис. 2.17. Переход к шифрованию системного диска

Данный способ шифрования системного диска с использованием USB-флеш-накопителя в качестве носителя ключа запуска можно использовать только на компьютере, BIOS которого поддерживает чтение USB-устройств в загрузочной среде. Также необходимо, чтобы BIOS был настроен на загрузку сначала с жесткого диска, а затем с USB-устройства. Поэтому его применение на виртуальной машине VMWare Player невозможно (VMWare Player не поддерживает загрузку с USB-устройства). Далее представлено описание действий, выполнение которых приведет к зашифрованию системного диска на реальной системе (не на виртуальной машине).

Шифрование системного диска на реальной системе

Для продолжения процедуры шифрования необходимо нажать кнопку «Далее».

Без TPM шифрование доступно только единственным способом – запрос ключа запуска при запуске системы (рисунок 18).

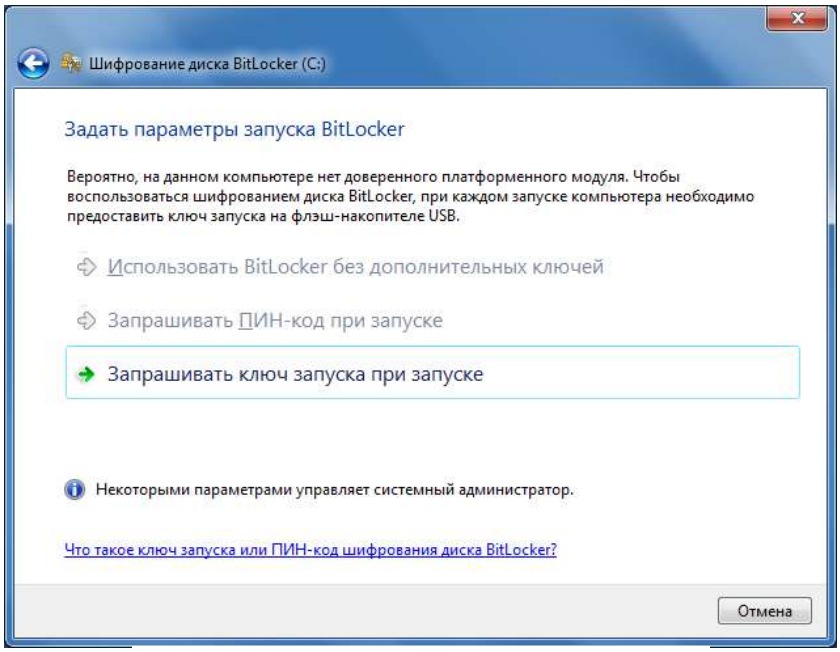


Рис. 2.18. Выбор параметров шифрования

Для сохранения ключа записи необходим USB-флеш-накопитель (рис. 2.19).

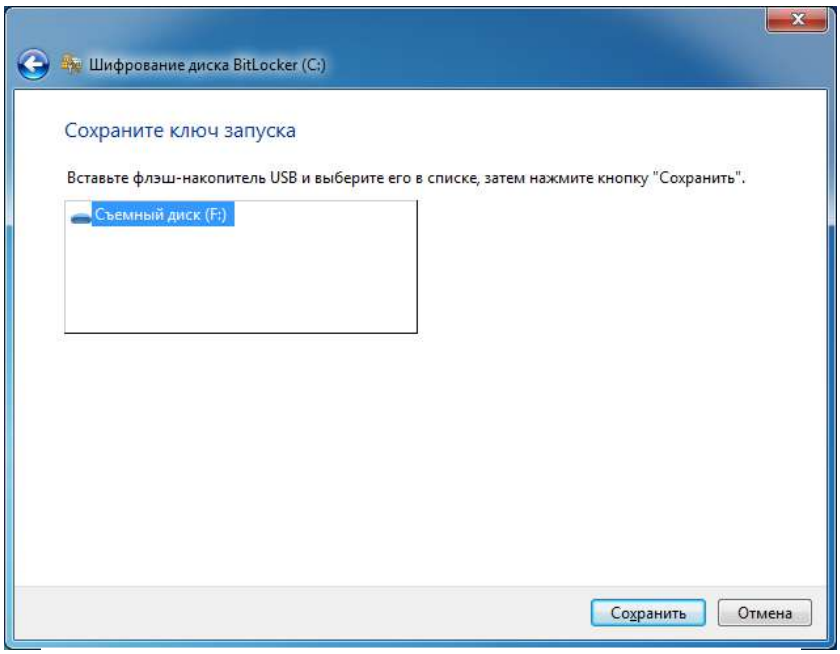


Рис. 2.19. Сохранение ключа на USB-флеш-накопителе

Затем будет предложен выбор способа сохранения ключа восстановления, необходимого для получения доступа к системному диску в случае утери USB-флеш-накопителя с ключом запуска (рис. 2.20).

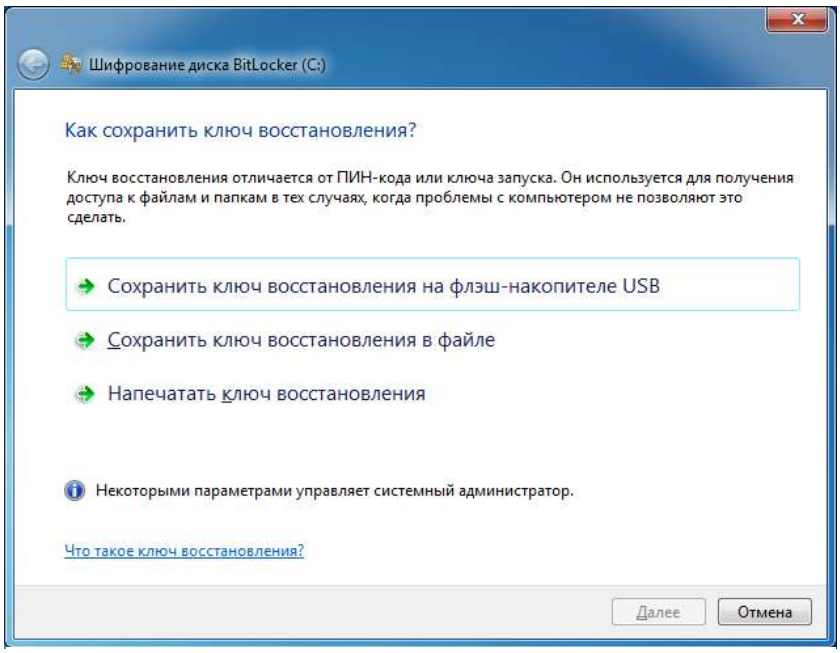


Рис. 2.20. Выбор способа сохранения ключа восстановления

После сохранения ключа восстановления будет предложено запустить проверку системы BitLocker (рис. 2.21), для этого система выполнит перезагрузку. Данную проверку желательно произвести, чтобы потом не возникли ошибки после зашифрования системного диска.

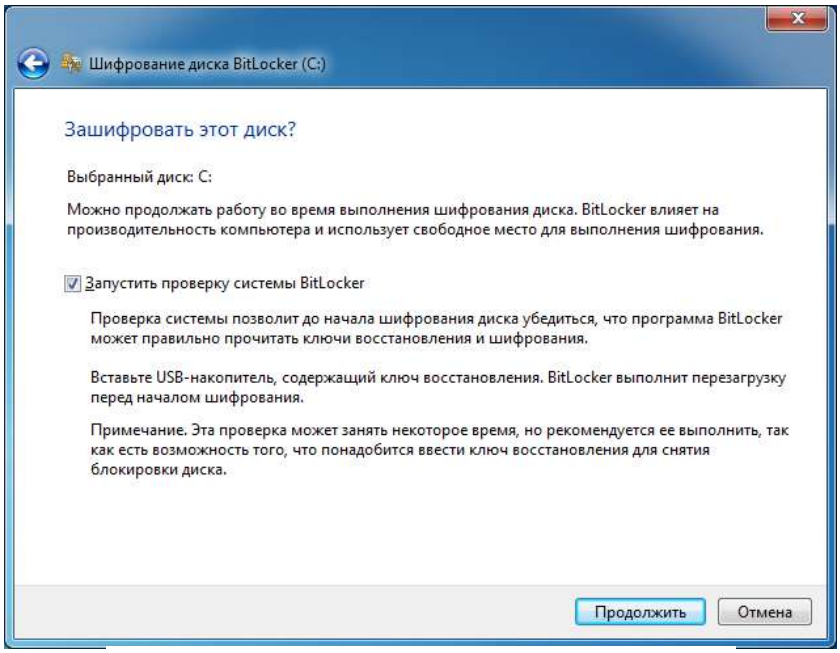


Рис. 2.21. Запуск проверки системы BitLocker

Если BIOS компьютера поддерживает чтение USB-устройств в загрузочной среде, то запустится процедура шифрования системного диска (рис. 2.22). В противном случае (например, если выполнять данные действия на виртуальной машине) отобразится ошибка, и процедура шифрования будет отменена (рис. 2.23).

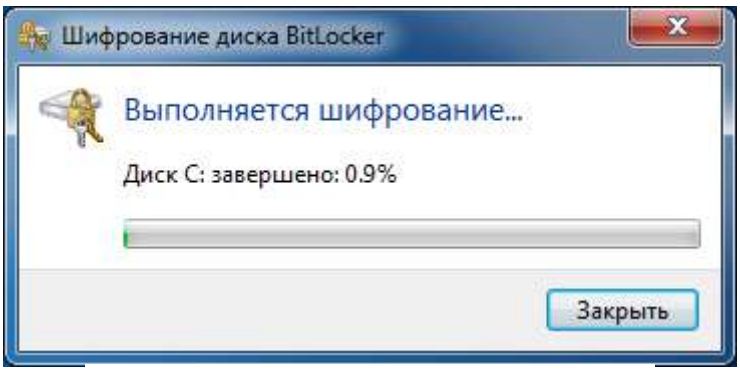


Рис. 2.22. Шифрование системного диска

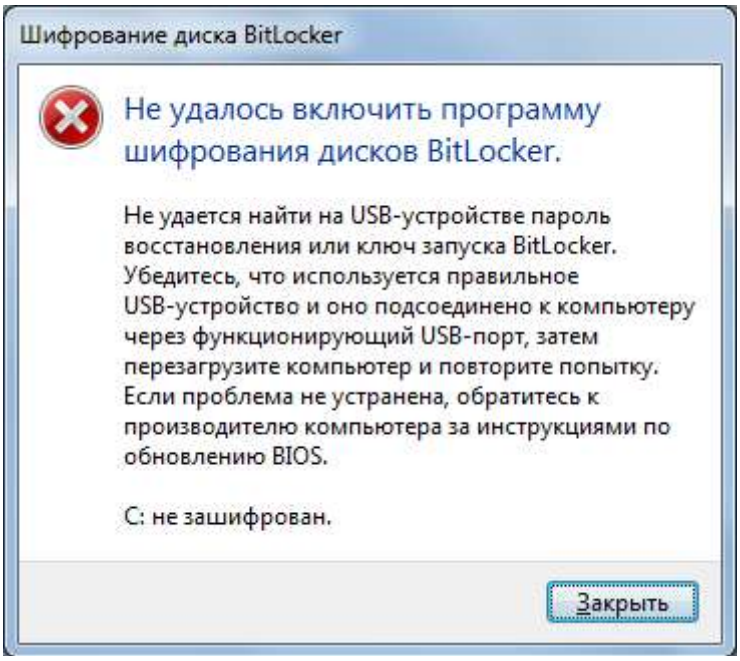


Рис. 2.23. Ошибка при выполнении проверки системы BitLocker

После зашифрования системного диска операционная система будет загружаться только при наличии вставленного USB-флеш-накопителя с ключом запуска во время загрузки системы (рис. 2.24).

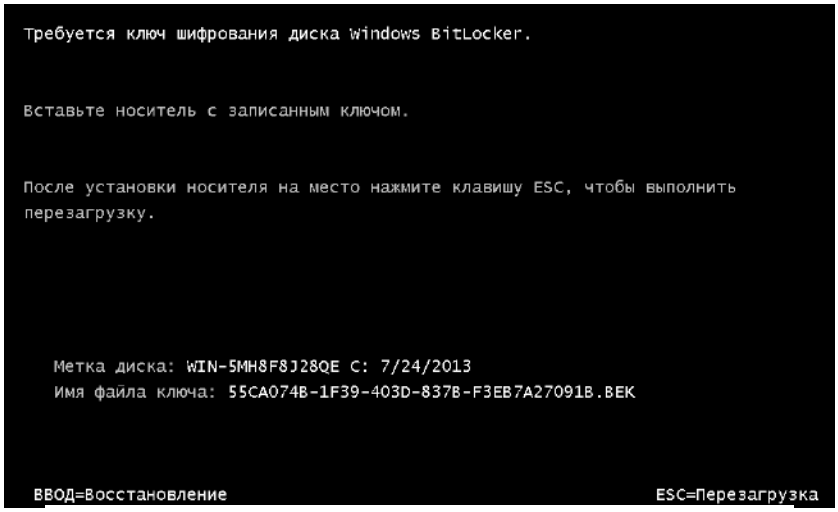


Рис. 2.24. Накопитель с ключом запуска не обнаружен

Если ключ запуска был по какой-либо причине утерян, то для загрузки системы можно воспользоваться ручным вводом 48-ми значного ключа восстановления (рис. 2.25).

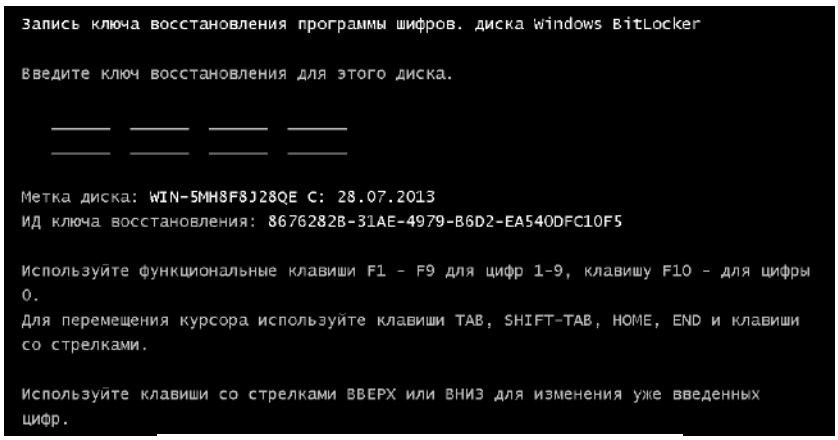


Рис. 2.25. Ввод ключа восстановления

Шифрование системного диска на виртуальной машине

Так как BIOS на виртуальной машине в VMWare Player не поддерживает чтение USB-устройств в загрузочной среде, то продолжение действий процедуры шифрования после выполнения подготовки диска не приведет к положительному результату (отобразится ошибка). Поэтому просто отмените продолжение процедуры шифрования системного диска (рис. 2.26).

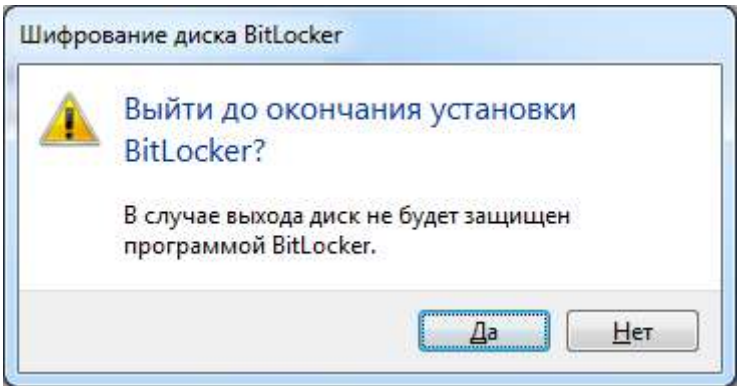


Рис. 2.26. Отмена процедуры шифрования системного диска

Чтобы зашифровать системный диск на виртуальной машине для сохранения ключа воспользуемся носителем другого типа, нежели USB-накопитель. Для этого необходимо сделать носителем, хранящим ключ запуска операционной системы, обычную дискету (загрузка с дискеты поддерживается на виртуальной машине). Чтобы осуществить это используем непосредственно командную строку, а не инструмент «Шифрование диска BitLocker». Также необходимо, чтобы BIOS был настроен на загрузку сначала с жесткого диска, а затем с дискеты.

Для того чтобы создать образ дискеты откройте меню программы VMWare Player, нажав кнопку «Player», и откройте настройки виртуальной машины, выполнив команду «Manage/Virtual Machine Settings…» (рис. 2.27).

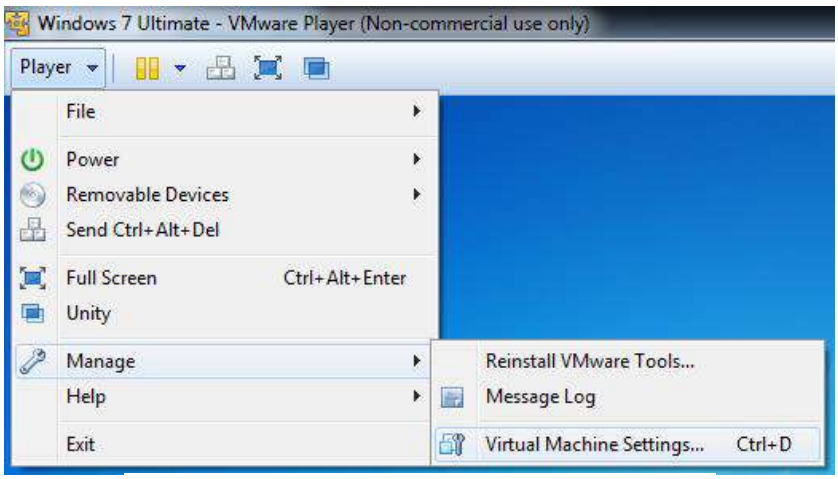


Рис. 2.27. Настройки виртуальной машины

В открывшемся окне настроек виртуальной машины перейдите во вкладке «Hardware» на пункт «Floppy». Отметьте пункт «Use floppy image drive» и создайте образ дискеты, нажав кнопку «Create…». Также отметьте пункт «Connected», чтобы подключить созданную дискету к виртуальной машине (рис. 2.28). Нажмите кнопку «ОК».

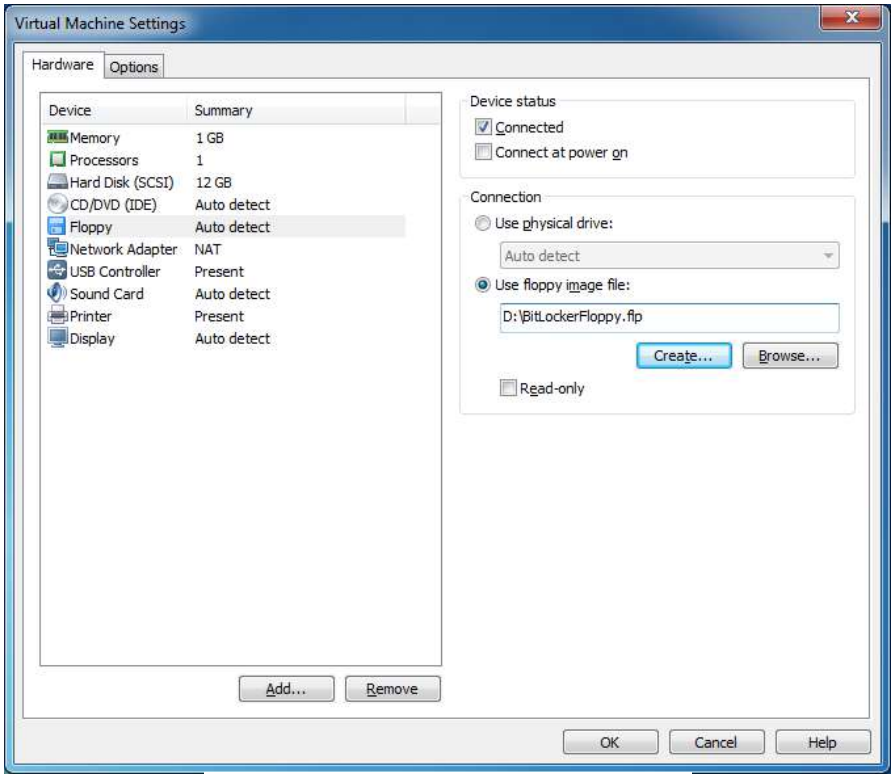


Рис. 2.28. Создание образа дискеты

После откройте дисковод A и отформатируйте дискету (рис. 2.29).

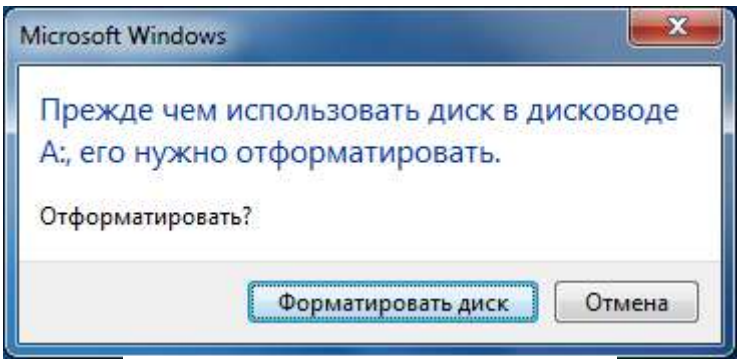


Рис. 2.29. Форматирование дискеты

Теперь можно приступить к шифрованию системного диска. Откройте меню «Пуск», в поле поиска введите «cmd». Запустите командную строку от имени администратора (рис. 2.30).

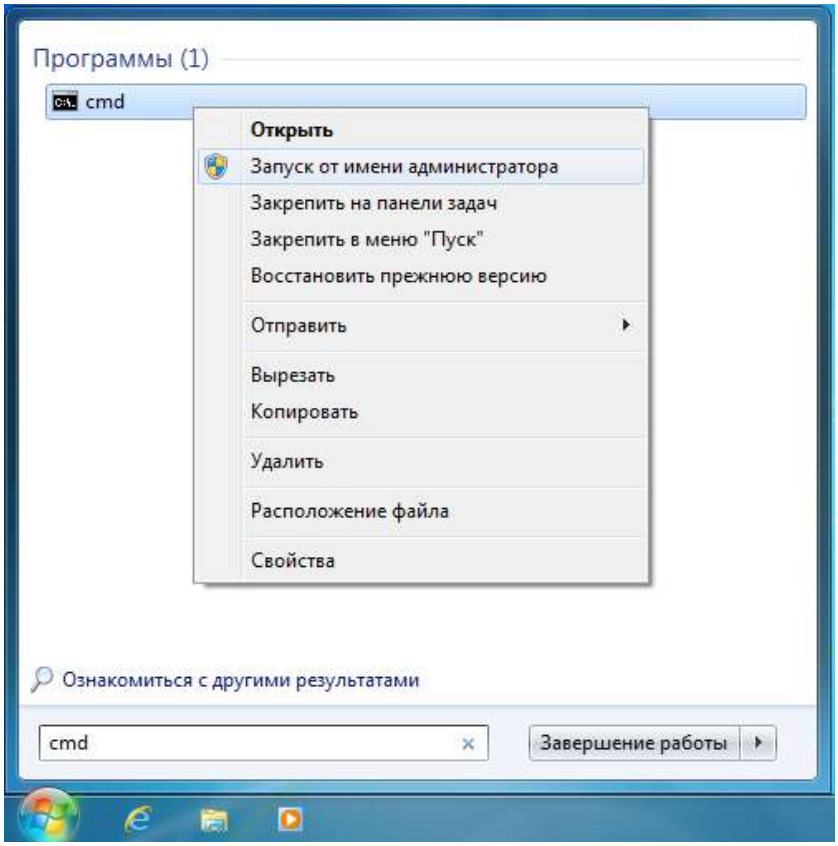


Рис. 2.30. Запуск командной строки от имени администратора

В командной строке введите следующую команду (рис. 2.31):
cscript C:\Windows\system32\manage-bde.wsf -on C: -rp -sk A:

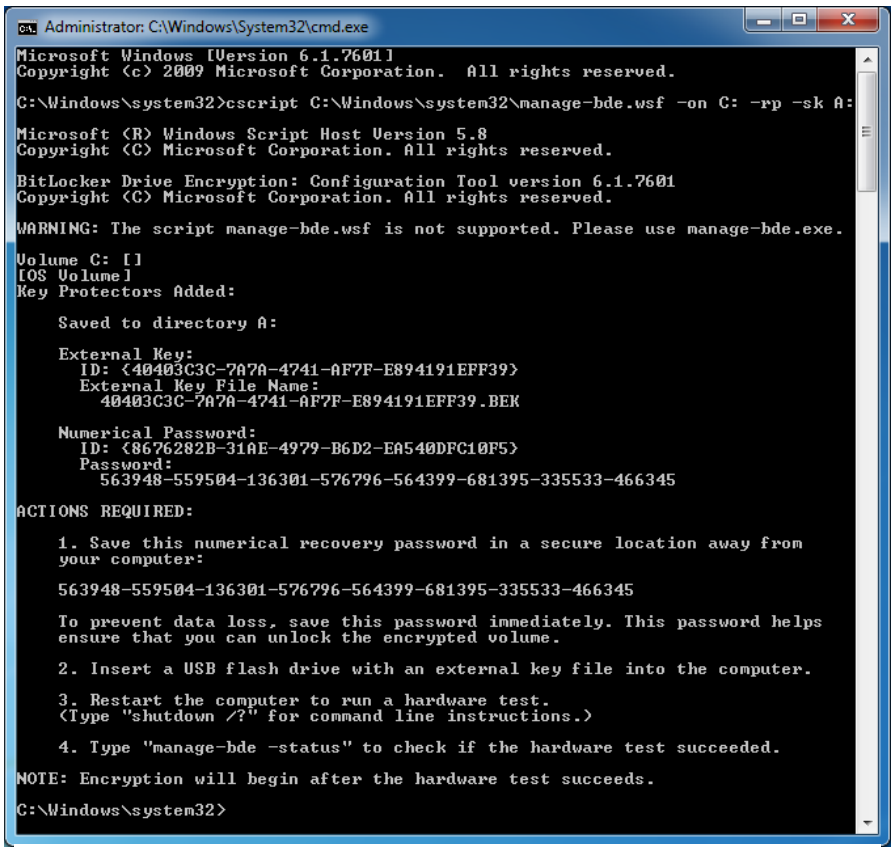


Рис. 2.31. Ввод команды на создание ключа запуска на дискете

Запишите полученный 48-мизначный ключ восстановления (recovery password) в любом месте, кроме жесткого диска виртуальной машины! Лучше всего записать его либо на бумаге, либо сохранить на жестком диске системы, из которой производится запуск виртуальной машины.

После выполнения команды появится запрос на перезагрузку компьютера для начала шифрования BitLocker (рис. 2.32). Выполните перезагрузку системы.

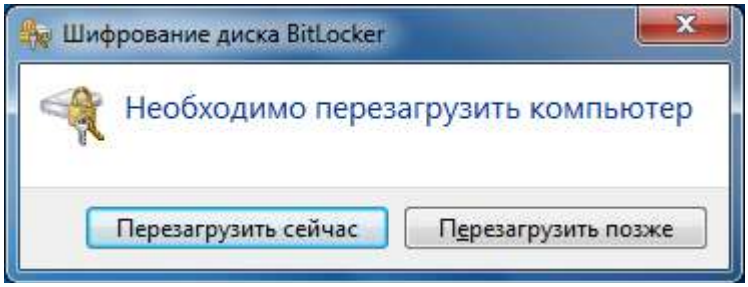


Рис. 2.32. Запрос на перезагрузку для начала шифрования BitLocker

Шифрование системного диска начнется сразу же после загрузки системы (рис. 2.33). Процесс шифрования занимает некоторое время, зависящее от объема диска.

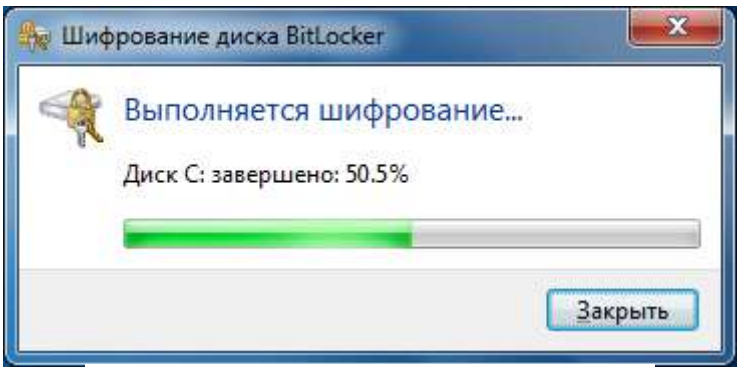


Рис. 2.33. Шифрование системного диска

После завершения процедуры шифрования проверьте работу зашифрованной системы. Отсоедините дискету с ключом запуска. Для этого снова откройте настройки виртуальной машины и снимите отметку с пункта «Connected» для дискеты. Далее выполните перезагрузку системы. При начале загрузки системы отобразится сообщение о том, что не был подключен накопитель с ключом запуска (рис. 2.34).

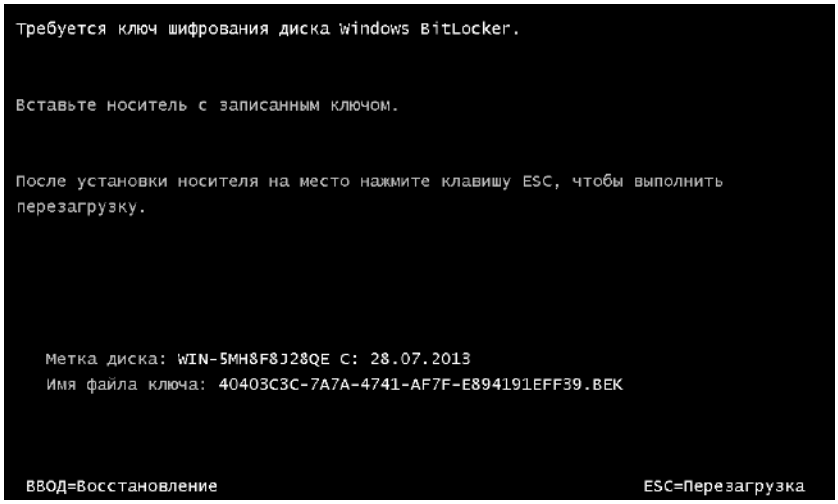


Рис. 2.34. Запрос на подключение носителя с ключом запуска

Подсоедините дискету и нажмите Esc. Операционная система запустится.

Если же по какой-либо причине был утерян ключ запуска или сам носитель с ключом запуска, то можно воспользоваться ключом восстановления. Для этого снова отсоедините дискету и перезагрузите систему. В окне запроса носителя с ключом запуска нажмите Enter, откроется окно с вводом ключа восстановления. Введите 48-мизначный ключ восстановления, указанный системой до выполнения шифрования системного диска (рис. 2.35). После ввода правильного ключа восстановления выполнится запуск операционной системы.

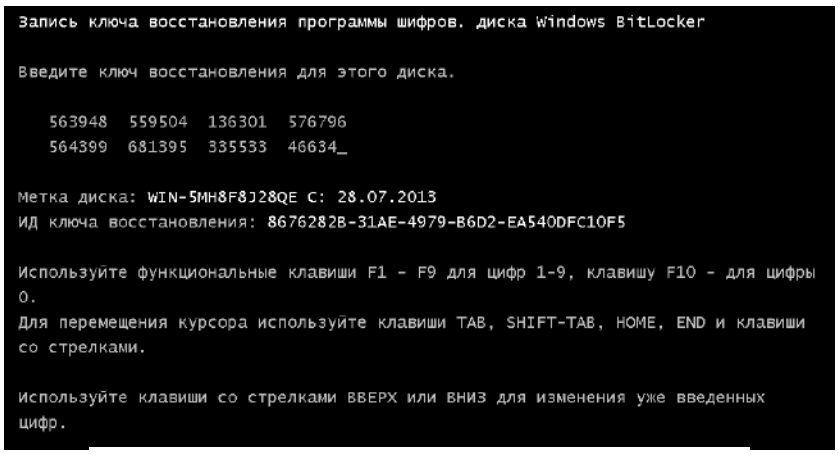


Рис. 2.35. Запрос на ввод ключа восстановления

Контрольные вопросы:

1) В каких версиях Windows присутствует технология шифрования дисков BitLocker?

2) В чем отличие BitLocker от EFS?

3) Какой алгоритм шифрования применяется в BitLocker?

4) Для чего используется функция BitLocker To Go?

5) Какие режимы работы системы шифрования возможны для шифрования системных дисков?

6) Что такое TPM?

Лабораторная работа № 7
Применение шифрования и электронной подписи в электронном документообороте

Цель работы

Целью данной лабораторной работы является изучение специфики работы криптосистем с открытым ключом на примере работы с клиентом электронной почты «The Bat!». В рамках данной работы предусмотрено изучение таких возможностей программы, как:

- шифрование писем
- подпись писем
- расшифровывание полученного письма
- проверка подписи у полученного письма

Ход работы

Наиболее широкое распространение в мире имеют асимметричные криптосистемы, также иначе называемые криптографическими системами с открытым ключом. Под данным понятием имеется в виду система шифрования и/или цифровой подписи (ЦП), при которой ***открытый ключ*** передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЦП и для шифрования сообщения. Тогда как для генерации ЦП и для расшифровки сообщения используется ***секретный ключ***.

Данный вид криптосистем наиболее часто используется в различных сетевых протоколах, таких как TLS и его предшественнике *SSL*. Также асимметричная криптосистема используется в библиотеке функций PGP и стандарте для шифрования и подписи в электронной почте S/MIME.

TLS (*Transport Layer Security* — безопасность транспортного уровня), как и его предшественник ***SSL*** (*Secure Socket Layers* — уровень защищенных сокетов) — криптографические протоколы, обеспечивающие защищённую передачу данных между узлами в сети Интернет.

PGP (*Pretty Good Privacy* – «действительно хорошая защита») – библиотека функций, позволяющая выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде.

S/MIME (*Secure / Multipurpose Internet Mail Extensions*– «безопасность/многоцелевое расширение интернет-почты») — стандарт для шифрования и подписи в электронной почте с помощью открытого ключа.

Данная лабораторная работа полностью выполняется на виртуальной машине с установленной операционной системой Windows XP. Для работы потребуется установить почтовый клиент “The Bat!”. Запустим файл thebat_rus_5-2-2.msi. Откроется окно установщика, где нам будет предложено принять лицензионное соглашение для продолжения установки. В качестве вида установки – выберем полную версию программы. После чего будет предложено установить программу на компьютер, и выдано сообщение об успешном завершении процедуры.

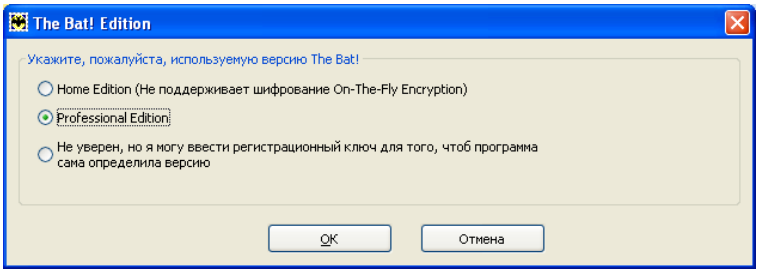


Рис.1 – Выбор версии программы

При первом запуске программа предлагает пользователю уточнить то, где будут храниться файлы почты. В случае, если есть необходимость выбрать нестандартное месторасположение – существует ряд вариантов.

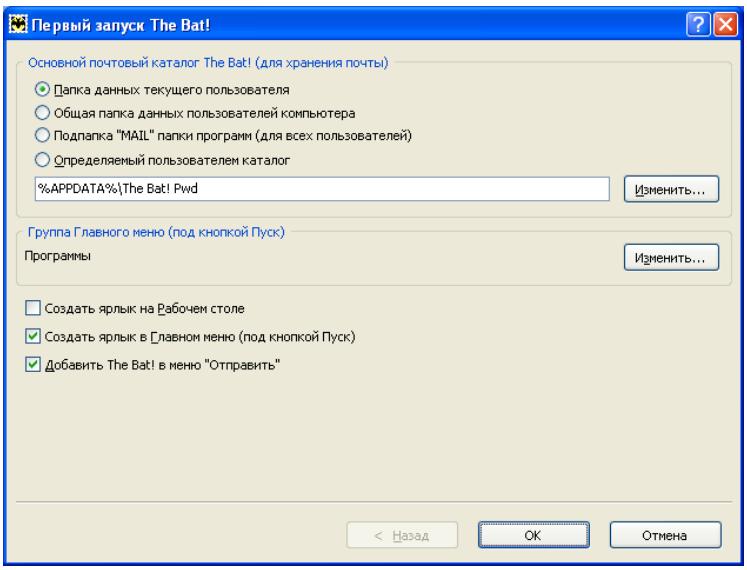


Рис.2 – Первый запуск

Согласно встроенным параметрам – пользователю предоставляется возможность защитить свои почтовые ящики на данном компьютере. Для чего предлагается несколько путей решения данного вопроса:

1) Задать мастер-пароль
2) Использовать USB ключ eToken
3) Использовать USB ключ iKey1000

Поскольку в данной работе нами изучается не принцип защиты данных посредством USB-ключей, а технология защиты писем в программе почтового клиента, программа будет защищена мастер-паролем.

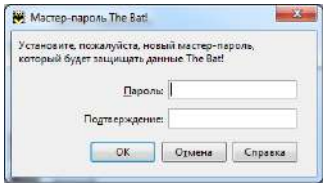


Рис.3 – Окно создания мастер-пароля

Для дальнейшего осуществления работы с программой теперь будет нужно вводить мастер-пароль при всех действиях с почтовыми ящиками и с настройками почтового клиента «The Bat!».

Рис.4 – Окно ввода мастер-пароля для входа в систему

Поскольку до этого в системе не было почтового клиента, либо был использован другой – программа сообщит об изменении ассоциаций.

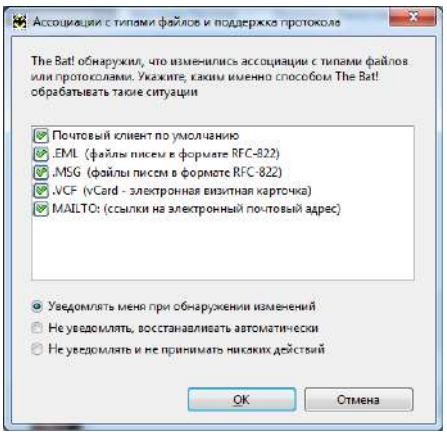


Рис.5 – Уведомление об изменении ассоциаций

В программе существует возможность восстановления почтового ящика из резервной копии. Нами будет создан новый, e-mail адресом которого будет Ваш адрес на students.isib.su (начиная с 2012-го года студенты кафедры КИБЭВС автоматически получают персональный e-mail адрес, совпадающий с именем учетной записи). В случае если Вы выберете другой почтовый сервер – Вы должны быть уверены, что сможете настроить использование протоколов соединения отправки и получения писем.

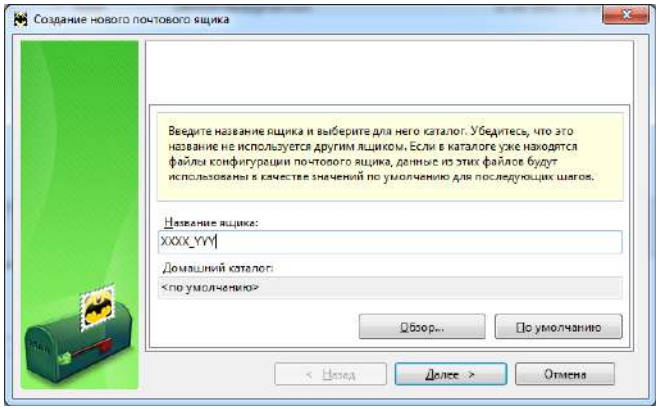


Рис.6 – Название основано на логине студента

Для удобства назовем почтовый ящик так же, как и логин учетной записи, где XXXX – номер группы, а YYY – инициалы студента.

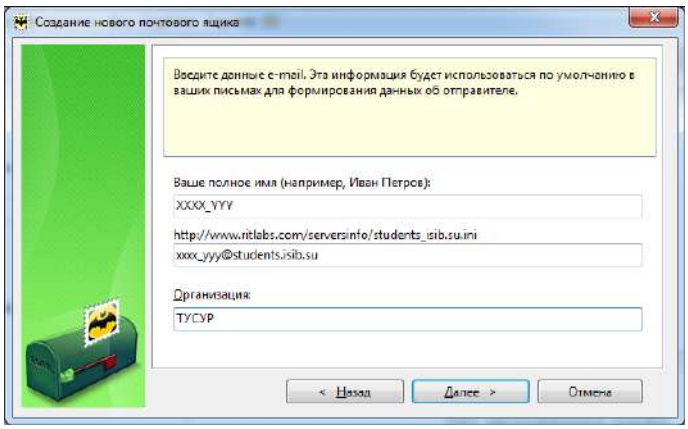


Рис.7 – Задание e-mail адреса

Остановимся на выборе доступа к серверу через протокол. Программа поддерживает следующие три вида протоколов:

- ***POP3*** (*Post Office Protocol Version 3*) — стандартный Интернет-протокол прикладного уровня, используемый клиентами электронной почты для извлечения электронного сообщения с удаленного сервера по TCP/IP-соединению.
- ***IMAP*** (*Internet Message Access Protocol*) — протокол прикладного уровня для доступа к электронной почте. Базируется на транспортном протоколе TCP и использует порт 143. Почтовая программа, использующая этот протокол, получает доступ к хранилищу корреспонденции на сервере так, как будто эта корреспонденция расположена на компьютере получателя. Электронными письмами можно манипулировать с компьютера пользователя (клиента) без постоянной пересылки с сервера и обратно файлов с полным содержанием писем.
- ***MAPI*** (*Messaging Application Programming Interface*) — программный интерфейс, позволяющий приложениям работать с различными системами передачи электронных сообщений. MAPI позволяет получать, читать, создавать, отправлять сообщения, присоединять к ним файлы, получать доступ к присоединенным файлам и т. д.

Для передачи сообщений используется протокол ***SMTP***. SMTP (*Simple Mail Transfer Protocol*) — это широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP. В то время, как электронные почтовые сервера и другие агенты пересылки сообщений используют SMTP для отправки и получения почтовых сообщений, клиентские почтовые приложения обычно используют SMTP только для отправки сообщений на почтовый сервер для ретрансляции.

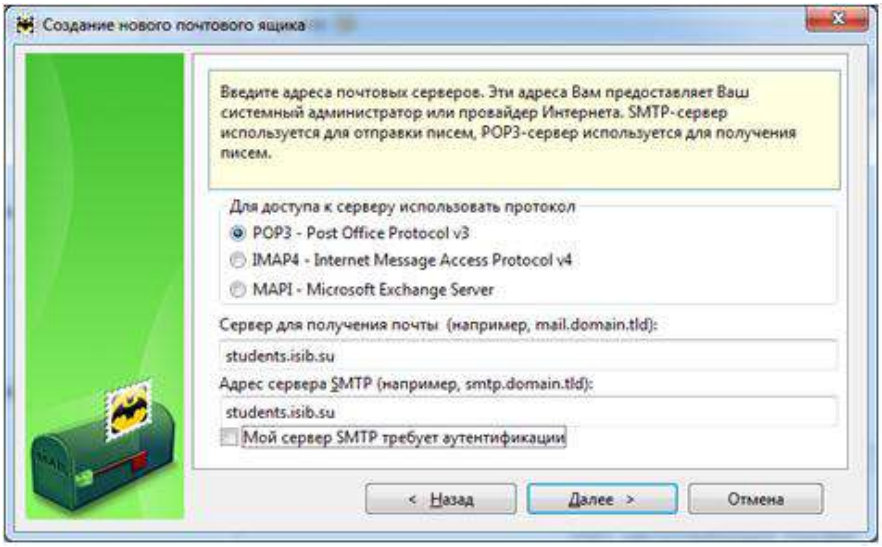


Рис.8 – Выбор способа доступа по протоколу

После чего укажем пароль для данного e-mail адреса и укажем, что письма необходимо оставлять на сервере. Иначе при запуске программы все письма окажутся в памяти компьютера и в случае утраты доступа к нему или по истечению срока доступа к программе – письма будут потеряны.

Кроме того, программа предоставляет возможность использовать шифрованный метод аутентификации ***APOP***. По умолчанию сервер POP посылает все пароли открытым текстом (т.е. незашифрованными). Если Вас волнуют вопросы защиты, то пересылка по сети паролей в открытом виде, безусловно, недопустима, а при аутентификации требуется более жёсткий контроль. В таком случае нужна поддержка APOP.

Это организовано следующим образом: сервер посылает вызов подключающемуся клиенту. Клиент присоединяет пароль пользователя к этому вызову, затем шифрует его с использованием MD5 и посылает хеш обратно на сервер. Затем сервер сравнивает ответ клиента со своим собственным расчётным значением контрольной суммы (параметры вызова + пароль пользователя). Если они совпадают, клиент считается опознанным и регистрируется на сервере POP3.

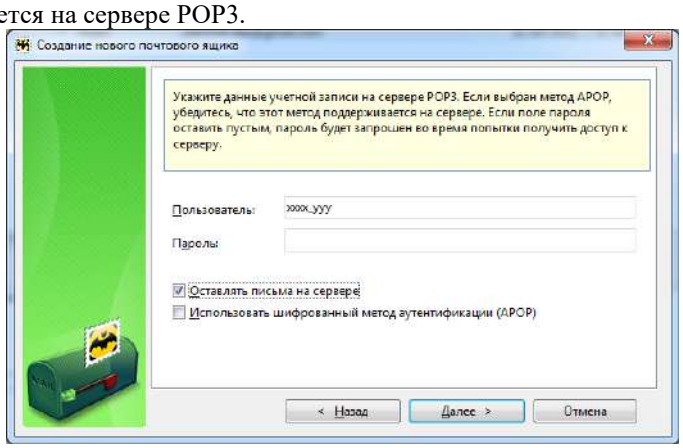


Рис.9 – Задание логина, пароля и параметров

Программа предложит проверить прочие свойства почтового ящика, где среди прочего будет представлена возможность изменить настройки соединения с почтовым сервером. В случае необходимости проверки свойств ящика – можно их открыть в любой момент, выбрав соответствующее меню в меню «Ящик». Проверьте, чтобы у SMTP порт был равен 25, POP3 – 110, IMAP – 143. Эти номера портов соответствуют официально принятому перечню в перечне зарегистрированных портов ***IANA*** (*Internet Assigned Numbers Authority* — «Администрация адресного пространства Интернет»).

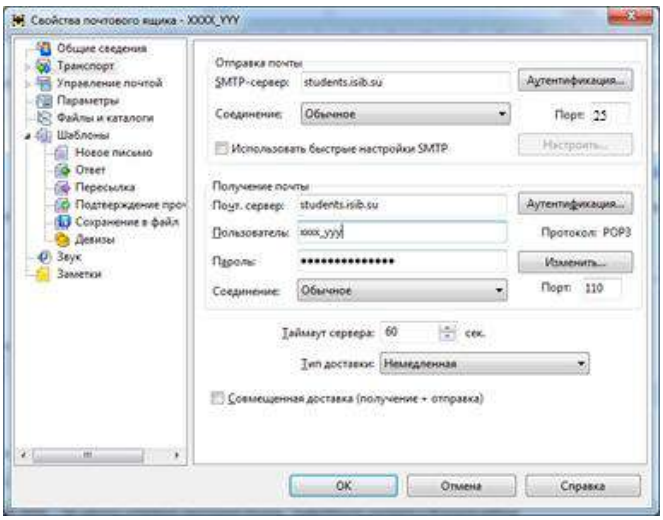


Рис.10 – Проверка свойств почтового ящика.

Приступим к непосредственному изучению возможностей The Bat. Для этого первым делом протестируем возможность пересылки писем программой. Интерфейс программы ориентирован на простого пользователя, и все необходимые функции находятся на первом плане.

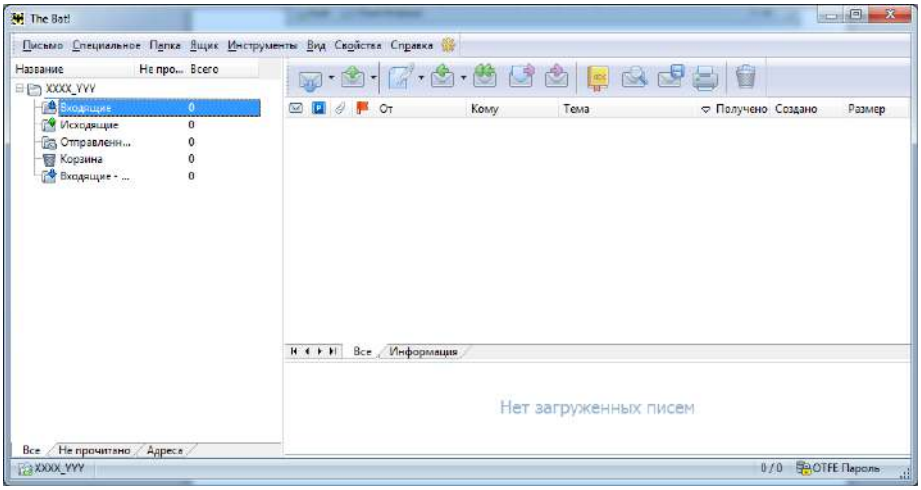


Рис.11 – Интерфейс программы

Для того, чтобы создать новое письмо, нажмите на иконку  . После этого откроется редактор письма. В качестве адресата используйте адрес кого-нибудь из группы и отправьте этому человеку простое письмо. В случае, если письмо от Вас было отправлено, а у другого человека прекрасно получено – перейдем к созданию комплектов ключей для каждого из участников общения. Если возникли ошибки при соединении с сервером – это будет отображено в журнале работы, вызвать который можно при помощи соответствующего пункта в меню «Ящик».

Перейдем к рассмотрению реализации защиты данных в рассматриваемой программе. В программу встроена возможность использовать ключи ***PGP***. (*Pretty Good Privacy* – действительно хорошая защита). В том числе создавать их, принимать и следить за их состоянием.

Для того чтобы создать новый комплект ключей, создадим новое письмо и в меню «Криптография и безопасность» выберем пункт «Управление ключами OpenPGP».

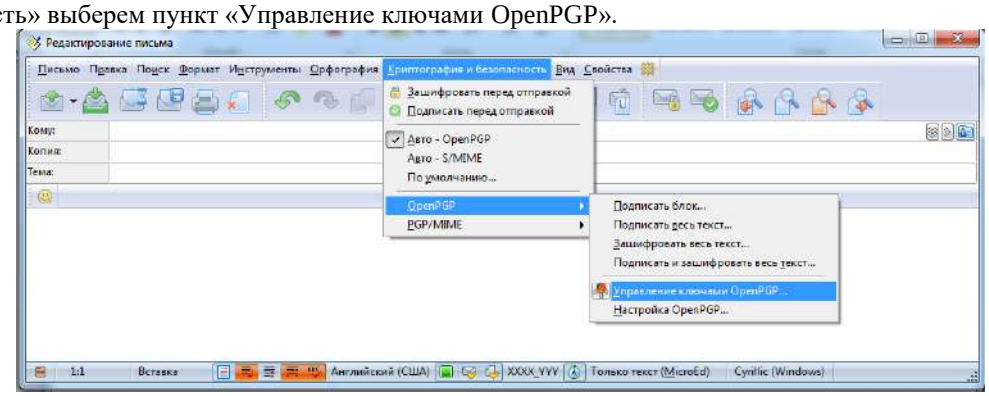


Рис.12 – Выбор пункта

Стоит отметить, что в программе есть возможность использовать ***MIME*** (сокращение для ***Multipurpose Internet Mail Extensions*** – многоцелевое расширение для интернет-почты). Стандарт PGP/MIME обеспечивает безопасный обмен электронной почтой в соответствии с:

- RFC 1991 PGP Message Exchange Formats
- RFC 2015 MIME Security with Pretty Good Privacy (PGP)
- RFC 2440 OpenPGP Message Format
- RFC 3156 MIME Security with OpenPGP

Согласно комментариям производителей использование PGP/MIME для шифрования и подписи почты обеспечивает большую гибкость и удобство.

В открывшейся библиотеке ключей OpenPGP на данный момент находится лишь ключ компании-разработчика The Bat.

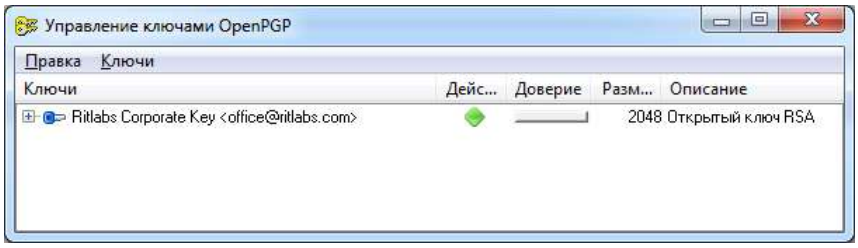


Рис.13 – Библиотека ключей

Выберем в пункте «Ключи» подпункт «Создать новую пару ключей…».

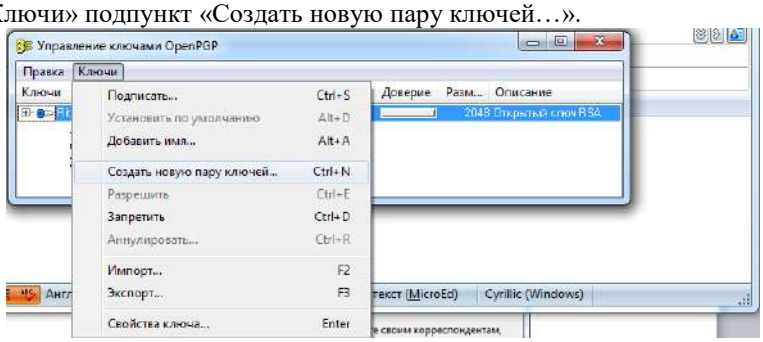


Рис.14 – Создание ключей

Программа откроет мастер создания ключей, где для указанного в созданном почтовом ящике e-mail адреса будет создан комплект ключей по указанным пользователем параметрам. В частности указать размер ключа, срок его действия и пароль для использования ключа.

Как видно из предложенного перечня размеров ключей – в программе реализована защита для зашифрованных писем настолько сильная, что методом «грубой атаки» ее не взломать. Поскольку минимальный размер ключа, которого достаточно для защиты – 768 бит. Группе инженеров из Японии, Швейцарии, Нидерландов и США в 2010 году удалось успешно вычислить данные, зашифрованные при помощи криптографического ключа стандарта RSA длиной 768 бит.

Рис.15 – Выбор размера ключа

Чем короче срок действия ключей и чем чаще они меняются – тем выше защищенность данных и меньше шансы для взлома их со стороны злоумышленников. Соответственно, предпочтительней выбирать короткие сроки жизни ключей. Что хоть и вызовет ряд неудобств, но является необходимой мерой защиты.

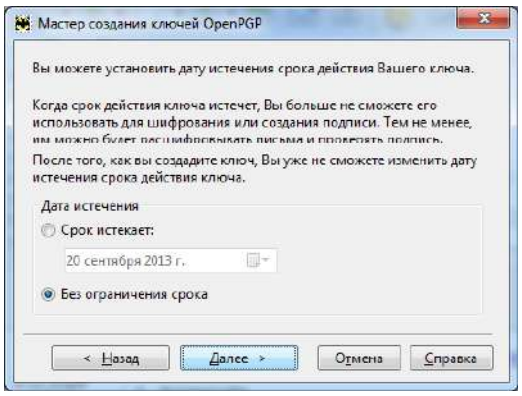


Рис.16 – Выбор срока действия ключа

Для создания ключевой пары немаловажен пароль, по которому она создается. Следует учесть, что пароль должен быть таким, чтобы его ввод все же не приносил пользователю слишком много неудобств и его не приходилось хранить записанным на листке или в файле. Этот пароль будет необходим при проверке подписи и расшифровывании писем.

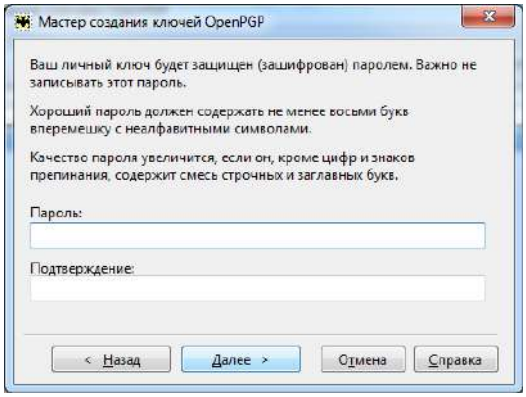


Рис.17 – Выбор пароля для ключей

После с помощью набора случайных чисел, для получения которых потребуется или водить курсором по окну программы или нажимать клавиши, будет сформирован конечный ключ. В результате нами буден получен комплект ключей, который можно использовать при общении с другими пользователями в защищенном режиме.

Полученная пара ключей появится в библиотеке имеющихся ключей, где пользователь может просмотреть их свойства, скопировать, экспортировать или импортировать, выбрав соответствующий пункт в меню.

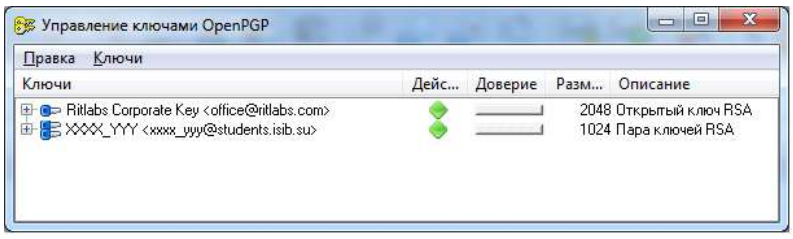


Рис.18 – Библиотека ключей с созданным ключом

В свойствах ключа можно просмотреть тип полученного ключа, его размер, срок действия, дату создания и основные параметры доверия данному ключу, а также изменить пароль или степень доверия.

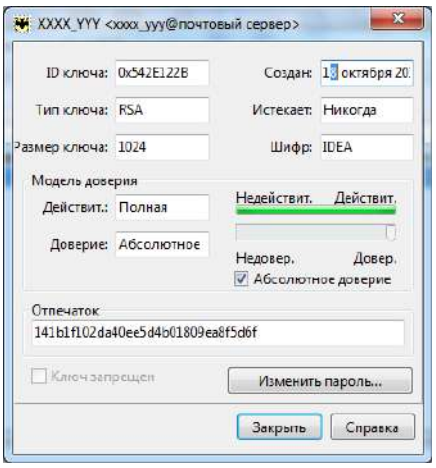


Рис.19 – Свойства ключа

Выберем в библиотеке ключей созданный ключ правой кнопкой и выберем пункт «Копировать». После чего вставим в содержимое письма полученную информацию. В результате в тексте письма появится открытый ключ, необходимый собеседникам, чтобы присылать нам зашифрованное и (или) подписанное письмо. Отправим данное письмо собеседникам.

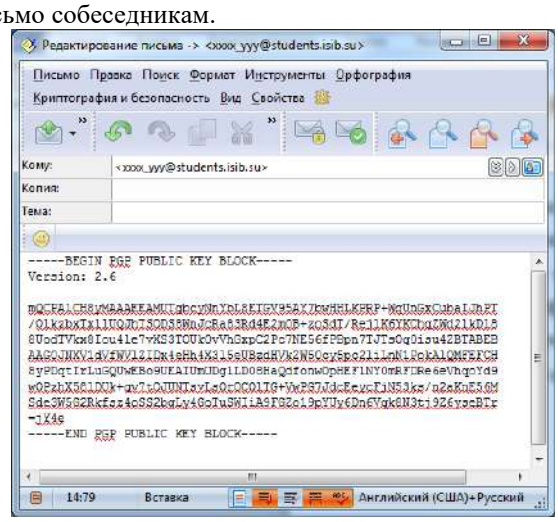


Рис.20 – Текст письма с открытым ключом

Собеседники, в свою очередь, будут вынуждены прислать Вам свои открытые ключи. Чтобы из полученного письма с ключом выделить необходимую информацию и сохранить в библиотеку ключей выберем пункт «Импортировать ключ (сертификат)» в меню «Криптография и безопасность» или нажмем на значок ключей справа от заголовка письма. Возможно сохранить текст письма в файл и импортировать напрямую из библиотеки ключей.

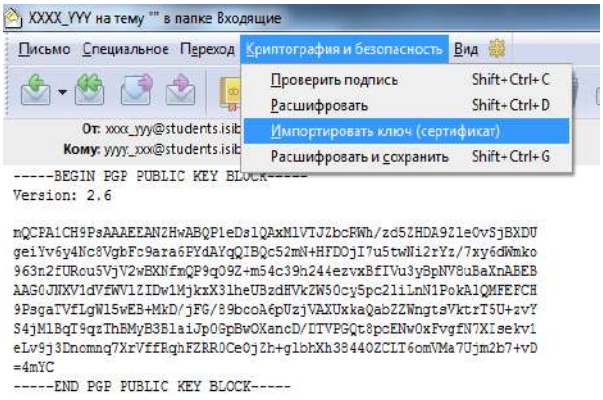


Рис.21 – Импорт ключа из письма

XXXX – номер группы отправителя. YYY – инициалы отправителя
YYYY – номер группы получателя. XXX – инициалы получателя

В результате откроется окно, где будут указаны все возможные ключи для импорта (а их может быть несколько, ведь нельзя исключать возможность, что у отправителя ключей несколько).

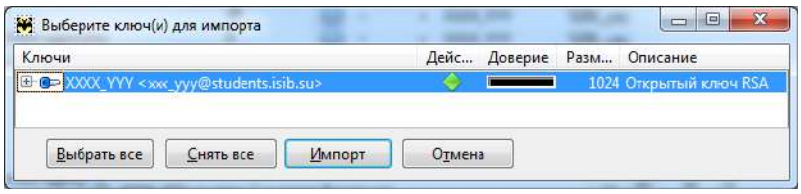


Рис.22 – Выбор импортируемых ключей

Нажмем на кнопку «Импорт». В результате данного действия в библиотеке появится ключ без доверия. Чтобы это исправить – зайдем в его свойства и поставим доверие на «абсолютное».

Открываем новое письмо и пишем любой текст, который хотим отправить тайно. После чего выбираем пункты «Зашифровать весь текст» а затем отправляем.

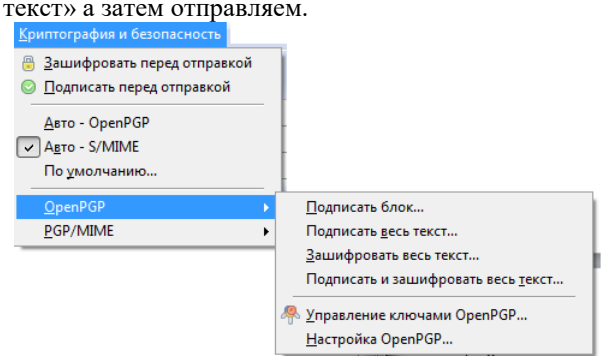


Рис.23 – Выбор шифрования или подписи

Шифрование PGP осуществляется последовательно хешированием, сжатием данных, шифрованием с симметричным ключом, и, наконец, шифрованием с открытым ключом, причём каждый этап может осуществляться одним из нескольких поддерживаемых алгоритмов. Симметричное шифрование производится с использованием одного из симметричных алгоритмов на сеансовом ключе, который генерируется с использованием криптографически стойкого генератора псевдослучайных чисел. Сеансовый ключ зашифровывается открытым ключом получателя с использованием алгоритма RSA. Каждый открытый ключ соответствует имени пользователя или адресу электронной почты.

Внутри полученного письма не будет привычного текста письма, а шифртекст. Зашифрованное сообщение будет заключено в теги, указывающие на начало и конец шифртекста. Чтобы получить содержимое – понадобится нажать на кнопку в правой части программы.

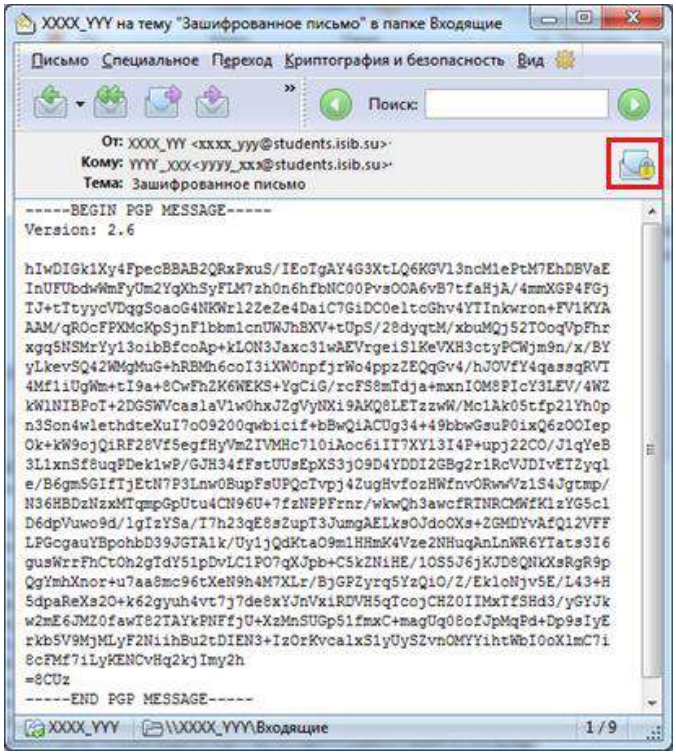


Рис.24 – Зашифрованное письмо

Программа попросит ввести пароль, дабы удостовериться, что запрос поступил от владельца ключевой пары и применение закрытого ключа правомерно и легально. В результате во вкладке «Расшифровано PGP» появится расшифрованное письмо, где будет отправленный текст.

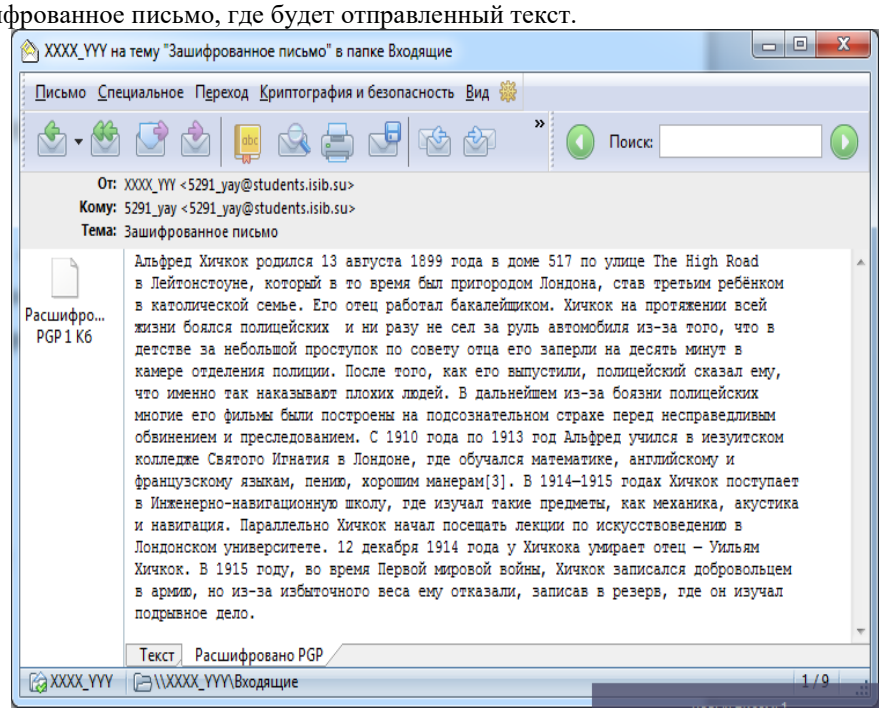


Рис.25 – Расшифрованное сообщение

А теперь проведем проверку подписи. Отправим тоже письмо, но выберем пункт «Подписать весь текст» в меню «Криптография и безопасноть» – «OpenPGP». Перед текстом появится тег, с которого начнется подписанное сообщение с указанием алгоритма хеширования (MD5), следом текст письма без преобразований и в конце хеш-значение письма.

MD5 (*Message Digest 5*) — устаревший, криптографически взломанный, 128-битный алгоритм хеширования, разработанный в 1991 году. Предназначен для создания «отпечатков» или дайджестов сообщения произвольной длины и последующей проверки их подлинности. Полученное хеш-значение подписывается цифровой подписью при помощи закрытого ключа отправителя. Шифруется не открытый текст сообщения, а его дайджест (хеш-значение), что дает большой выигрыш во времени.

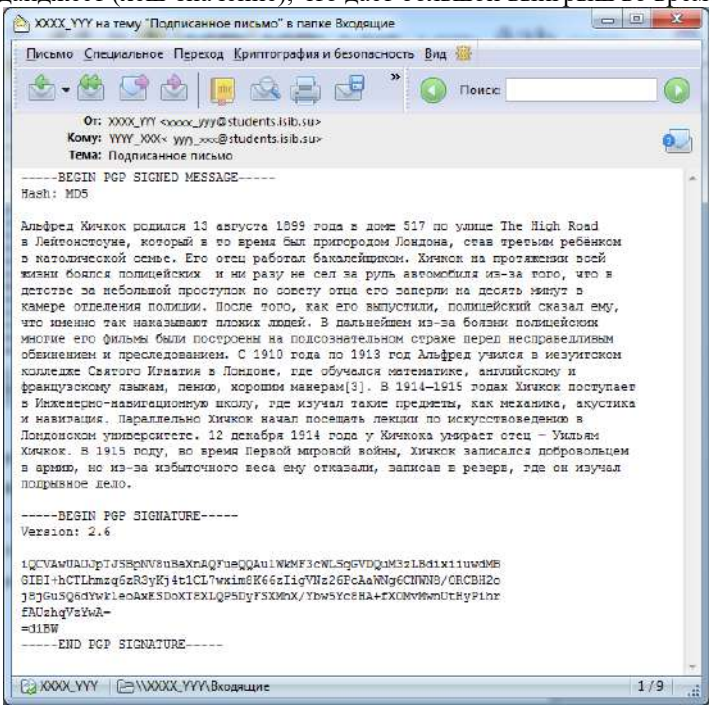


Рис.26 – Подписанное письмо

Чтобы проверить подпись – достаточно нажать на кнопку в правой части программы или выбрать в разделе «Криптография и безопасность» пункт «Проверить подпись». В истории проверок будет показана дата совершения подписи, кому она принадлежит и действительность хеша.

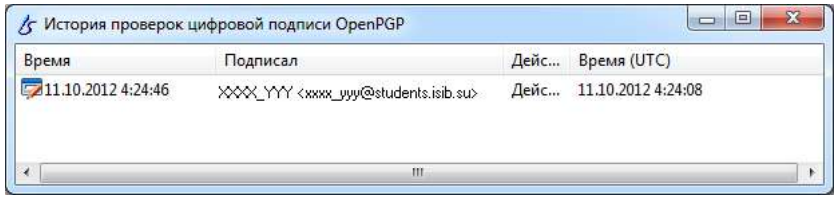


Рис.27 – Проверка подписей

ЛАБОРАТОРНАЯ РАБОТА

Шифрование электронных писем в Mozilla thunderbird.

1. Цель работы

Целью работы является получение навыка отправления зашифрованных и электронно подписанных сообщений при помощи приложений Mozilla thunderbird, Enigmail.

2. Краткие теоретические сведения

Электронная подпись – это особый реквизит документа, который позволяет установить отсутствие искажения информации в электронном документе с момента формирования ЭП и подтвердить принадлежность ЭП владельцу. Значение реквизита получается в результате криптографического преобразования информации.

Сертификат электронной подписи – документ, который подтверждает принадлежность открытого ключа (ключа проверки) ЭП владельцу сертификата. Выдаются сертификаты удостоверяющими центрами (УЦ) или их доверенными представителями.

Владелец сертификата ЭП – физическое лицо, на чье имя выдан сертификат ЭП в удостоверяющем центре. У каждого владельца сертификата на руках два ключа ЭП: закрытый и открытый.

Закрытый ключ электронной подписи (ключ ЭП) позволяет генерировать электронную подпись и подписывать электронный документ. Владелец сертификат обязан в тайне хранить свой закрытый ключ.

Открытый ключ электронной подписи (ключ проверки ЭП) однозначно связан с закрытым ключом ЭП и предназначен для проверки подлинности ЭП.

Mozilla Thunderbird – общедоступное ПО, использующее открытый код для работы с электронной почтой. Оно поддерживает работу с несколькими учетными записями разных провайдеров e-mail почты.Так же данное ПО может использовать расширения **Enigmail** и **GnuPG** для повышения уровня защищенности и приватности отправляемых сообщений. С их помощью можно реализовать шифрование OpenPGP в **Thunderbird**. Кроме того, можно подписывать сообщения, а также осуществлять проверку на подлинность других цифровых подписей.

Enigmail – дополнение к Thunderbird, которое позволяет работать с шифровальными возможностями GnuPG прямо из Thunderbird.

GNU Privacy Guard (GnuPG) – бесплатная шифровальная программа с открытым кодом, предназначенная для шифрования, расшифровки и создания цифровой подписи (как для текстовых сообщений, так и для файлов) **GnuPG** основана на принципе *криптографии с открытым ключом*. Каждый пользователь создает собственную пару *ключей*. Эту *пару ключей* можно использовать для шифрования, расшифровки и цифровой подписи. В паре два ключа: *секретный* и *открытый ключ*.

- *Секретный ключ* обеспечивает возможность читать зашифрованные (парным ему) *открытым ключом*, Также на основе секретного ключа осуществляется электронная подпись писем. Поэтому секретный ключ следует хранить в надежном месте. Для обеспечения безопасности *секретного ключа*, при доступе к нему осуществляется дополнительный этап аутентификации (необходимо ввести пароль, задаваемый на этапе создания *пары ключей*).
- С помощью уже **открытого ключа** создаются зашифрованные сообщения, расшифровать которые можно лишь при обладании ***парным ему секретным ключом.*** *Открытый ключ* не подходит для чтения зашифрованных сообщений или создания электронной подписи. Таким образом, правило простое: хотите зашифровать кому-нибудь письмо – при шифровании воспользуйтесь открытым ключом этого человека.

Дополнения **GnuPG** и **Enigmail** позволяют реализовывать процесс ***электронной подписи*** отправляемых писем. При этом используется ***секретный ключ***, так, для проверки подлинности электронной подписи, будет использоваться уже ***парный ему открытый ключ.*** Так если вы хотите, чтобы сторонний человек смог удостовериться в подлинности вашей электронной подписи, ему необходимо обладать вашим *открытым ключом*. И наоборот: если у вас есть чей-то *открытый ключ*, вы можете проверять его цифровые подписи.

3. Ход работы

3.1. ДОБАВЛЕНИЕ УЧЕТНОЙ ЗАПИСИ E-MAIL В THUNDERBIRD

Для начала лабораторной работы на рабочем столе виртуальной машины, откройте Mozilla thunderbird (Рис. 1).

Рис. 1 Mozilla thunderbird

При первом запуске Mozilla thunderbird требуется добавить учетную запись e-mail (Рис. 2).

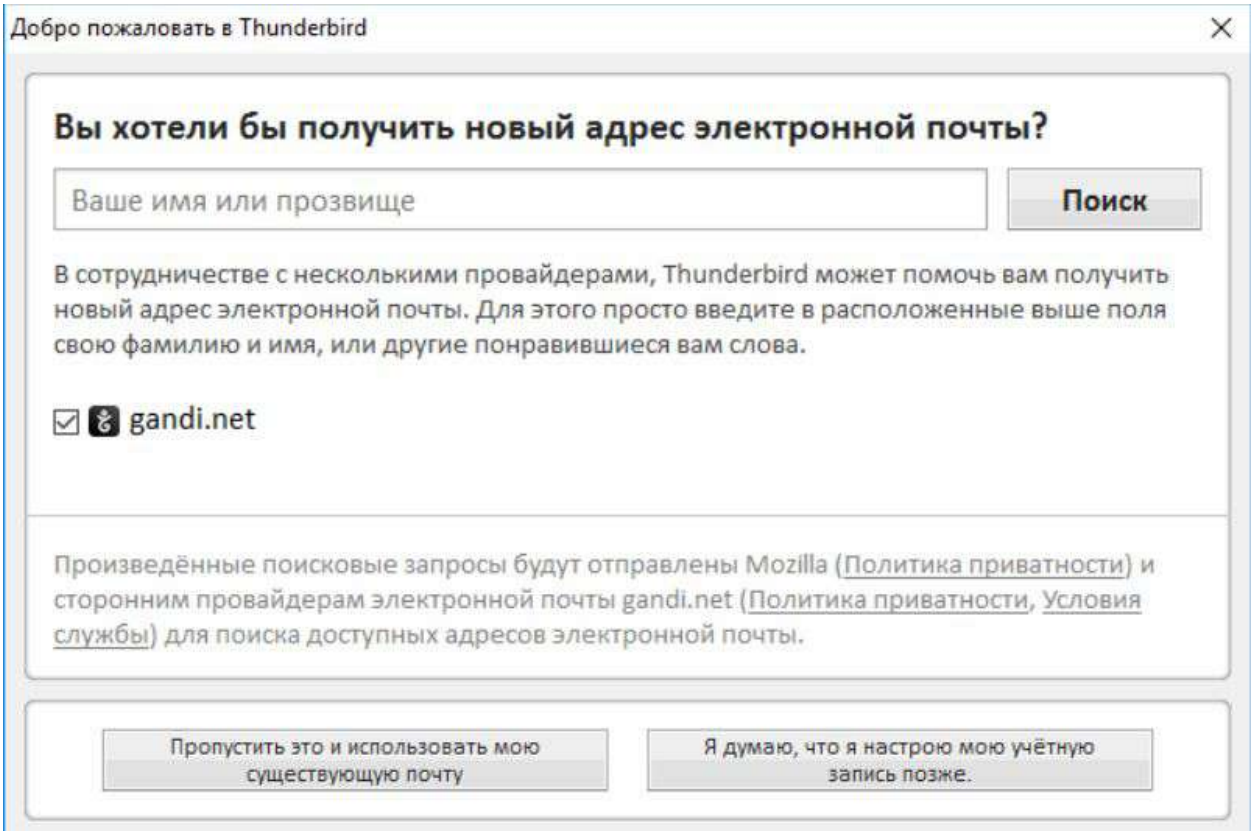


Рис. 2

Нажмите кнопку **[Пропустить это и использовать мою существующую почту]**, чтобы открыть окно настройки учетной записи.

Укажите имя, адрес e-mail и пароль для вашей учетной записи, который будете использовать в Thunderbird.

Нажмите кнопку **[Продолжить]**. Thunderbird проверит введенные вами данные(Рис.3)

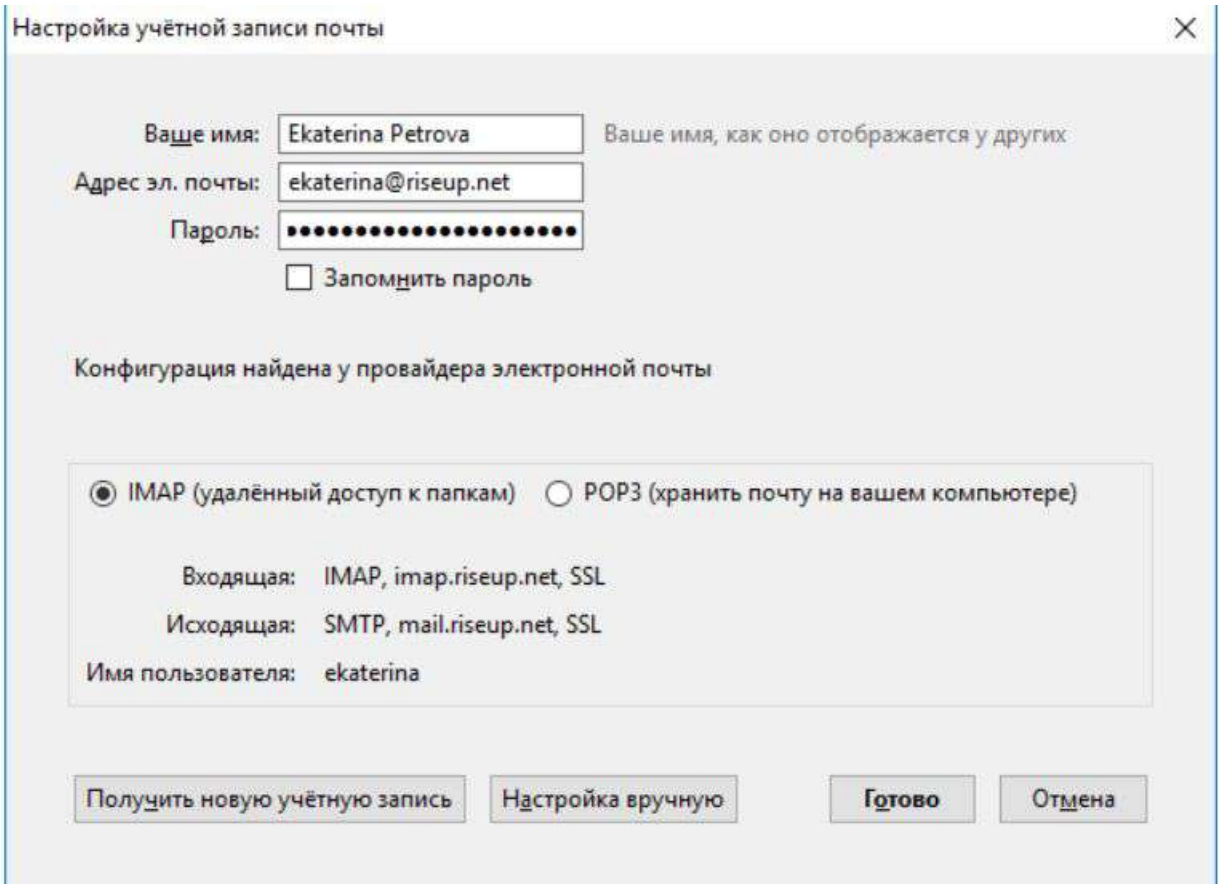


Рис. 3 Настройка учетной записи почты

Возможно, лучшим вариантом будет оставить выбор на "IMAP (удаленный доступ к папкам)". IMAP сохраняет мастер-копии ваших почтовых папок (включая папки Входящие, Черновики, Шаблоны, Отправленные и Корзина) на сервере и делает локальные копии на вашем устройстве. Это позволяет иметь доступ к одним и тем же сообщениям с разных устройств, причем данные будут синхронизироваться. Другой вариант – POP – подразумевает, что сообщения будут скачаны с сервера и сохранены на первом же устройстве. Это не значит, что они удалятся с сервера, но работать с ними, используя разные устройства, будет заметно труднее.

Важно. Убедитесь, что в полях Входящая и Исходящая (почта) есть упоминание о SSL (Secure Sockets Layer) или STARTTLS (Start Transport Layer Security). Оба варианта означают, что ваш провайдер e-mail поддерживает основы шифрования.

Нажмите кнопку **[Готово]** для создания учетной записи. Вы окажетесь в главном окне Thunderbird.

3.2 УСТАНОВКА ENIGMAIL

В Mozilla thunderbird дополнениях можно скачать актуальную версию Enigmail

Выберите в меню **Дополнения**. Появится окно управления дополнениями Thunderbird.

Наберите в поисковой строке “**Enigmail**” (правый верхний угол), **нажмите Enter**. (Рис.4)

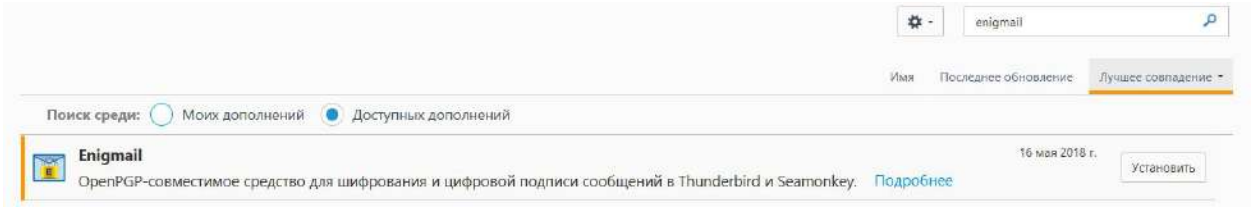


Рис. 4 поиск Enigmail

Нажмите кнопку “**Установить**” для установки Enigmail.
Когда Thunderbird установит дополнение, он известит об этом. (Рис.5)

Рис. 5 установка Enigmail

ссылку *Перезапустить сейчас* для перезапуска Thunderbird и окончания установки Enigmail.

Когда **Thunderbird** перезагрузится, он автоматически запустит настройку Enigmail, и вы сможете создать свои шифровальные ключи

3.3 СОЗДАНИЕ ШИФРОВАЛЬНЫХ КЛЮЧЕЙ

Выберите **[Enigmail > Мастер установки]**. Откроется мастер установки GnuPG. (Рис.6)

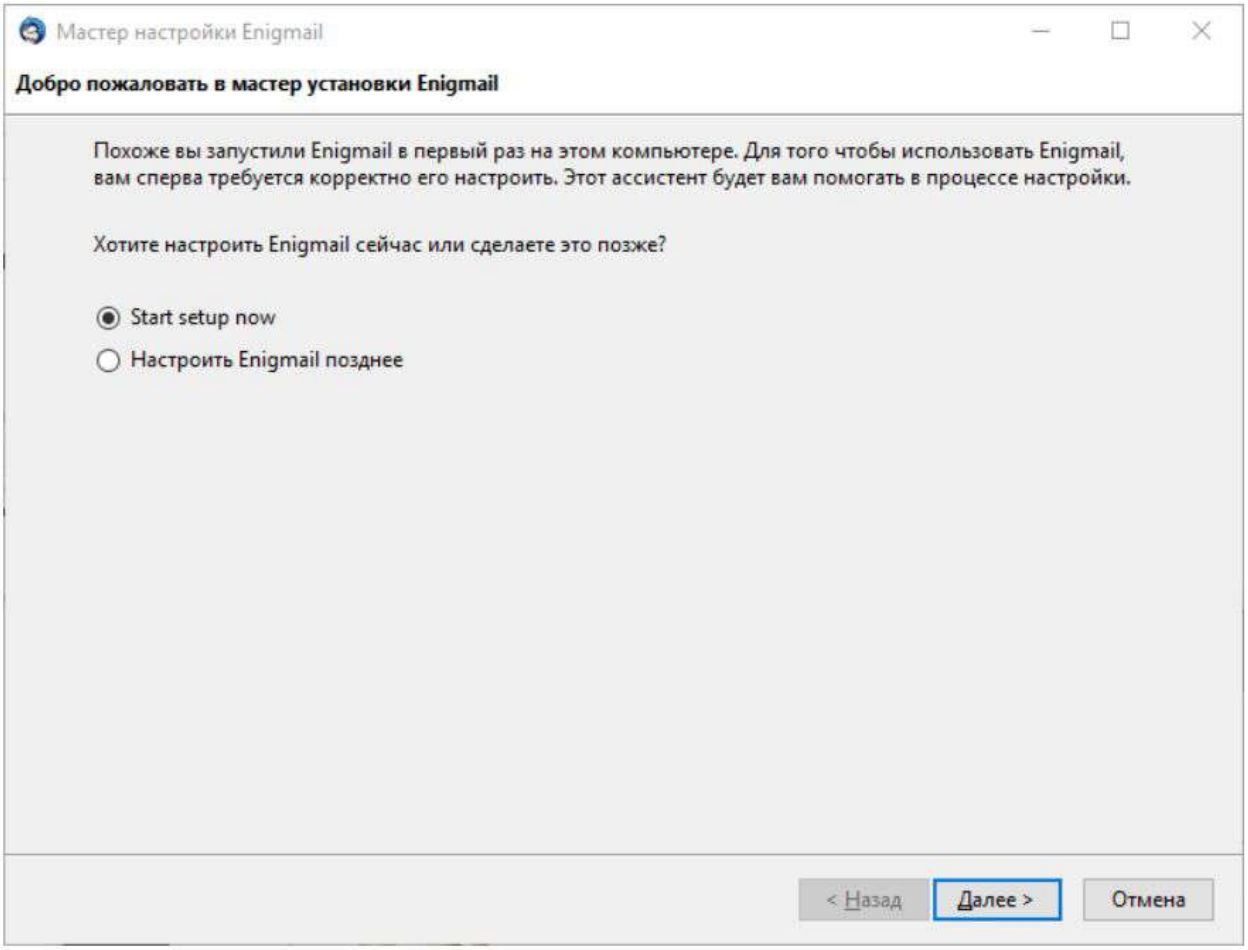


Рис. 6 мастер настройки Enigmail

Выберите [Start setup now] и нажмите кнопку [Далее]. (Рис.7)

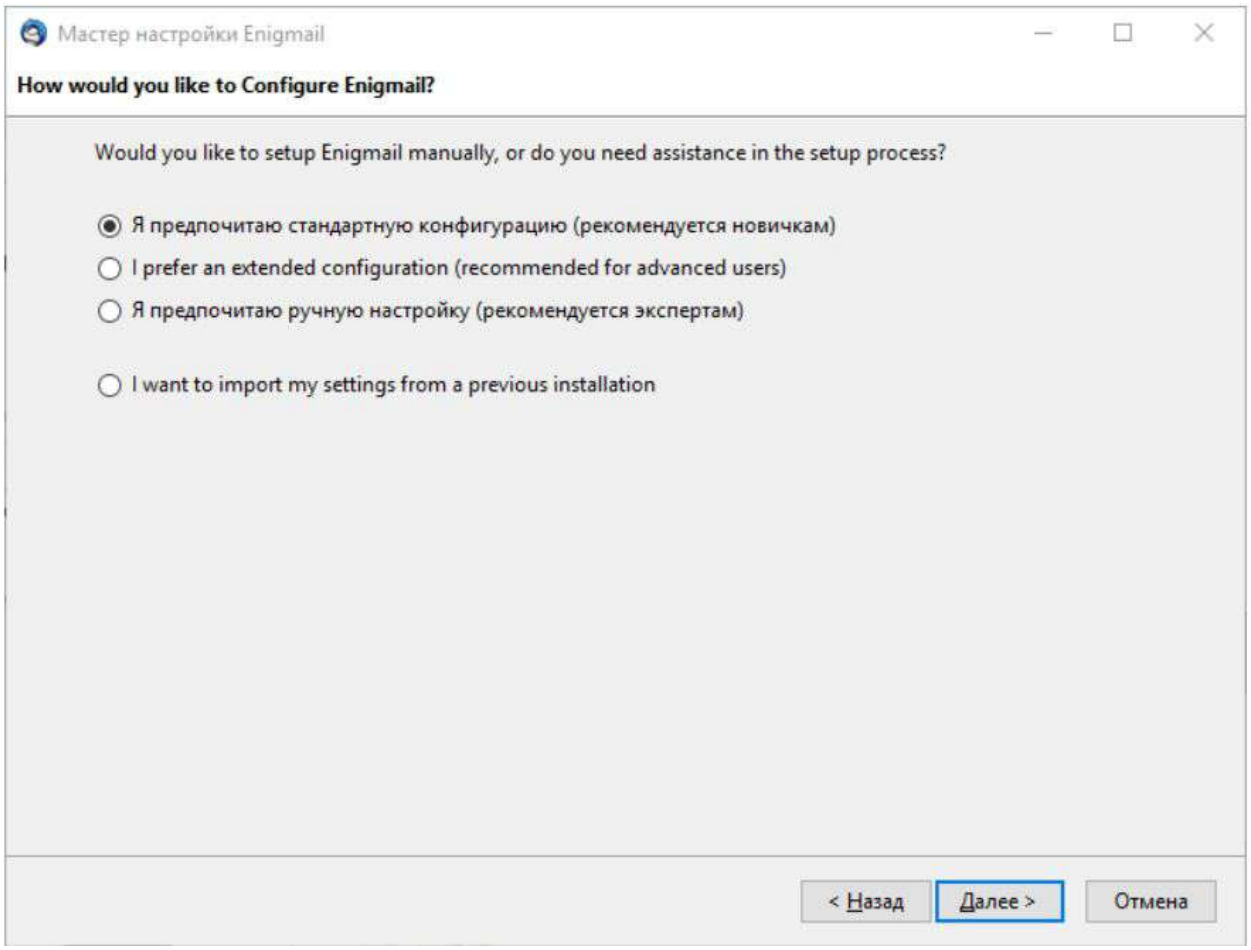


Рис. 7 Выбор конфигурации

Выберите [Я предпочитаю стандартную конфигурацию (рекомендуется новичкам)] и нажмите кнопку [Далее]

Далее придумайте надежный пароль и *наберите* его в обоих окнах.

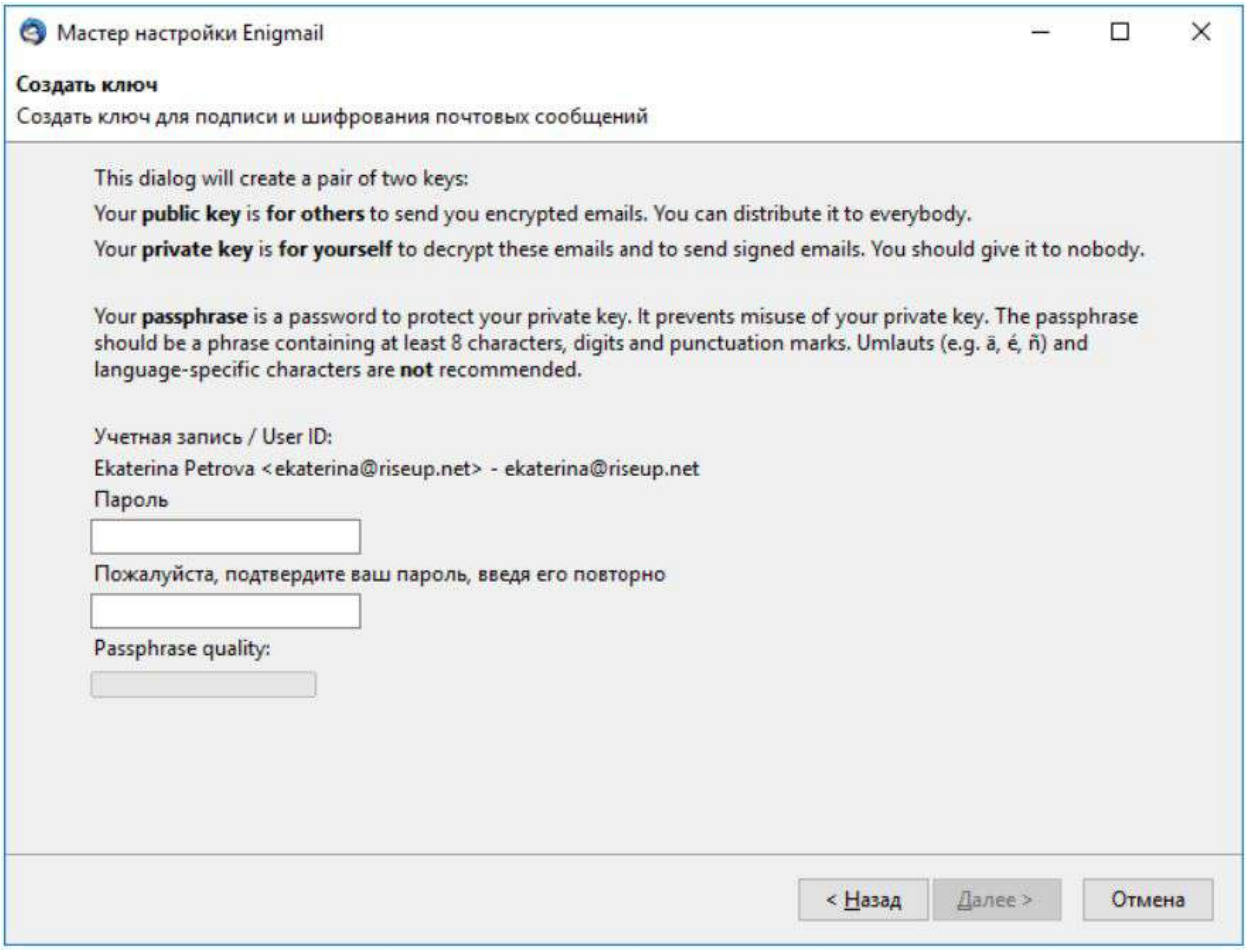


Рис. 8 Создание пары ключей GnuPG

Примечание. Этот пароль защищает ваш секретный ключ. Без него вы не сможете подписывать и расшифровывать сообщения. Не делитесь этим паролем ни с кем. Очень важно, чтобы пароль был действительно надежным, и чтобы вы его не забыли. Подробнее о паролях можно узнать из главы Как создавать и хранить надежные пароли. Мы не советуем использовать в пароле русские буквы, потому что это может создать проблемы в дальнейшем.

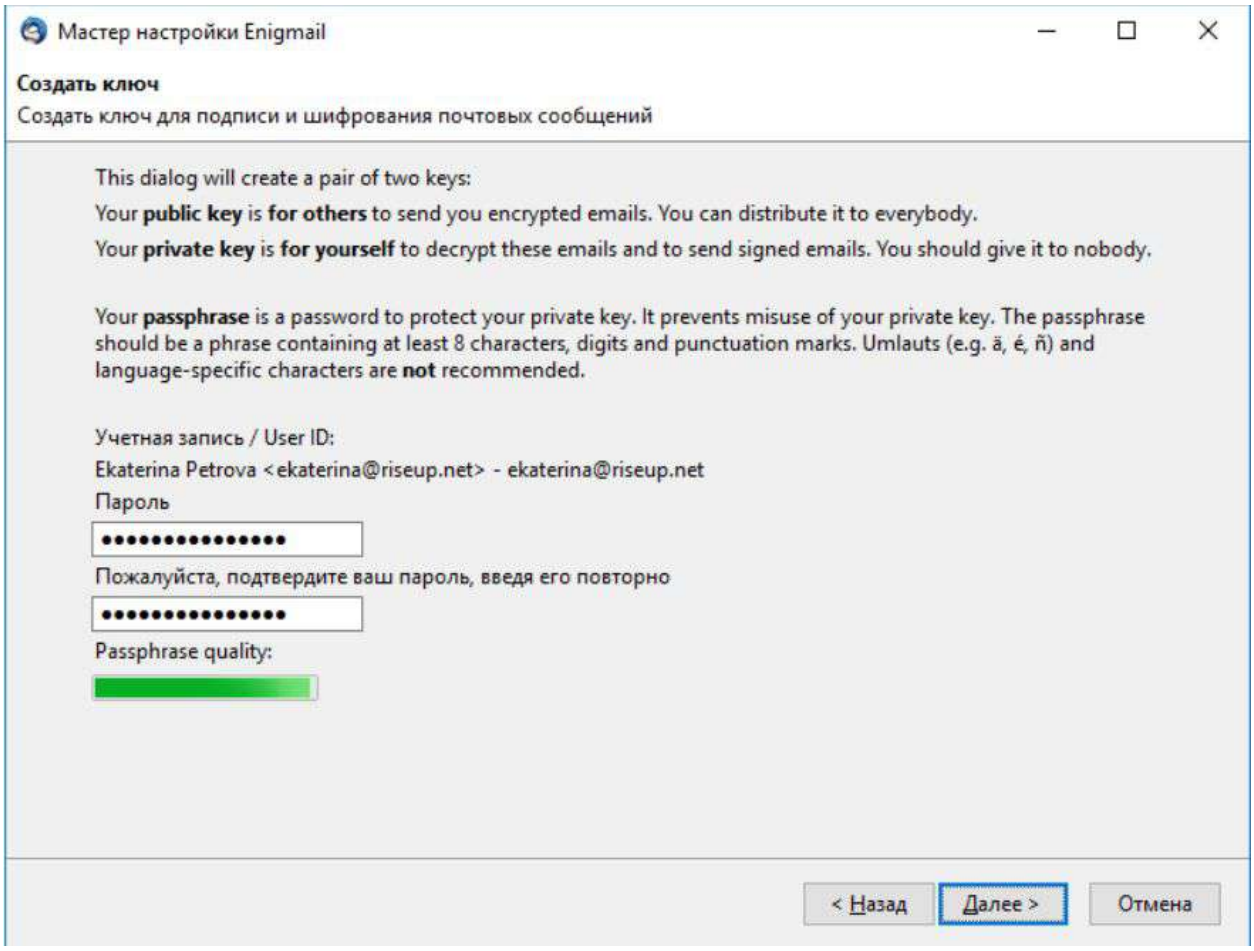


Рис. 9 Указание пароля для пары ключей GnuPG

Нажмите кнопку [Далее] для запуска процесса создания ключей. Подождите, пока процесс создания ключей завершится.

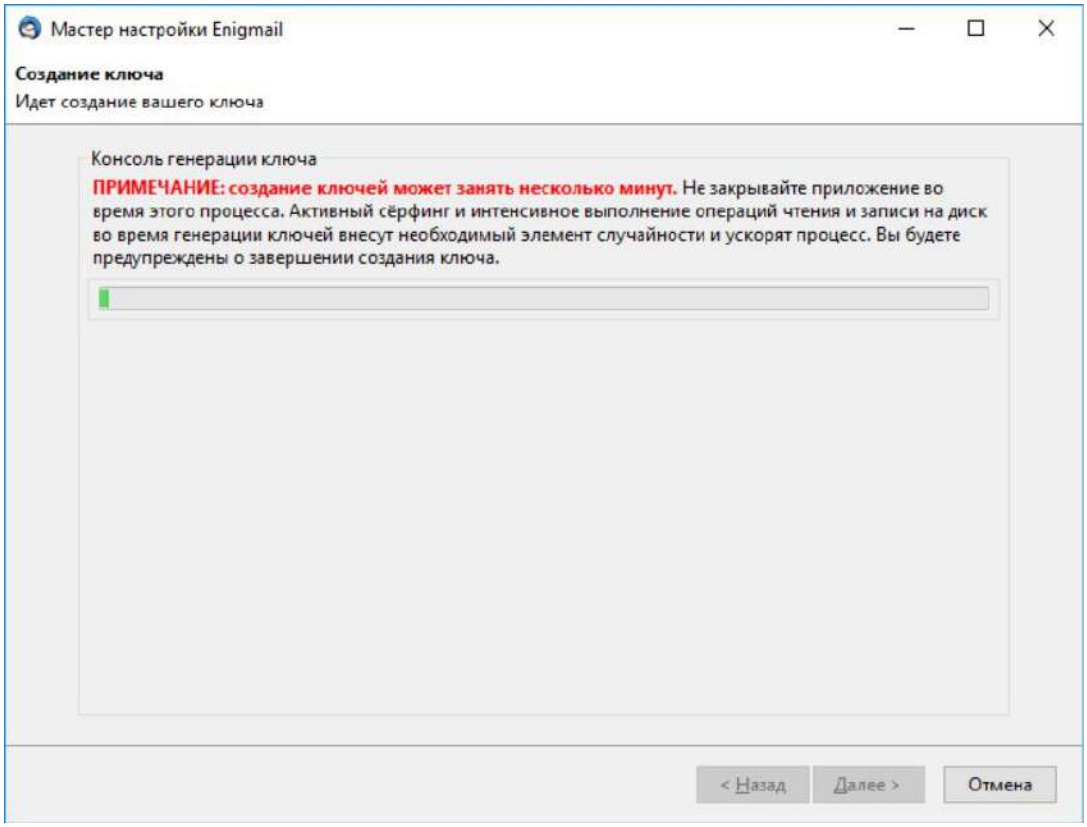


Рис. 10 Создание ключей

Когда Enigmail завершит создание пары ключей GnuPG, появится сообщение и кнопка Создать сертификат отзыва.

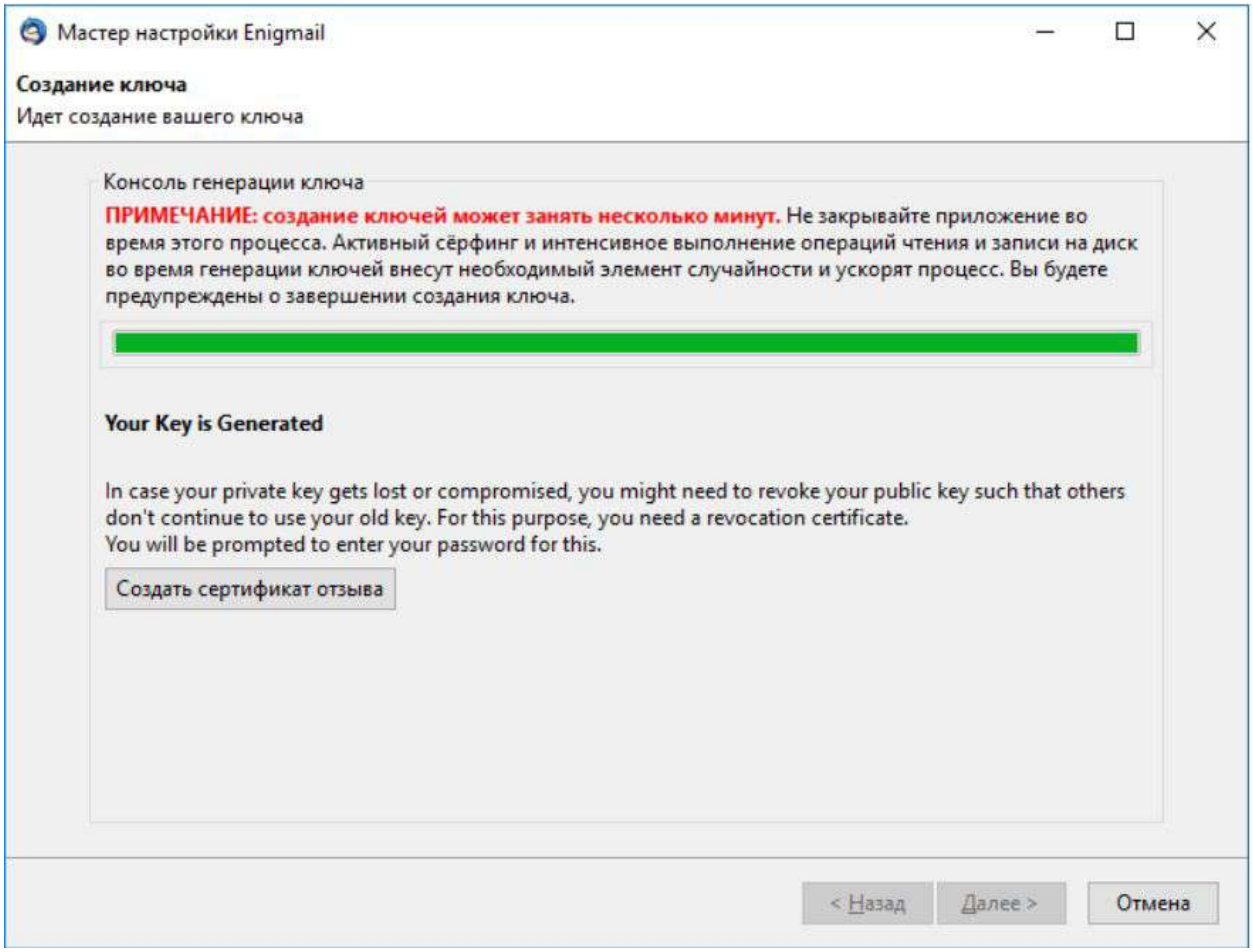


Рис. 11 Программа Enigmail предлагает создать сертификат отзыва

Сертификат отзыва может пригодится, если нужно объявить о недействительности ключа. Когда это может понадобиться:
- Вы решили перестать использовать эту пару ключей.
- Вы потеряли секретный ключ.
- Вы забыли пароль к секретному ключу.
- Вы полагаете, что секретный ключ скомпрометирован или стал известен кому-то еще.

Сертификат отзыва особенно важен, если вы собираетесь загрузить свой открытый ключ на сервер ключей. После того, как вы загрузите туда ключ, не останется никакого способа "удалить" этот ключ. Вы ведь вряд ли захотите, чтобы ваши старые ключи (может быть, скомпрометированные) сбивали людей с толку. Нажмите кнопку [Создать сертификат отзыва].

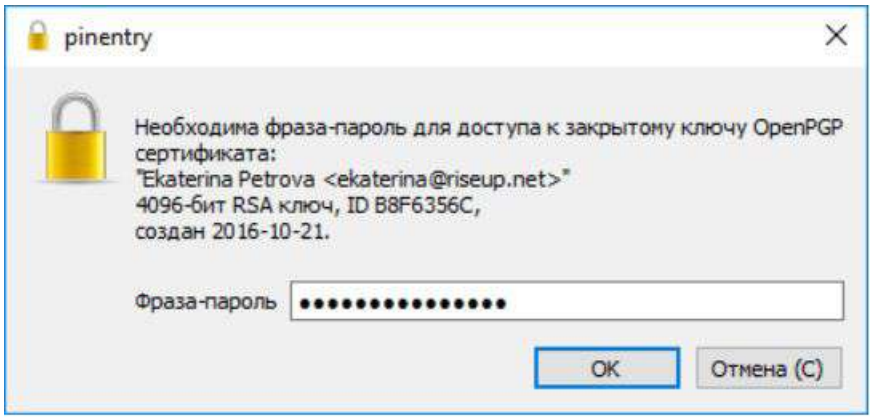


Рис. 12 Enigmail запрашивает пароль

Введите пароль, который указывали при создании пары ключей GnuPG, и нажмите кнопку OK.

Выберите имя файла и место для сохранения сертификата отзыва.

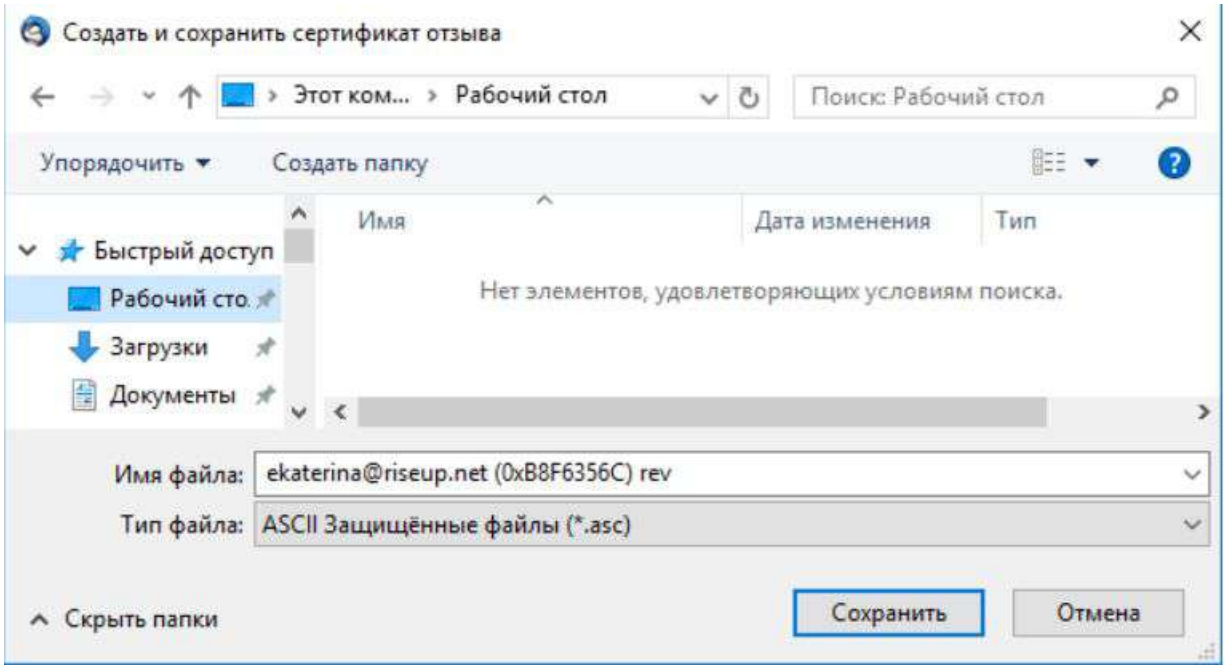


Рис. 13 Выбор имени и места для сохранения сертификата отзыва

В данном примере мы сохраним сертификат отзыва на Рабочем столе, но вы можете сохранить его в более безопасном месте.

Нажмите кнопку [Сохранить]. Enigmail предупредит о том, как важно хранить сертификат отзыва в безопасности.

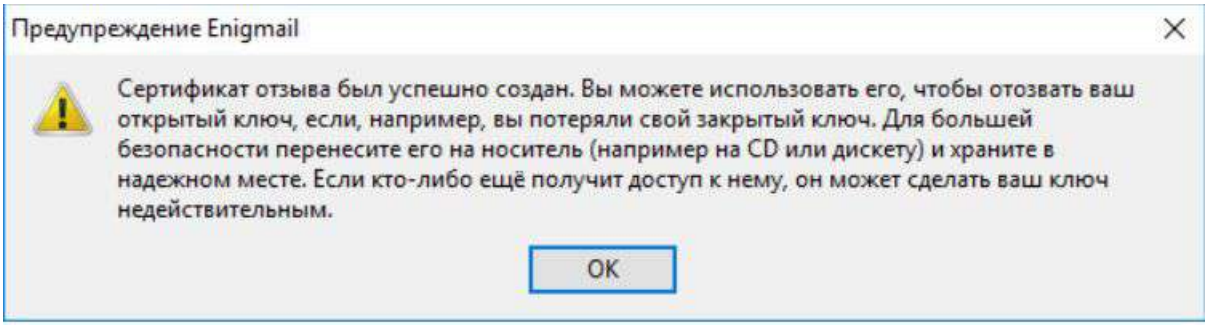


Рис. 14 Предупреждение о сертификате отзыва

Нажмите кнопку [OK], чтобы вернуться к мастеру установки.

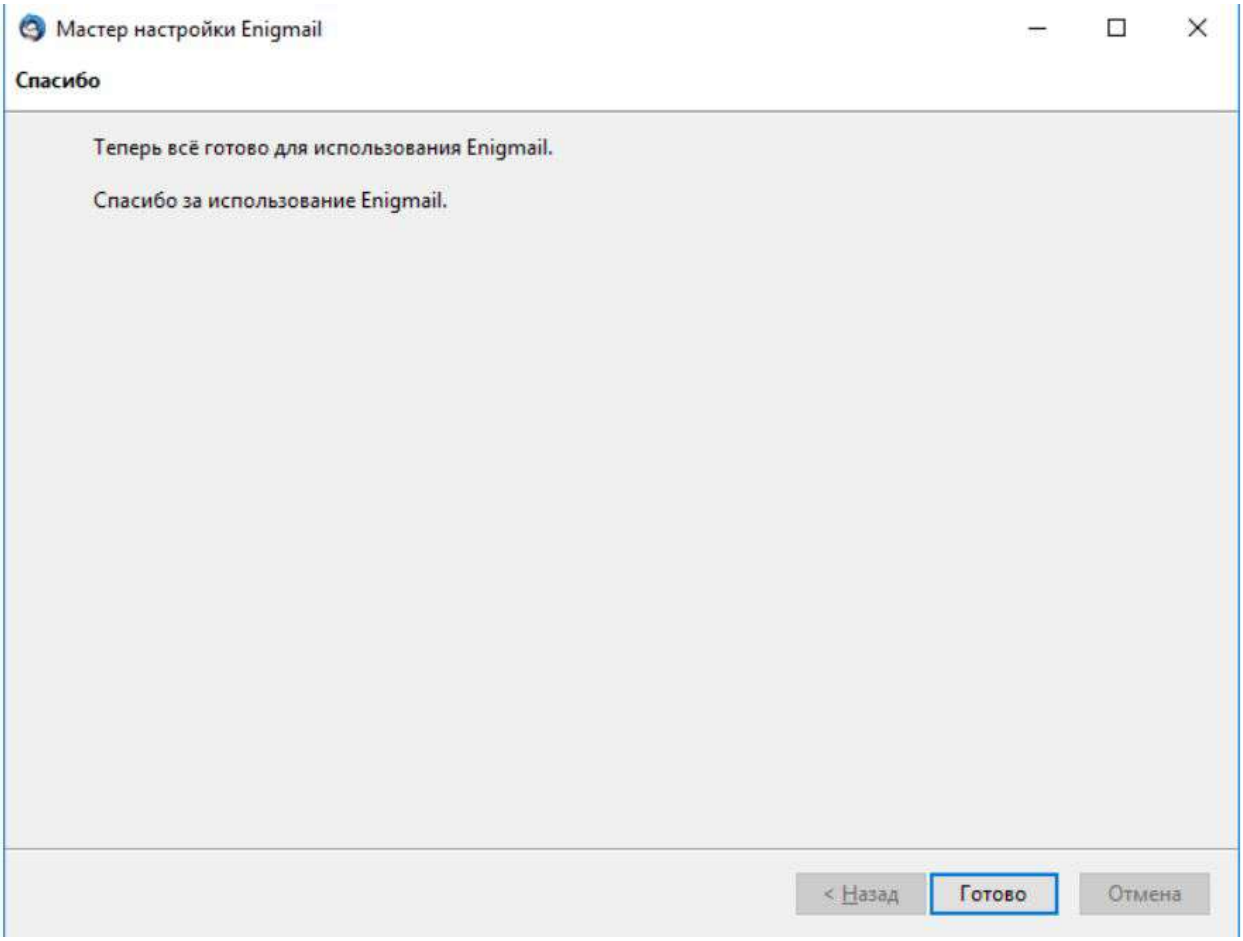


Рис 15 Мастер установки Enigmail

Нажмите кнопку [Готово], чтобы завершить процесс создания ключей.

3.4 НАСТРОЙКА ENIGMAIL ДЛЯ РАБОТЫ С ВАШЕЙ УЧЕТНОЙ ЗАПИСЬЮ

Нажмите меню и выберите в меню [Настройки > Параметры учетной записи].

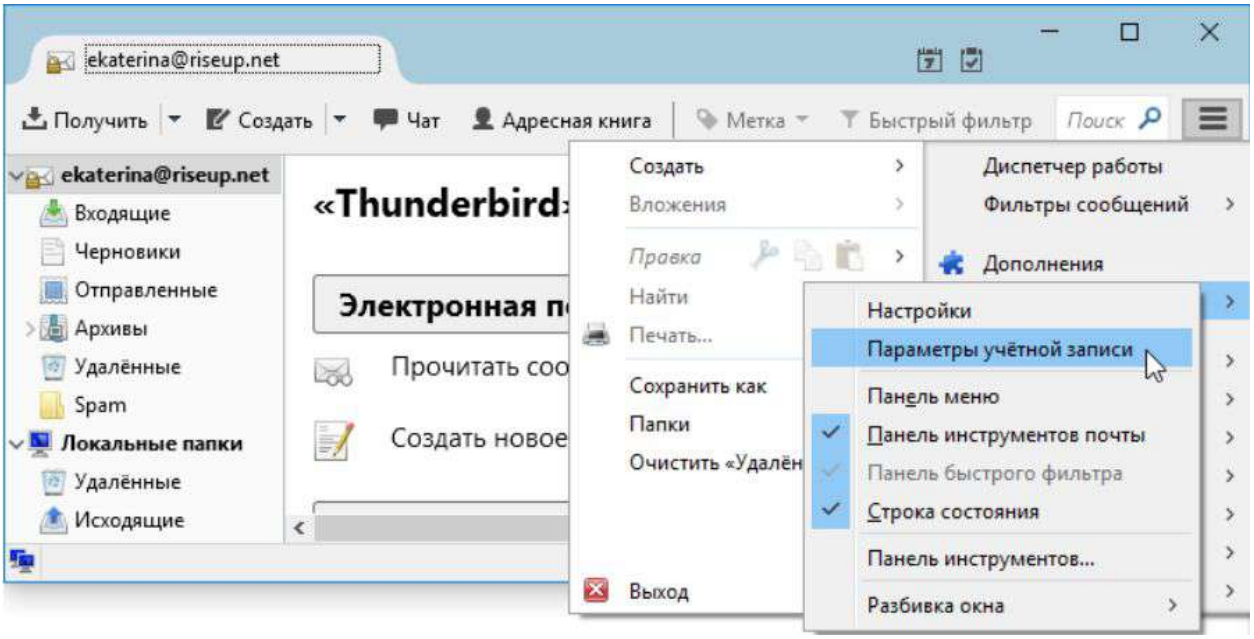


Рис. 16 Доступ к параметрам учетной записи в меню Thunderbird

Откроется окно Параметры учетной записи.

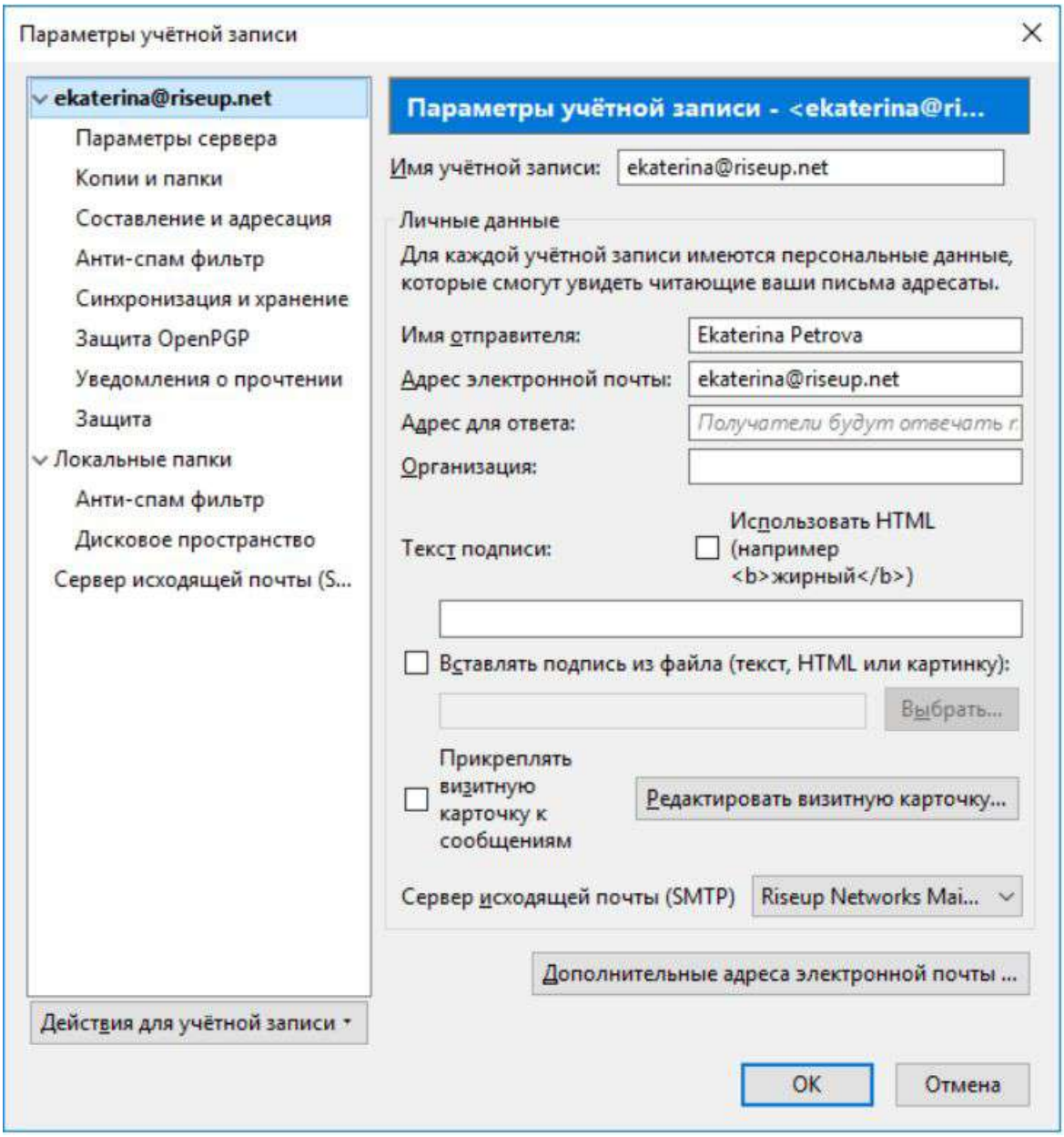


Рис. 17. Параметры учетной записи Thunderbird

Выберите в левом меню (под адресом e-mail) пункт Защита OpenPGP.

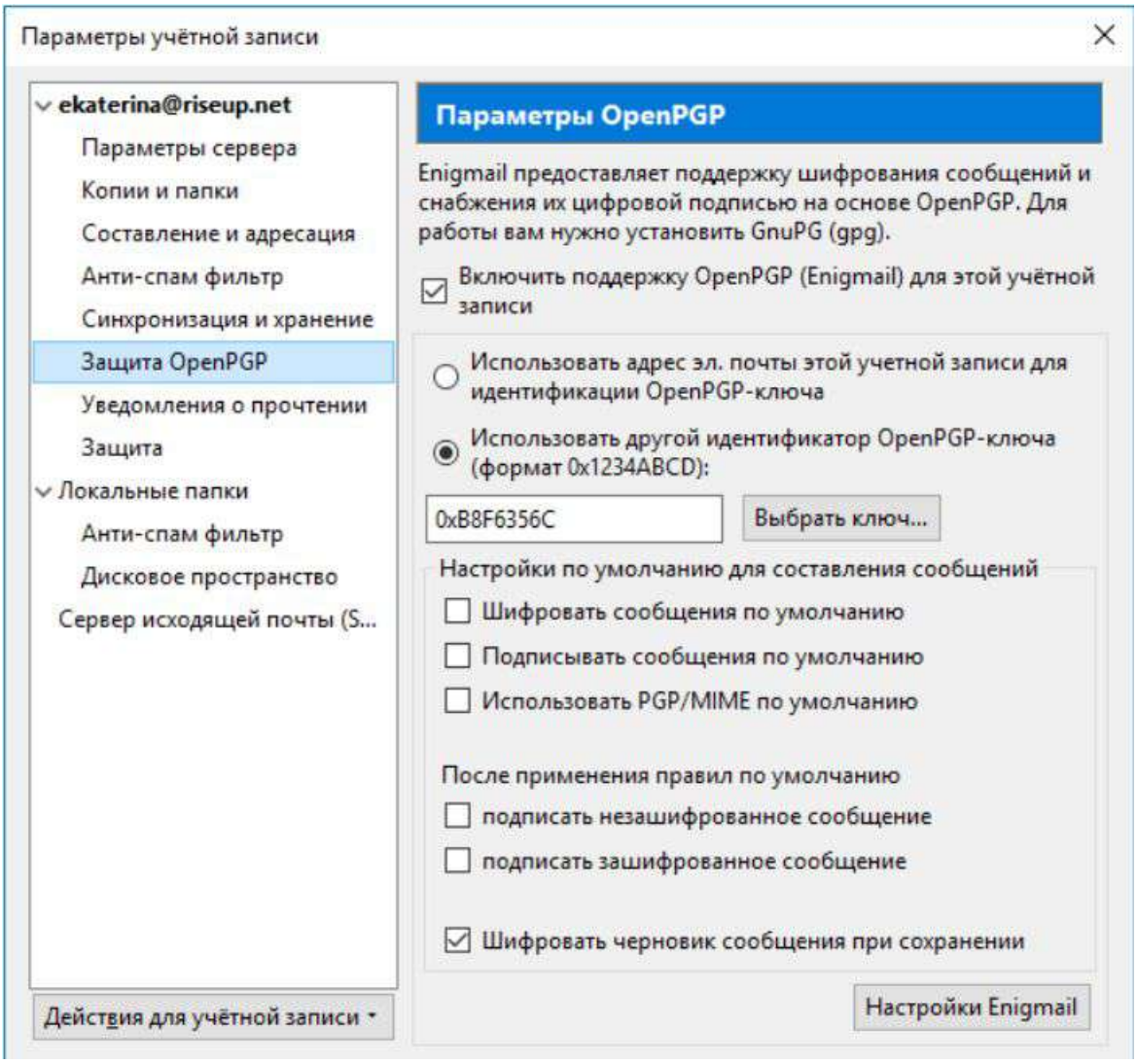


Рис. 18 Параметры OpenPGP

В этом окне находятся различные настройки **Enigmail**, связанные с шифрованием e-mail. Если вы создали пару ключей **GnuPG**, как было описано выше – после создания одной учетной записи **Thunderbird** – эта учетная запись уже должна быть настроена для работы с **Enigmail**. Она также должна быть связана с ключевой парой, которую вы создали

Нажмите кнопку [Выбрать ключ...], чтобы открыть окно Выберите OpenPGP-ключ для шифрования

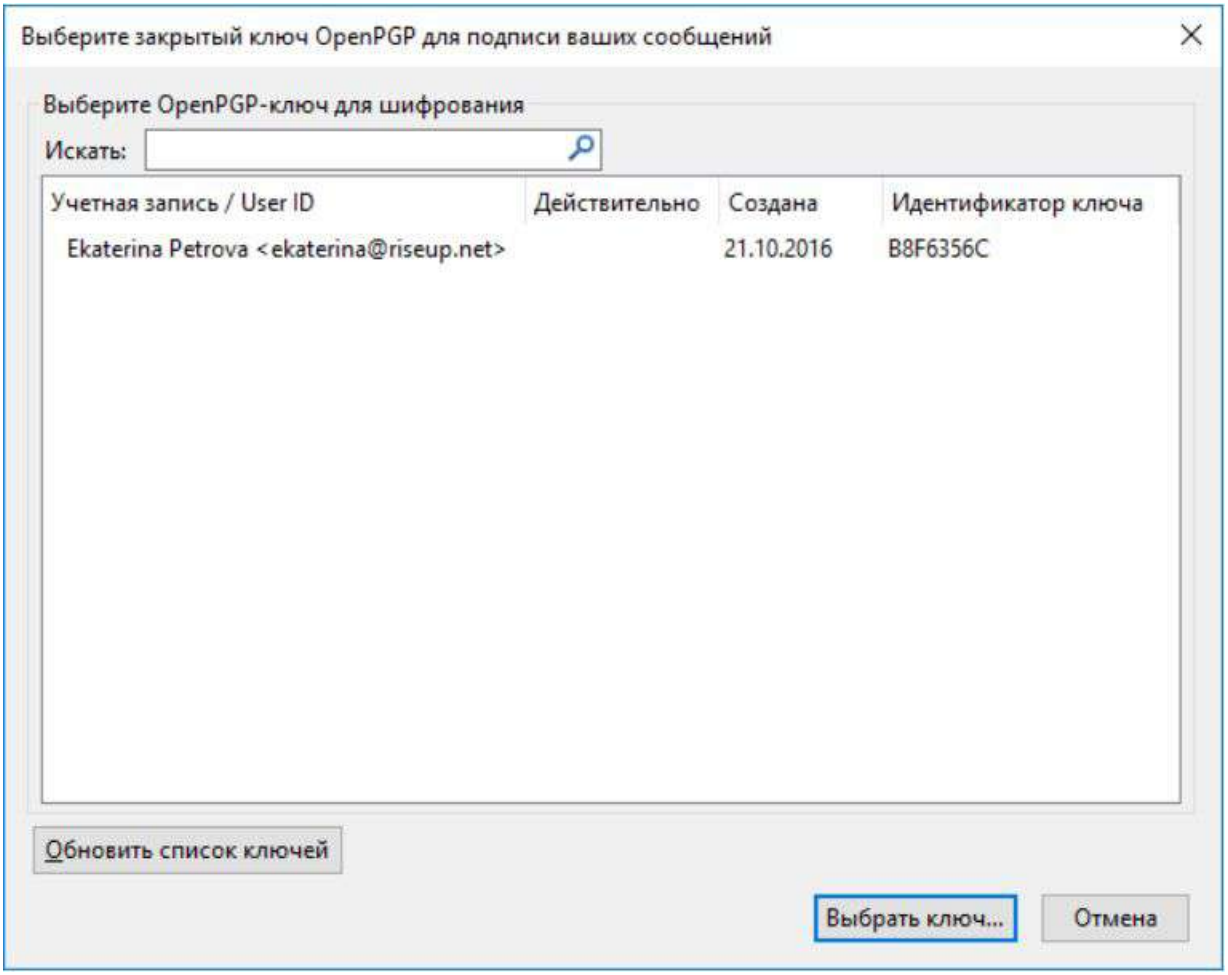


Рис. 19 Окно выбора OpenPGP-ключ для шифрования

Выберите ключевую пару, которую хотите использовать для этой учетной записи e-mail.

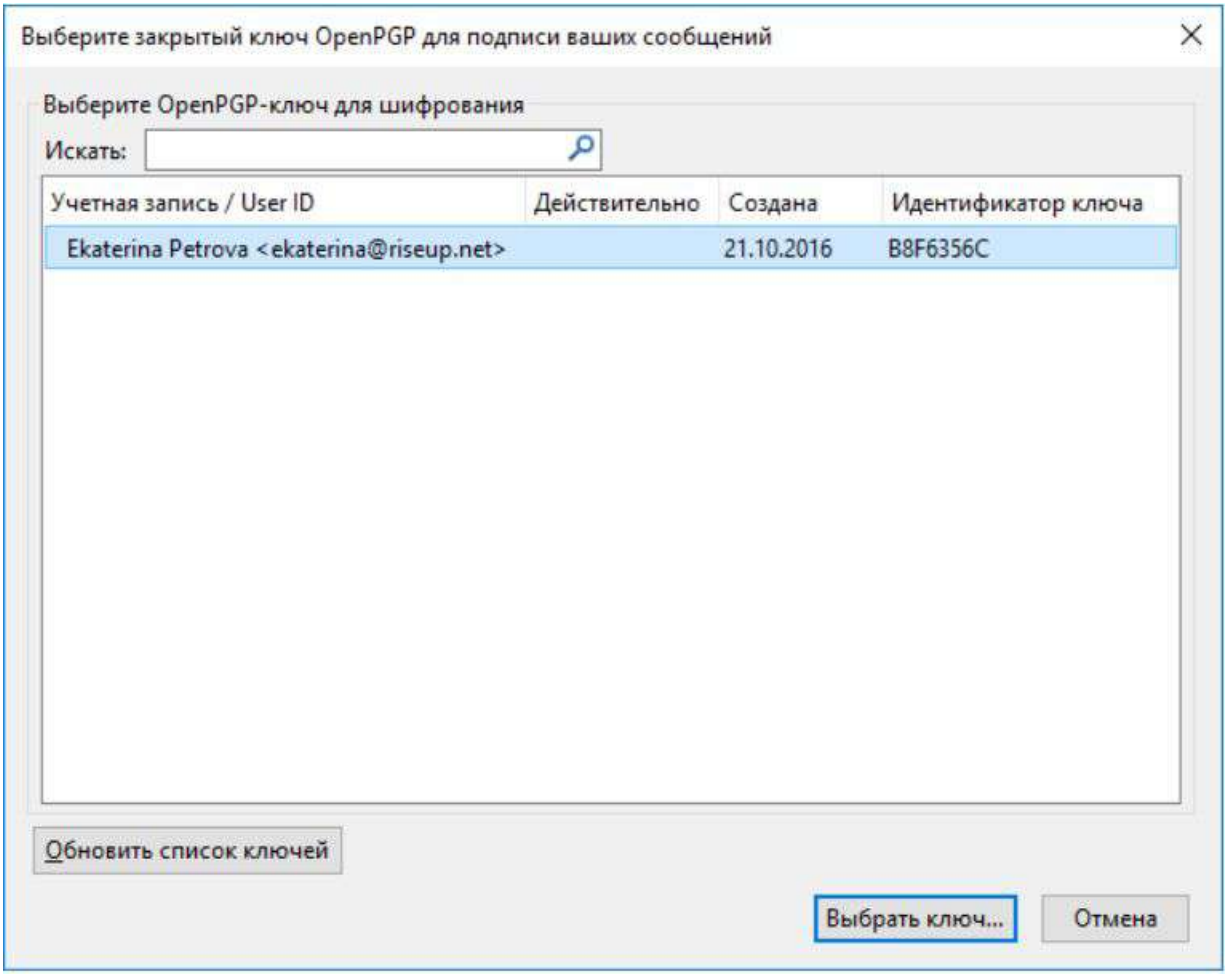


Рис. 20 Выбор ключевой пары для использования с учетной записью Thunderbird

3.5 СВОЙСТВА КЛЮЧЕЙ И УПРАВЛЕНИЕ КЛЮЧАМИ

Когда пара ключей **GnuPG** создана, а ваша учетная запись настроена для работы с **Enigmail**, можно посмотреть свойства ключей
Нажмите меню и выберите в меню [Enigmail > Менеджер ключей].

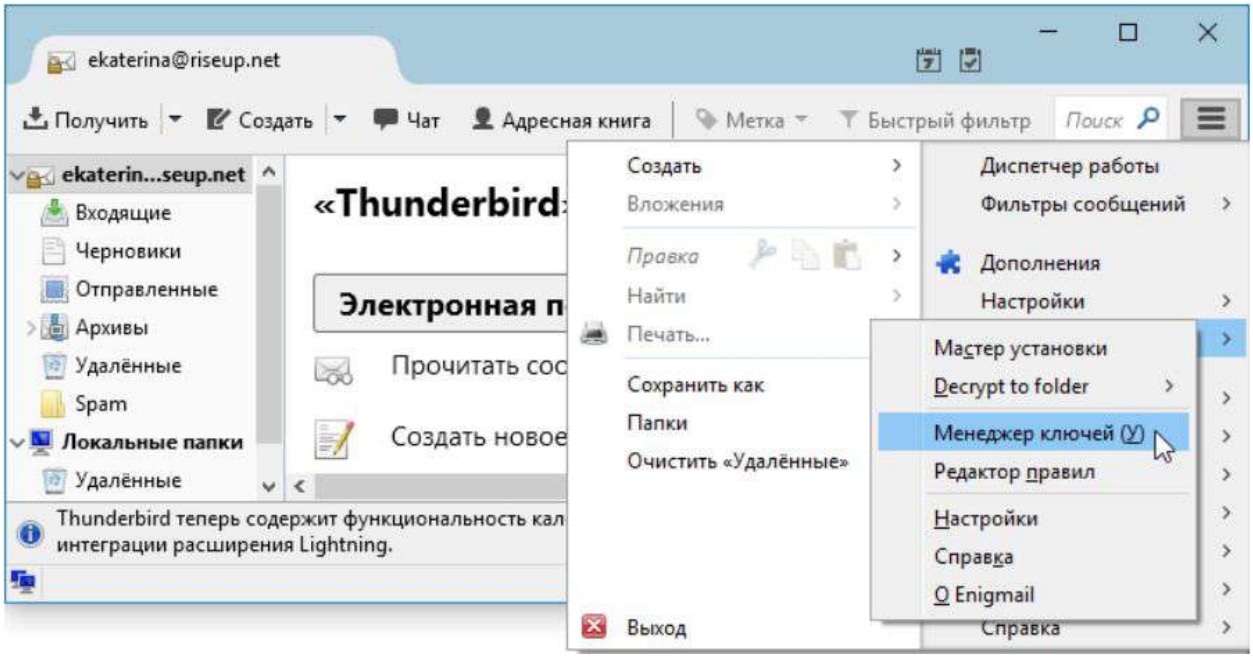


Рис 21 Доступ к менеджеру ключей Enigmail из меню

Откроется окно менеджера ключей.

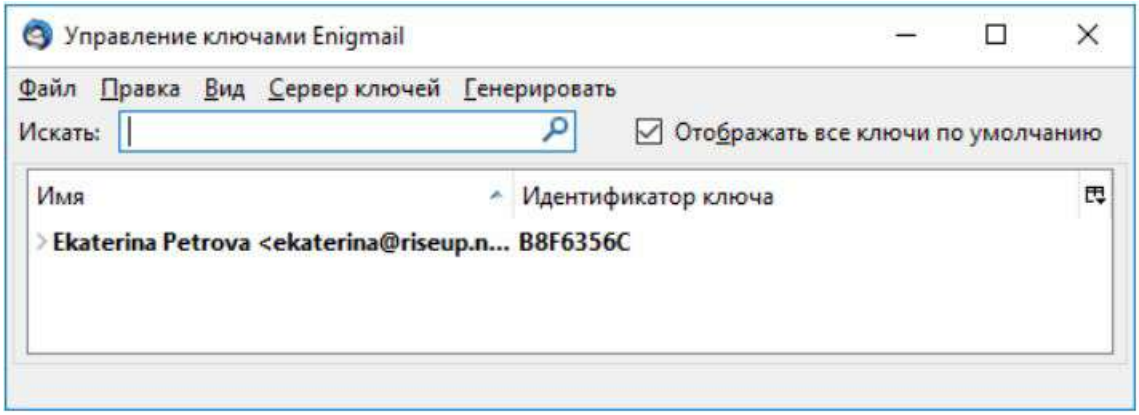


Рис 22 Менеджер ключей Enigmail

Дважды щелкните по ключевой паре, чтобы увидеть/редактировать ее свойства.

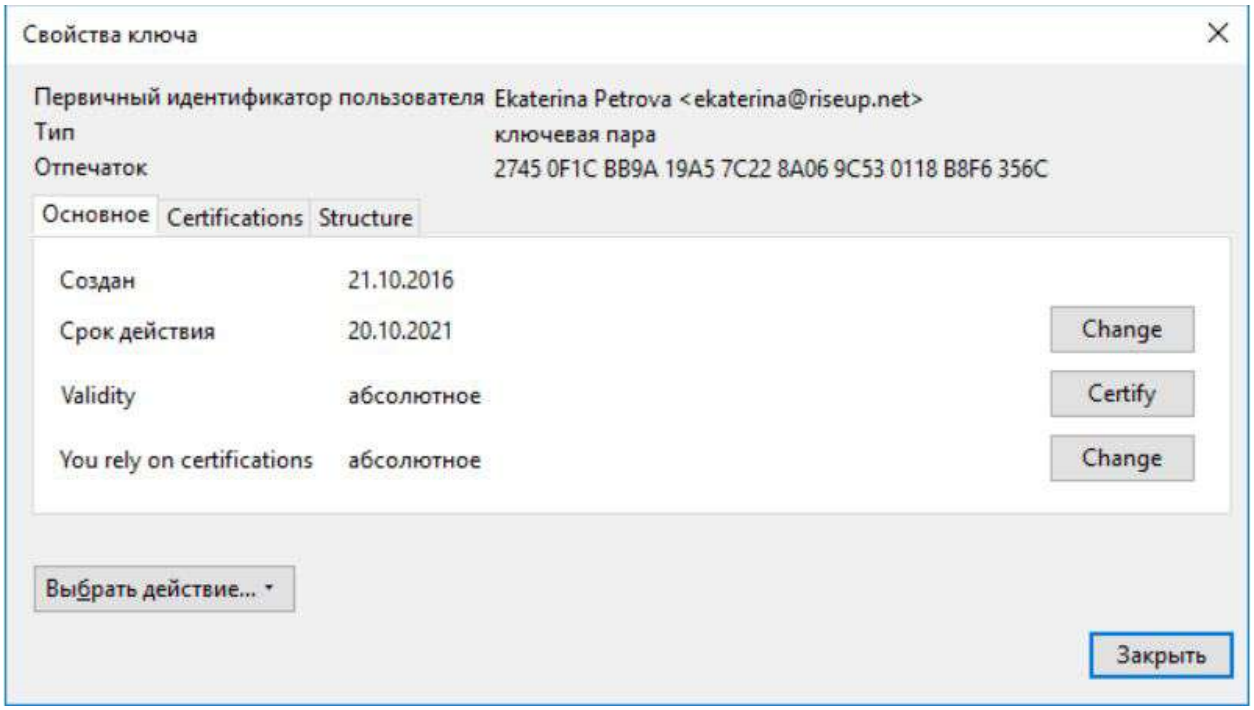


Рис 23. Свойства ключевой пары

В этом окне показаны важные свойства вашей *пары ключей* **GnuPG**:

- **Key ID.** *Идентификатор ключа* для *ekaterina@riseup.net* – **0xB8F6356C**. (Последние восемь знаков полного *отпечатка ключа*).
- **Отпечаток ключа.** Для данной *ключевой пары* – **2745 0F1C BB9A 19A5 7C22 8A06 9C53 0118 B8F6 356C**. *Отпечаток необязательно хранить в секрете*. Более того, отпечатки часто сообщают друг другу.
- **Срок действия.** Эта *ключевая пара* перестанет работать после 20 октября 2021 года.

3.6 ИЗМЕНЕНИЕ СРОКА ДЕЙСТВИЯ КЛЮЧЕВОЙ ПАРЫ

Если вы хотите изменить срок действия вашей ключевой пары GnuPG. Это может пригодиться, если срок действия текущих ключей подходит к концу и вам нужно больше времени, чтобы создать новую пару и оповестить о ней всех, с кем вы обмениваетесь зашифрованными сообщениями e-mail. Способ помогает продлить действие ключа.

Нажмите кнопку [Change] в строке "Срок действия".

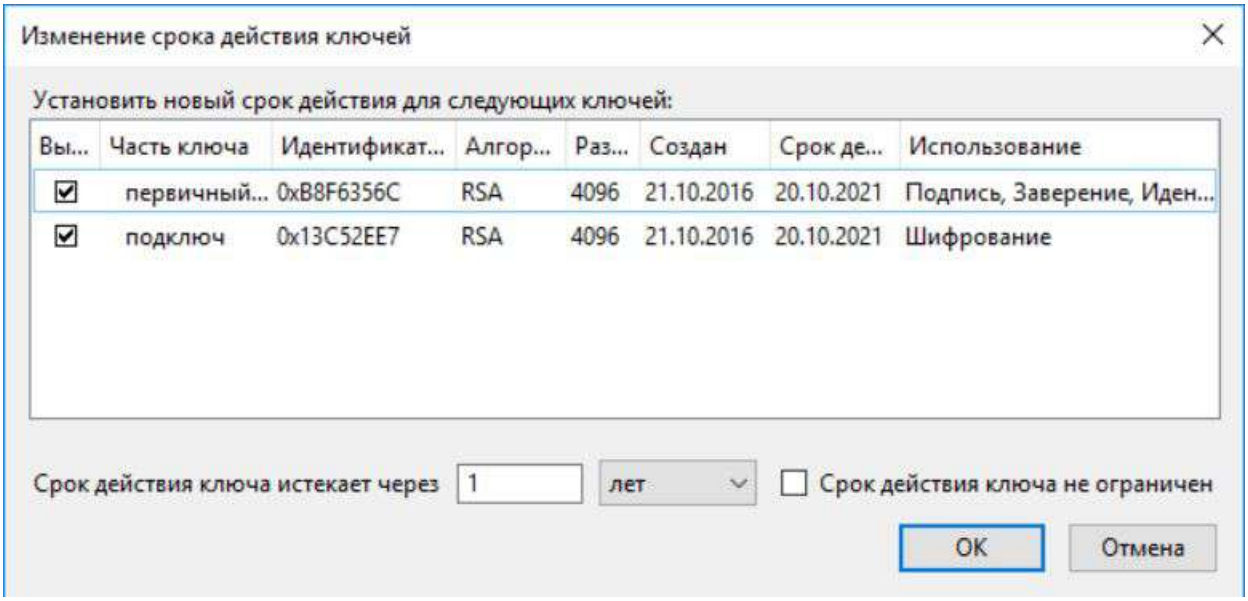


Рис 24 Изменение срока действия ключевой пары

Появится окно Изменение срока действия ключей.

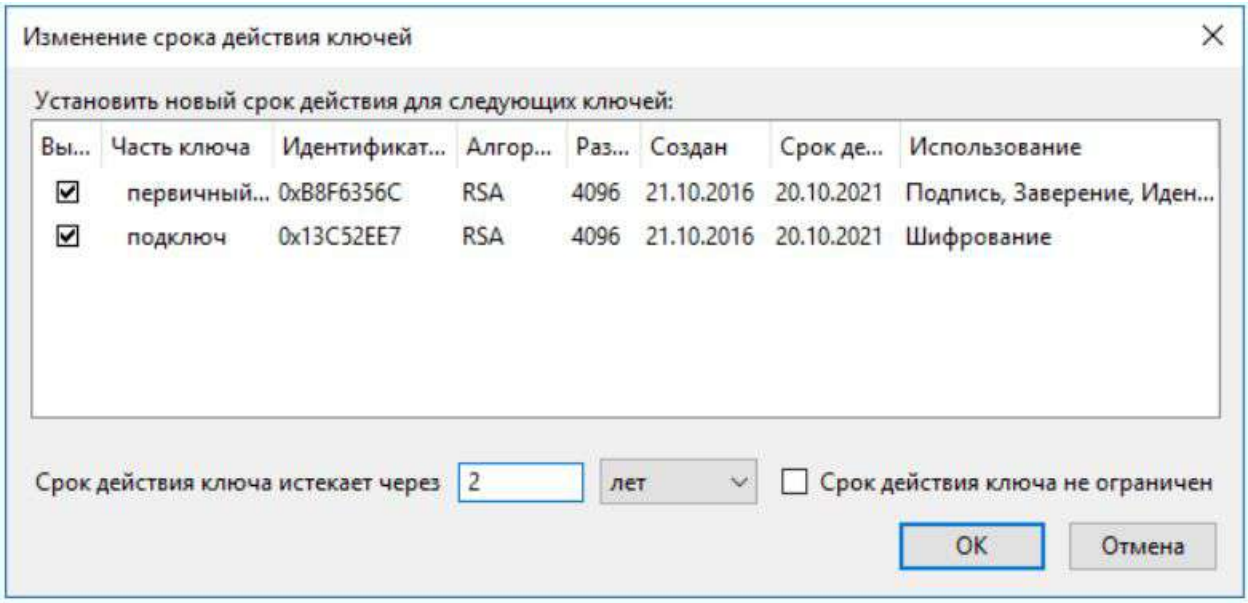


Рис 25. Окно Изменение срока действия ключей Enigmail

Примечание. Число лет в нижней части окна не обязательно соответствует реальному сроку истечения действия ключей. Если вы неосторожно нажмете кнопку [OK], ничего не меняя в окне, то можете сократить срок действия своей ключевой пары.

Выберите число лет, начиная с сегодняшнего дня, в течение которых ваша ключевая пара должна работать.

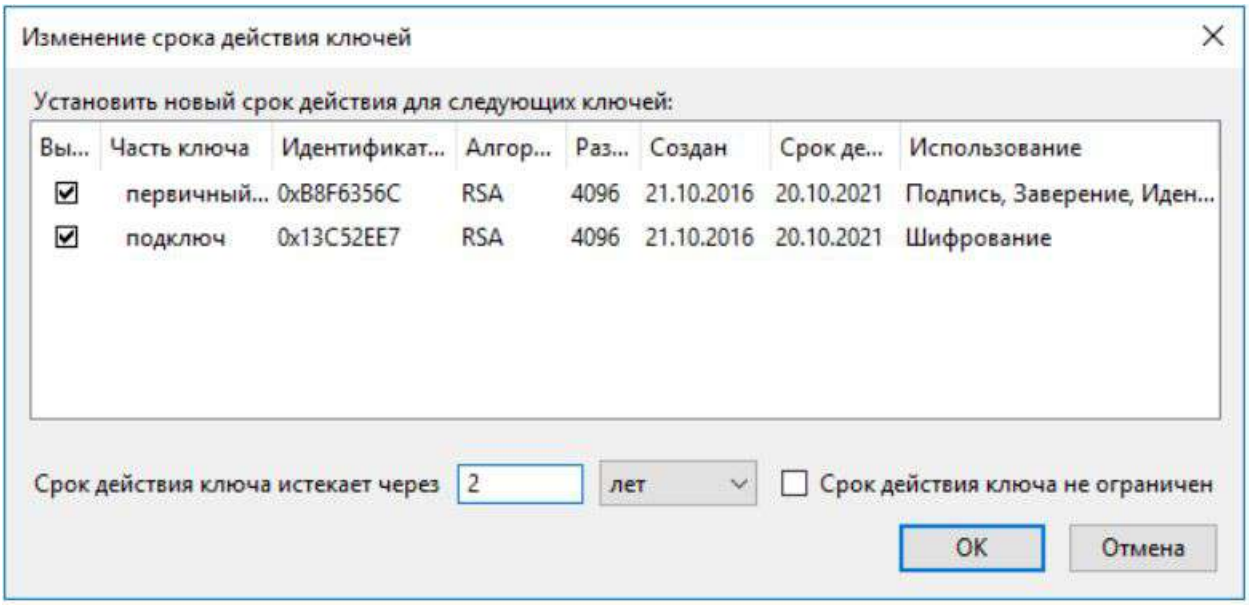


Рис 26. Изменение срока действия ключевой пары GnuPG

Нажмите кнопку [OK], чтобы ввести пароль к секретному ключу.

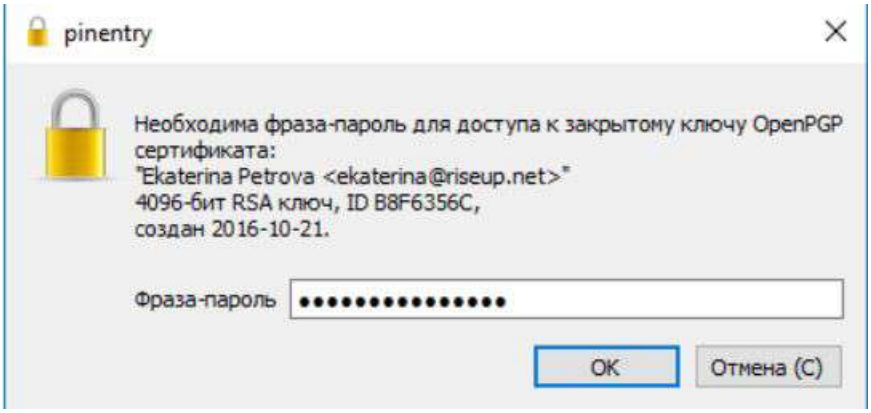


Рис 27. Ввод пароля к секретному ключу

Введите ваш пароль.

Нажмите кнопку [OK], чтобы изменить срок действия ключевой пары GnuPG.

3.7 ОТПРАВКА ОТКРЫТОГО КЛЮЧА В ВИДЕ ВЛОЖЕНИЯ E-MAIL

Аналогичным образом ваши друзья должны отправить вам их открытые ключи.

Откройте Thunderbird, нажмите в меню [Создать].

Выберите в меню [Enigmail > Присоединить мой открытый ключ...]. (Как вариант, вы можете выбрать пункт [Присоединить мой открытый ключ] (над вашим адресом e-mail)

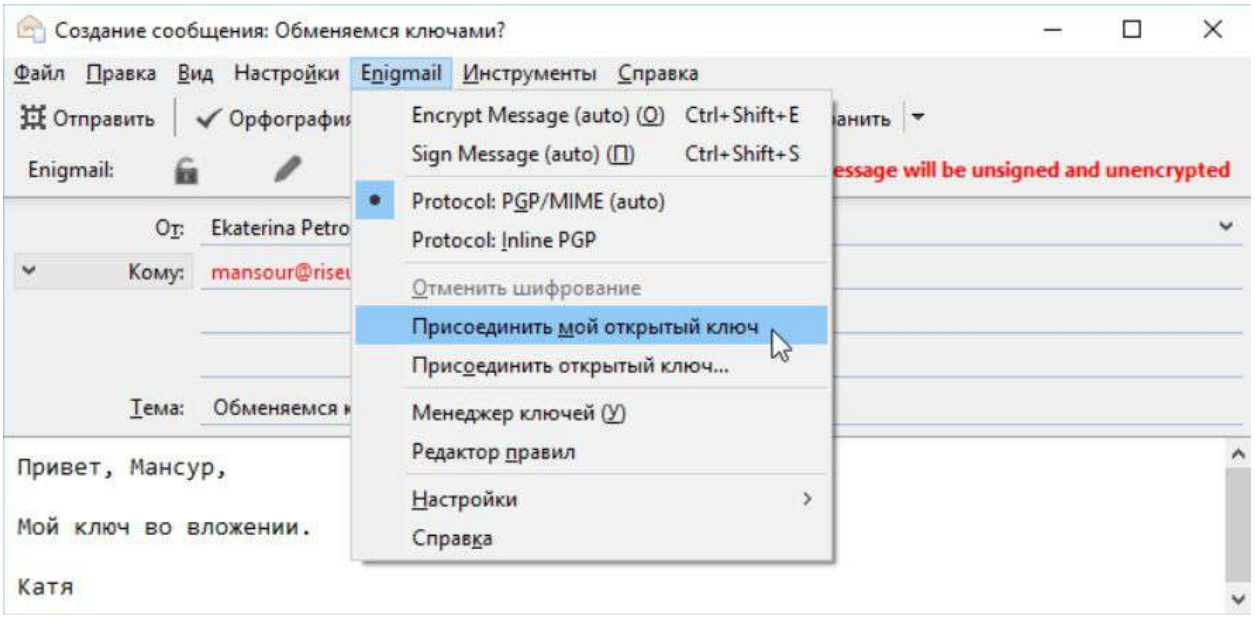


Рис 28 Присоединение открытого ключа

Выберите ключ, который хотите присоединить (по умолчанию тот, который связан с вашей текущей учетной записью e-mail), и нажмите кнопку [Отправить].

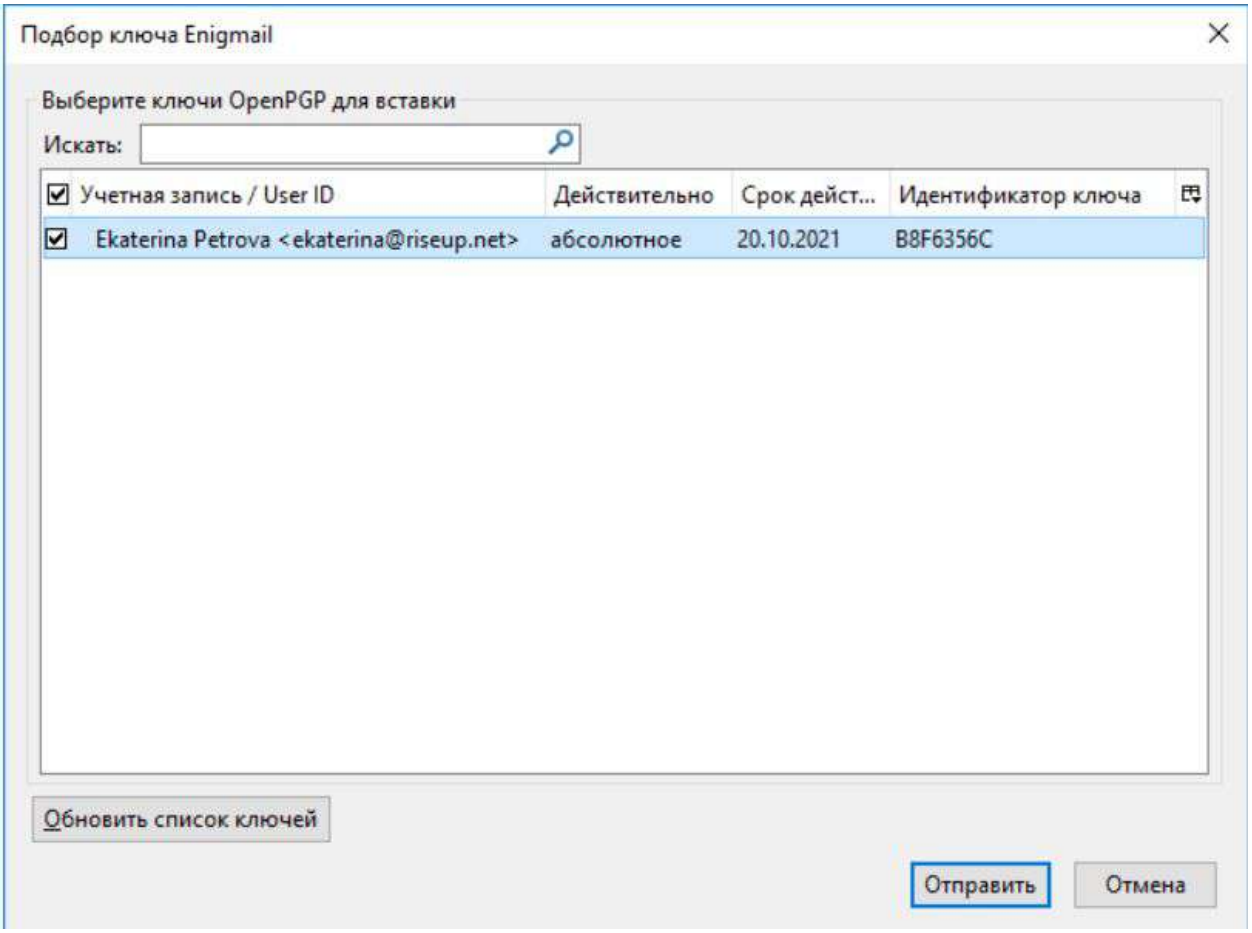


Рис 29. Выбор открытого ключа для вложения

Нажмите кнопку [Отправить], чтобы отправить сообщение.

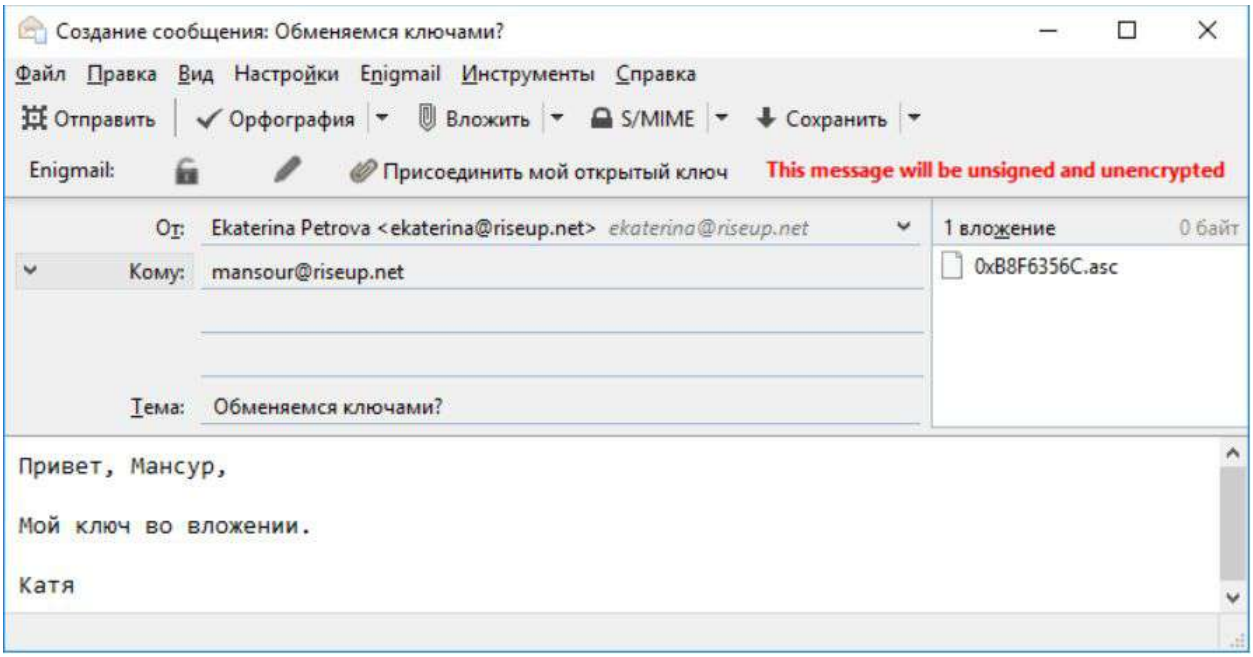


Рис 30 Вложенный ключ, готовый к отправке

3.8 ИМПОРТ ОТКРЫТОГО КЛЮЧА ИЗ ФАЙЛА-ВЛОЖЕНИЯ

Как вы, так и ваш адресат должны импортировать открытые ключи друг друга.

Файл-вложение с открытым ключом должен быть виден под текстом письма, в которое он был вложен.

Рис 31. Открытый ключ во вложении

Щелкните правой кнопкой мыши по вложению. Выберите пункт Импорт ключа OpenPGP.

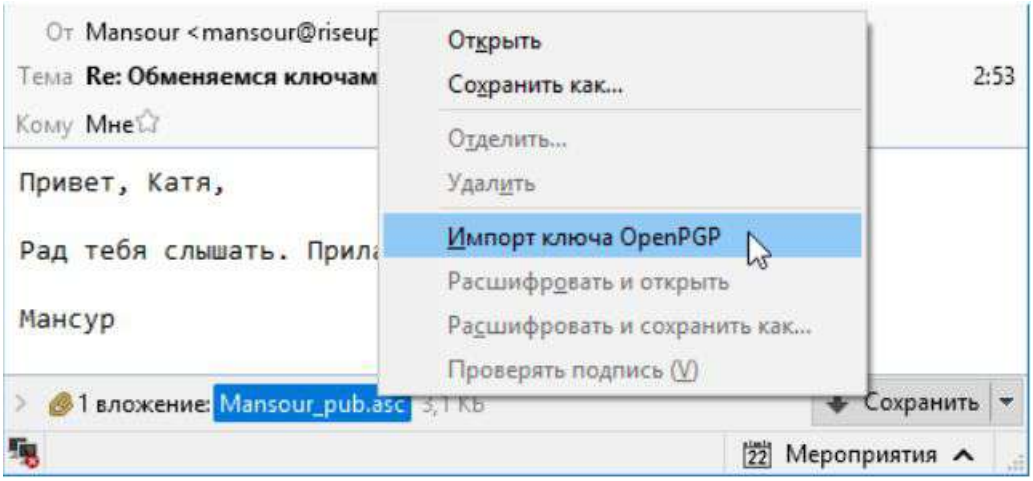


Рис 32. Контекстное меню для ключа

Нажмите кнопку [Да], чтобы импортировать открытый ключ.

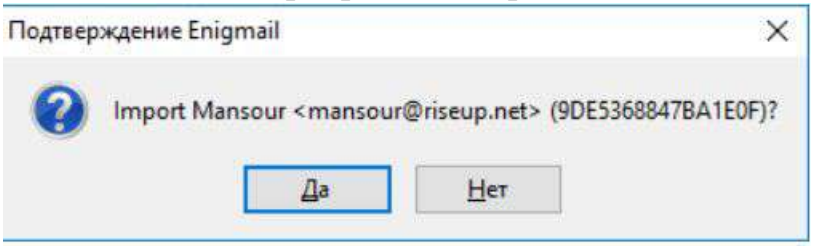


Рис 33 Подтверждение импорта открытого ключа

Нажмите кнопку [OK].

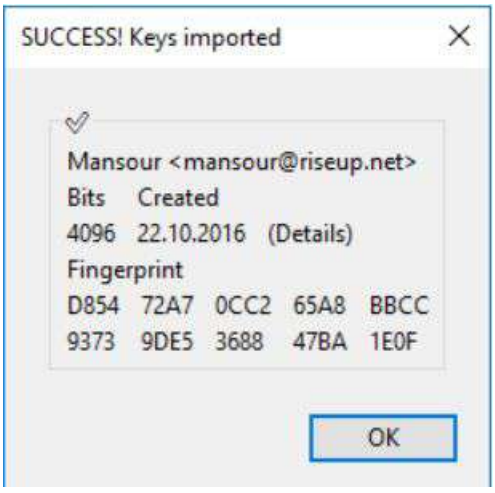


Рис 34. Открытый ключ успешно импортирован

Нажмите кнопку и выберите [Enigmail > Менеджер ключей].

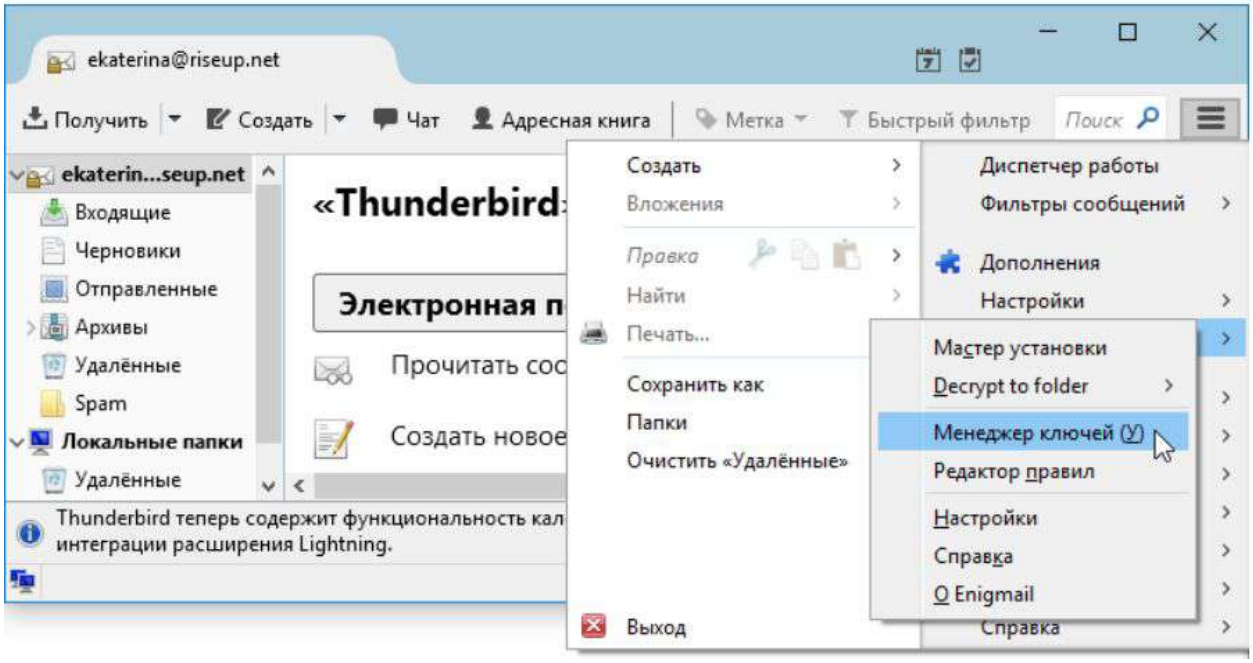


Рис 35. Доступ к менеджеру ключей Enigmail через меню

Теперь вы можете видеть открытый ключ вашего собеседника:

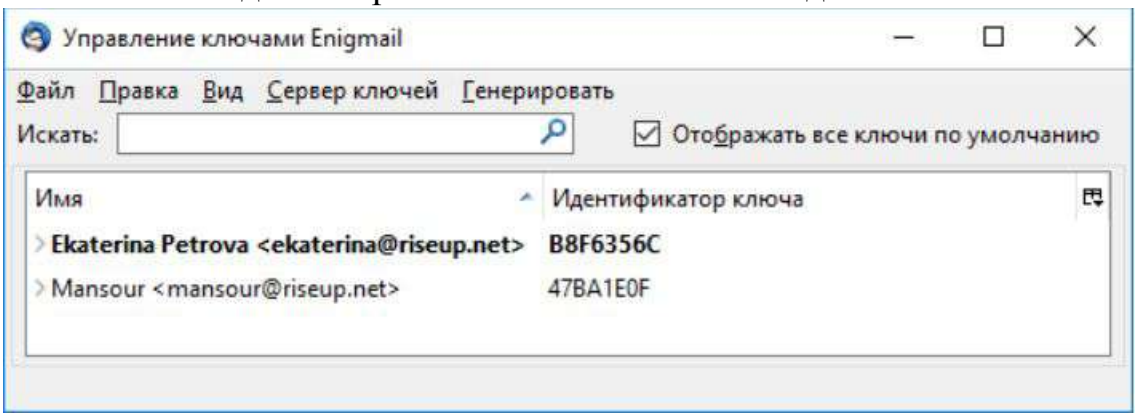


Рис 36. Новый открытый ключ в менеджере ключей Enigmail

3.9 ОТПРАВКА ЗАШИФРОВАННОГО ПИСЬМА

Итак, вы и ваш собеседник успешно импортировали, проверили и подписали ключи друг друга. Теперь вы можете обмениваться шифрованными сообщениями.

Откройте Thunderbird, нажмите [Создать] и составьте сообщение для адресата, чей подписанный открытый ключ у вас есть.

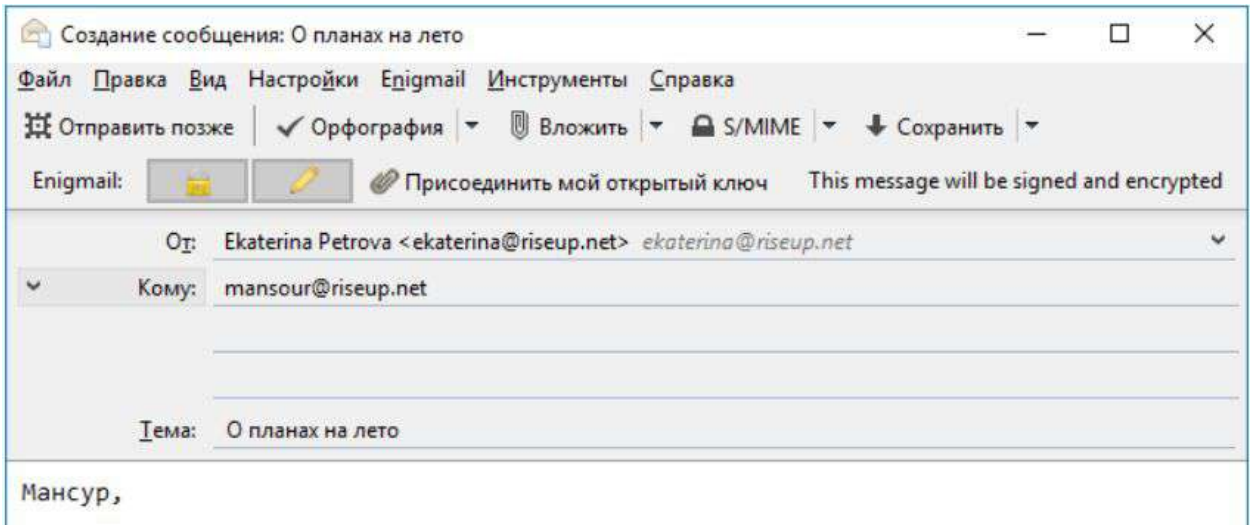


Рис 37. Составление зашифрованного письма

Важно. Включенная кнопка "замка" на панели инструментов говорит, что ваше сообщение будет зашифровано. Кнопка карандашика – что оно будет подписано. Убедитесь, что обе кнопки включены.

- По умолчанию Enigmail автоматически шифрует письма тем адресатам, чьи проверенные открытые ключи у вас есть.
- Мы включили подписывание зашифрованных сообщений в настройках Параметры учетной записи > Защита OpenPGP (см. выше).

Чтобы не шифровать или не подписывать сообщения, можно до отправки письма воспользоваться теми же кнопками замочка и карандашика. (Можно настроить Thunderbird так, чтобы письма по умолчанию не шифровались. Это можно сделать в меню Enigmail, далее пункт Настройки > Отправка > Установить собственные настройки шифрования).

4. Задание на лабораторную работу

1) Добавить учетную запись e-mail в Mozilla thunderbird
2) Установить расширение Enigmail
3) Создать пару ключей шифрования
4) Установить время действия ключа
5) Написание письма на почту своему напарнику
6) Шифрование сообщения
7) Добавление подписи в сообщении
8) Приложить открытый ключ к сообщению
9) Расшифровать письмо от напарника

5. Контрольные вопросы

1) Что такое Mozilla thunderbird, GnuPG и Enigmail?
2) Для чего нужна электронная подпись?
3) Для чего предназначены секретный и открытый ключи шифрования?
4) Чем отличается IMAP от POP3
5) Какие свойства имеют ключи шифрования

Лабораторная работа № 8
Одноранговые сети

1. Цель работы

Целью данной работы является получение навыков работы в локальных компьютерных сетях с ОС Windows.

2. Краткие теоретические сведения

Одноранговая сеть – это сеть равноправных компьютеров, каждый из которых имеет уникальное имя и может иметь пароль для входа во время загрузки ОС. Имя компьютера и пароль входа назначаются владельцем компьютера средствами ОС. Каждый компьютер такой сети может одновременно являться и сервером, и клиентом сети, хотя допустимо назначение одного компьютера только сервером, а другого только клиентом.

Достоинством одноранговых сетей является их высокая гибкость: в зависимости от конкретной задачи сеть может использоваться очень активно, либо совсем не использоваться. Из-за большой самостоятельности компьютеров в таких сетях редко бывает ситуация перегрузки, тем более, что количество компьютеров в таких сетях обычно невелико. Установка одноранговых сетей довольно проста, для них не требуются дополнительные дорогостоящие серверы. Кроме того, нет необходимости в системном администрировании, пользователи могут сами управлять своими ресурсами.

В одноранговых сетях допускается определение различных прав пользователей на доступ к сетевым ресурсам, но система разграничения прав не слишком развита. Если каждый ресурс защищен своим паролем, то пользователю приходится запоминать большое число паролей.

К недостаткам одноранговых сетей относятся также слабая система контроля и протоколирования работы сети, трудности с резервным копированием распределенной информации. Выход из строя любого компьютера-сервера приводит к потере части общей информации, по возможности все компьютеры должны быть высоконадежными.

Эффективная скорость передачи информации по одноранговой сети часто оказывается недостаточной, поскольку трудно обеспечить быстродействие процессоров, большой объем оперативной памяти и высокие скорости обмена с жестким диском для всех компьютеров сети. К тому же компьютеры сети работают не только на сеть, но и решают другие задачи.

3. Ход работы

3.1. Рабочие группы

Данная лабораторная работа выполняется на двух виртуальных машинах под управлением операционной системы Windows 8.1.

Для работы с рабочими группами на виртуальных машинах необходимо проверить, что в параметрах сетевого адаптера установлен пункт «Внутренняя сеть» (рис. 1). Так же устанавливаем внутреннюю сеть на Windows 8.1.

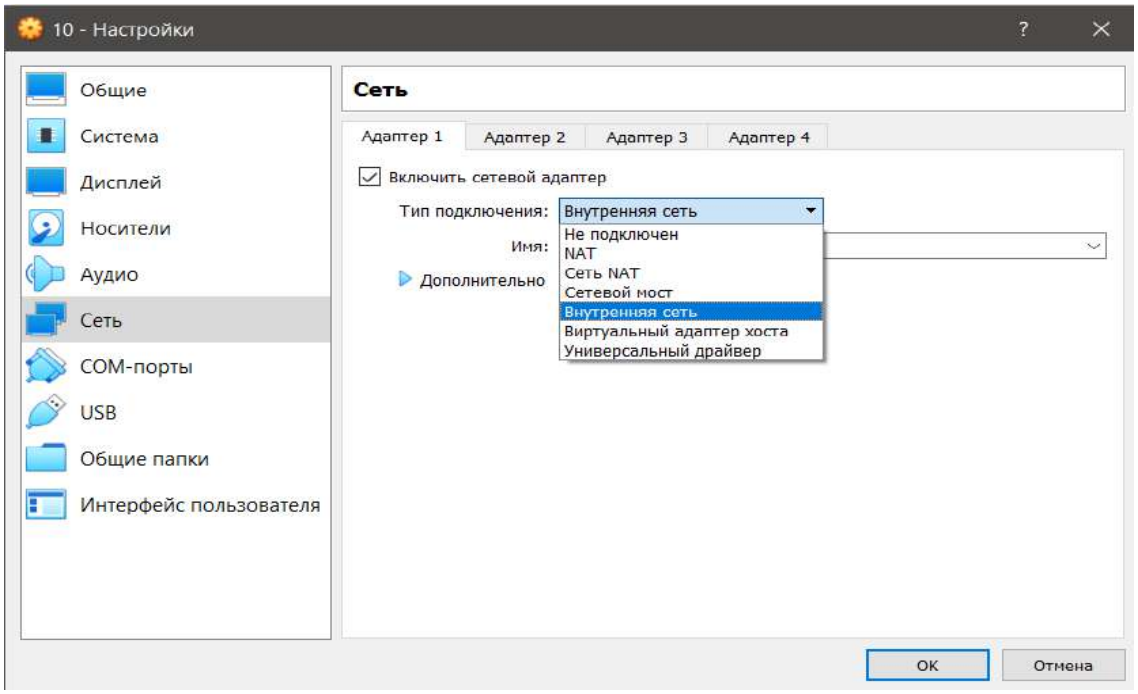


Рис. 1. Установка внутренней сети для операционной системы Win 10

При настройке сети Windows автоматически создает рабочую группу и присваивает ей имя. Существует возможность присоединиться к уже существующей рабочей группе в сети и создать новую.

Для проверки принадлежности компьютера к рабочей группе откройте свойства компьютера, перейдите на вкладку «Имя компьютера» (Пуск – Компьютер – Свойства – Дополнительные параметры системы – Имя компьютера). Чтобы компьютеры могли взаимодействовать они должны принадлежать одной рабочей группе (рис. 2).

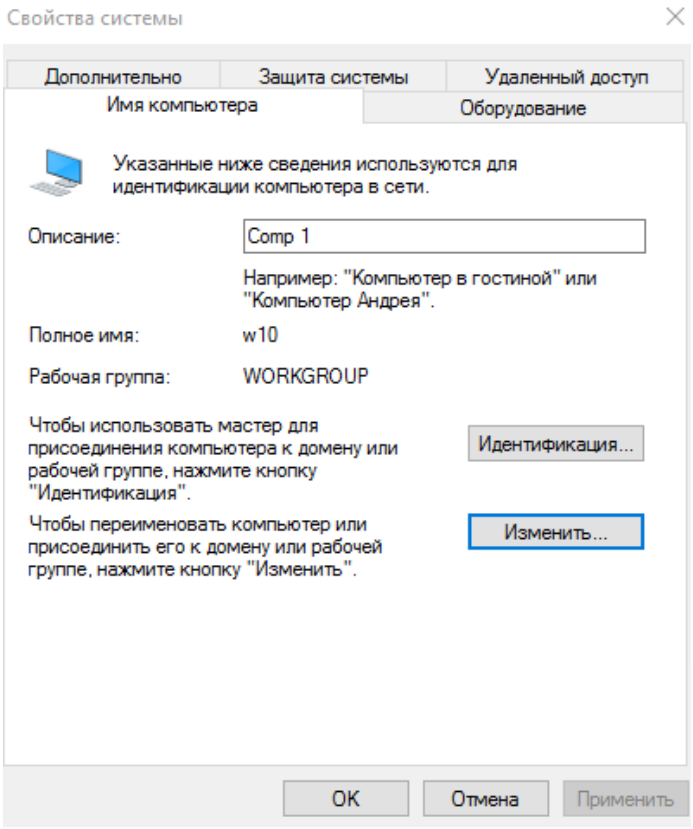


Рис. 2. Проверка принадлежности компьютера к рабочей группе

Чтобы переименовать компьютер или присоединить его к рабочей группе, нажмите кнопку «Изменить».

Чтобы присоединиться к существующей рабочей группе, необходимо ввести имя новой рабочей группы и нажать «ОК».

Для создания новой рабочей группы, также нужно ввести имя новой рабочей группы и нажать «ОК».

Присоедините гостевые ОС к одной рабочей группе: пользователей:

– в свойствах системы на вкладке «Имя компьютера» нажмите кнопку «Изменить»;

– выберите параметр «Является членом рабочей группы», введите имя рабочей группы (рис. 3) и нажмите «ОК»;

– в появившемся окне с сообщением о вступлении в рабочую группу нажмите «ОК» и перезагрузите гостевую ОС.

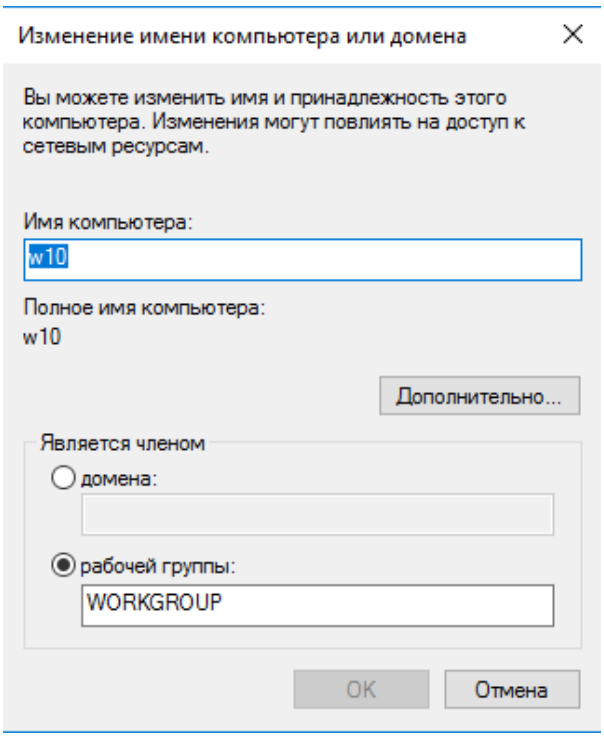


Рис. 3. Изменение рабочей группы компьютера

Далее заходим в центр управления сетями и общим доступом жмем на подключение “Ethernet”, заходим в свойства, находим в списке IP версии 4 (TCP/IPv4) и жмем на кнопку Свойства (рис. 4), в появившемся окне включаем использование следующих IP-адресов и вводим IP-адреса (рис.5).

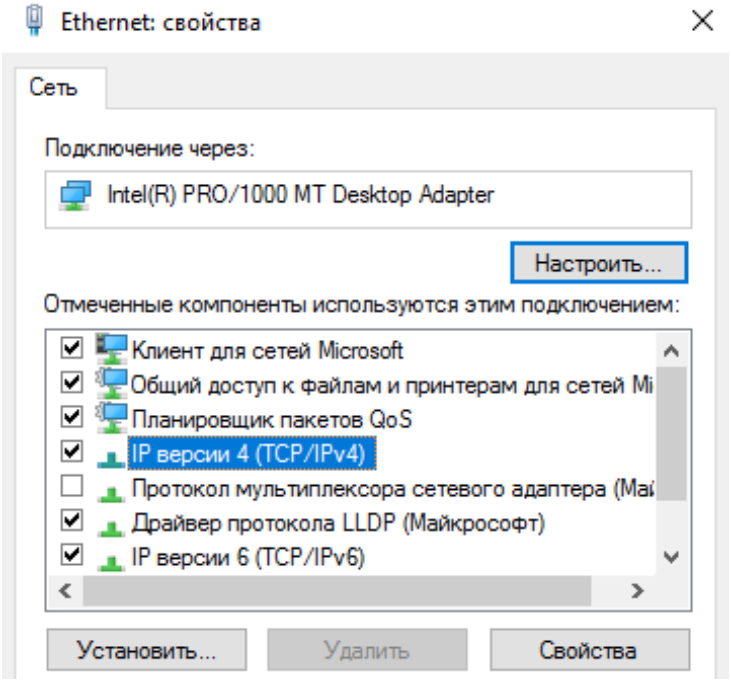


Рис. 4. Ethernet свойства

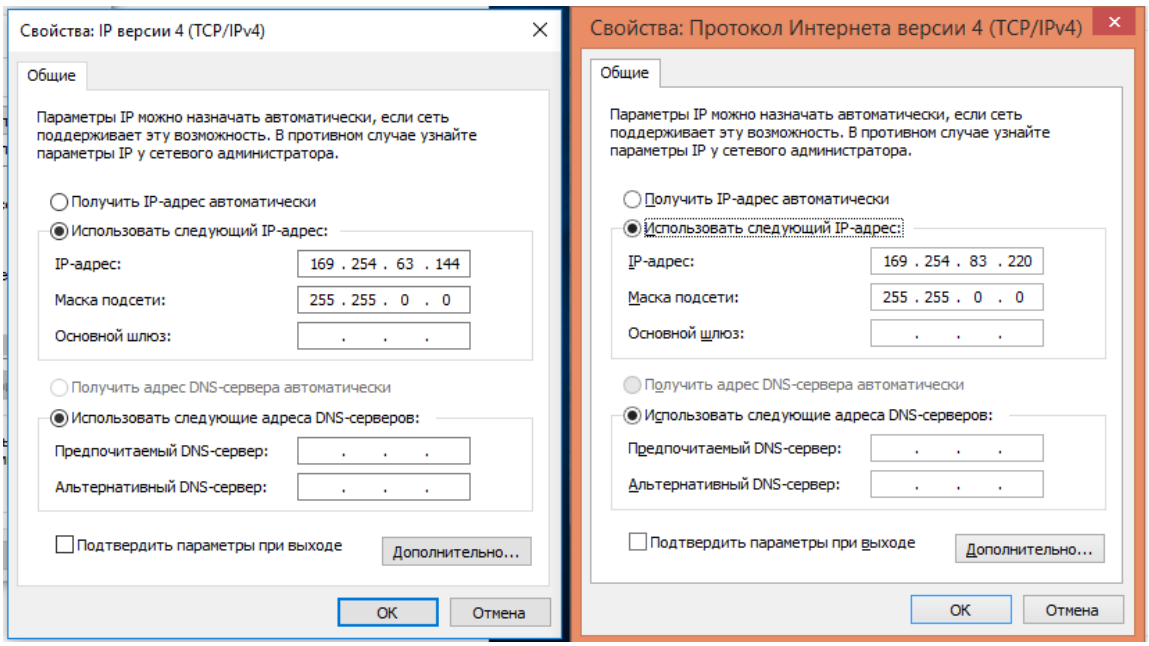


Рис. 5. Протокол Интернета версии 4 (TCP/IPv4)

Для просмотра компьютеров рабочей группы в графическом интерфейсе нужно открыть Сетевое окружение и нажать «Отобразить компьютеры рабочей группы».

Для просмотра компьютеров рабочей группы в командной строке запустите командную строку и выполните команду: net view (рис. 6).

```
C:\Windows\system32>net view
Имя сервера             Заметки

-------------------------------------------------------------------------------
\\W10                   comp 1
\\W81                   Comp 2
Команда выполнена успешно.
```

Рис. 6. Просмотр компьютеров рабочей группы

3.2. Настройка общего доступа к каталогам

Перед настройкой папки, проверьте параметры общего доступа. Для этого перейдите в Центр управления сетями и общим доступом из Панели управления. Далее перейдите Изменить дополнительные параметры общего доступа. Включите сетевое обнаружение и общий доступ к файлам (рис. 7).

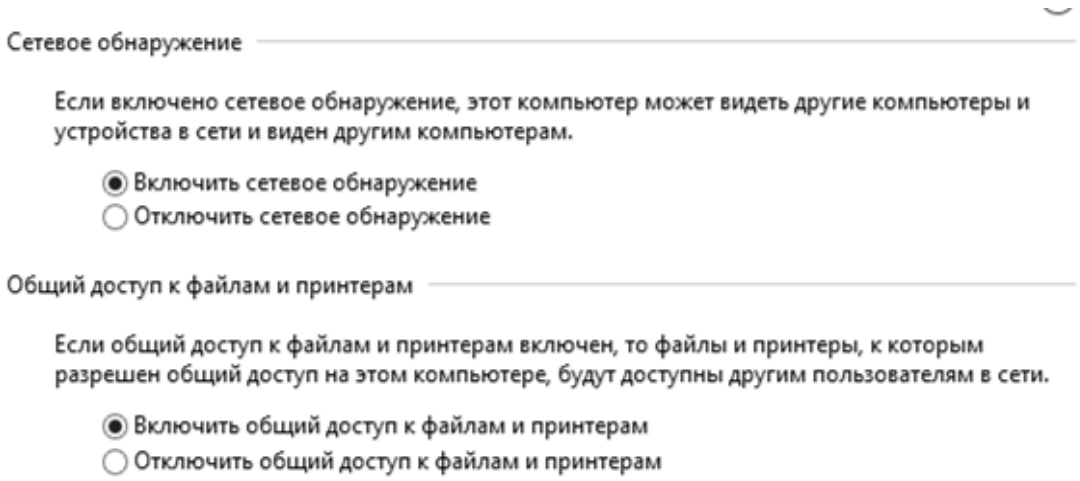


Рис. 7. Настройка сетевого обнаружения

Далее во вкладке Общий доступ с парольной защитой отключите её или установите пароль пользователю (рис. 8).

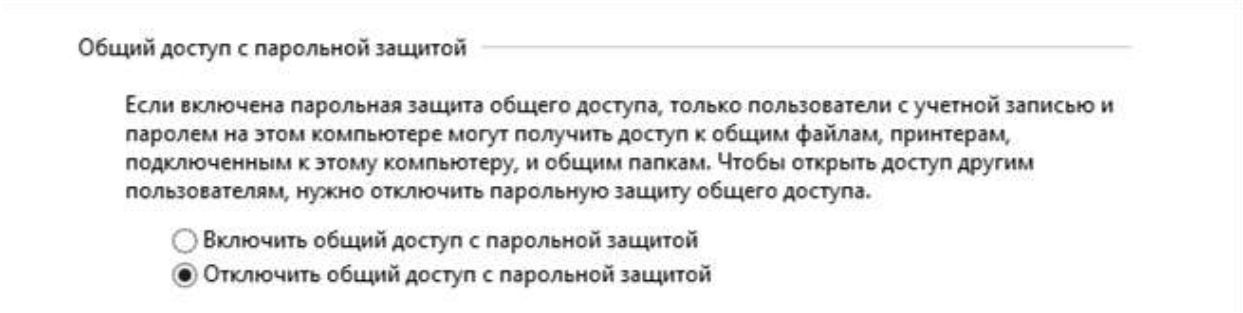


Рис. 8. Общий доступ с парольной защитой

Настройте общий доступ к папке, находящейся на сервере. Для этого выберите папку (можете создать папку на рабочем столе), нажмите на неё правой кнопкой мыши и выберете Свойства. Перейдите на вкладку Доступ и откройте «Общий доступ…», в выпадающем списке выберите пункт «Все» (рис. 9).

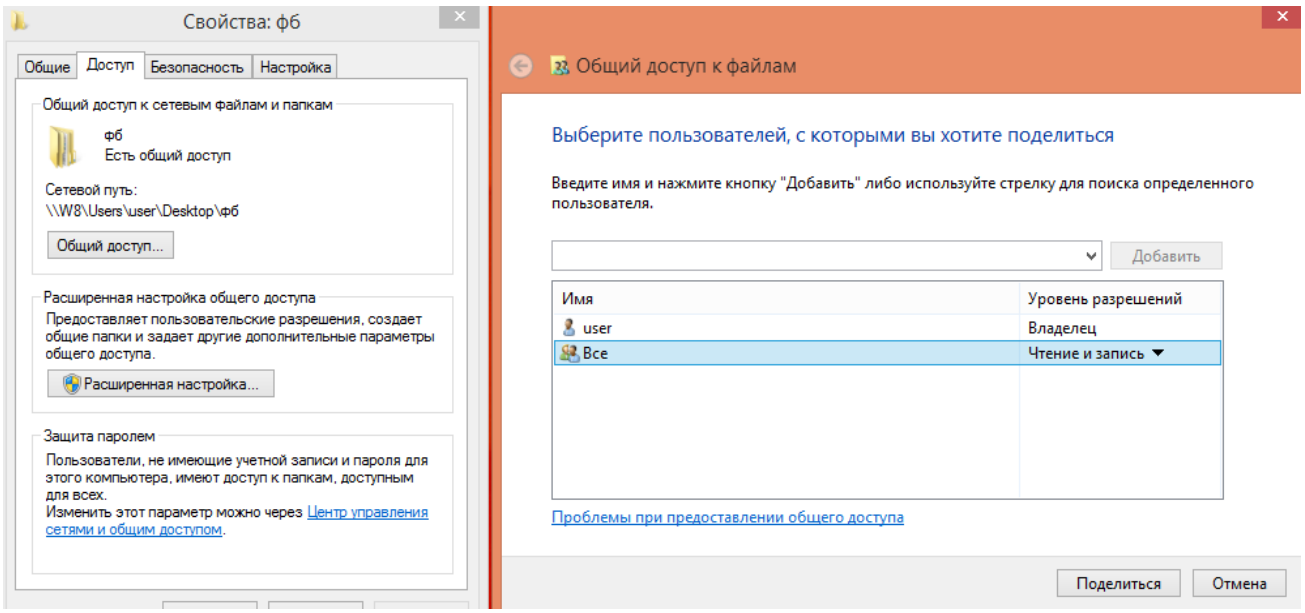


Рис. 9. Настройка общей папки

После настройки общего доступа к папке найдите ее в Сетевом окружении на второй машине и проверьте возможность добавления и изменения файлов.

Для подключения сетевой папки (т.е. для подключения общей папки как сетевого диска) на второй машине, вызовите контекстное меню Компьютера и выберите «Подключить сетевой диск» (рис. 10).

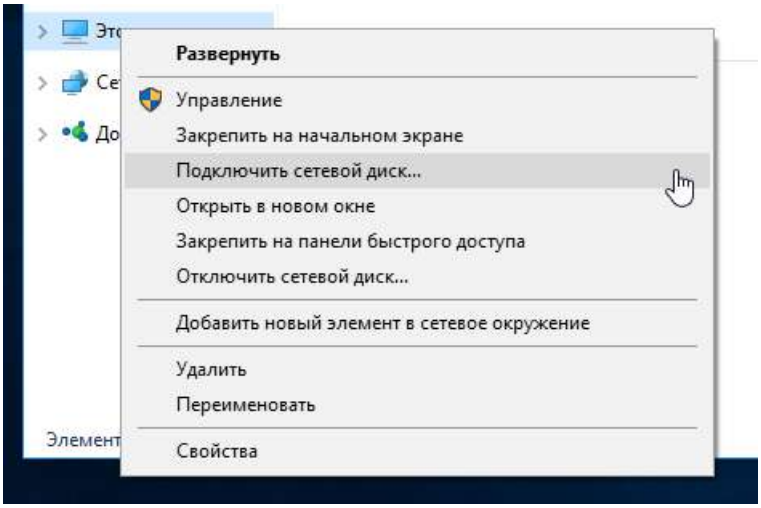


Рис. 10. Подключение сетевого диска

В появившемся окне (рис. 11) задайте букву сетевого диска и установите параметр «Восстанавливать при входе в систему», нажмите «Готово». Теперь общая папка будет отображаться в папке «Компьютер» как сетевой диск.

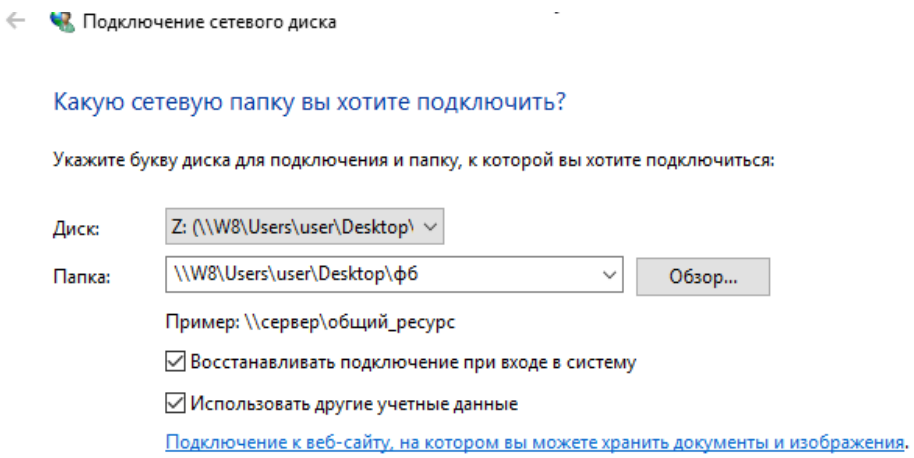


Рис. 11. Подключение сетевого диска

3.2. Настройка удаленного доступа

Для настройки удаленного доступа к компьютеру можно воспользоваться стандартными средствами Windows. Для этого удаленный компьютер должен быть включен и подключен к сети, удаленный доступ должен быть включен.

Настройте удаленный доступ:

– откройте свойства компьютера (win 10), выберите «Дополнительные параметры системы» и перейдите на вкладку «Удаленный доступ» (рис. 12.);

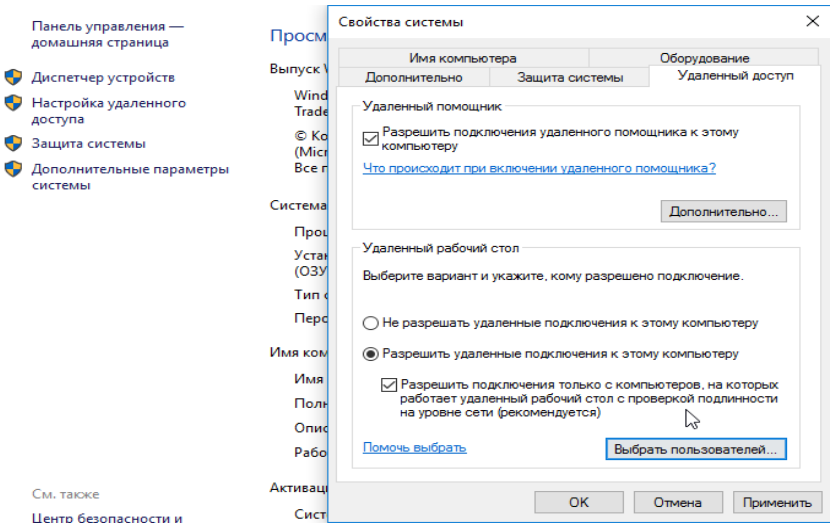


Рис. 12. Настройка параметров удаленного использования компьютера

– в группе «Удаленный помощник» установите параметр «Разрешить отправку приглашений удаленному помощнику», нажмите кнопку «Дополнительно», установите параметр «Разрешить удаленное

управление этим компьютером», задайте предельный срок 8 часов и нажмите «ОК»;

– в группе «Удаленный рабочий стол» выберите третий параметр и нажмите кнопку «Выбрать пользователей»;

– в появившемся окне нажмите кнопку «Добавить», введите имя пользователя, нажмите кнопку «Проверить имена» и нажмите ОК (рис. 13). Если учетные записи на машинах совпадают, как в данном случае, то этот пункт проделывать нет необходимости;

– нажмите кнопку «Применить» на вкладке «Удаленные сеансы» для вступления изменений в силу.

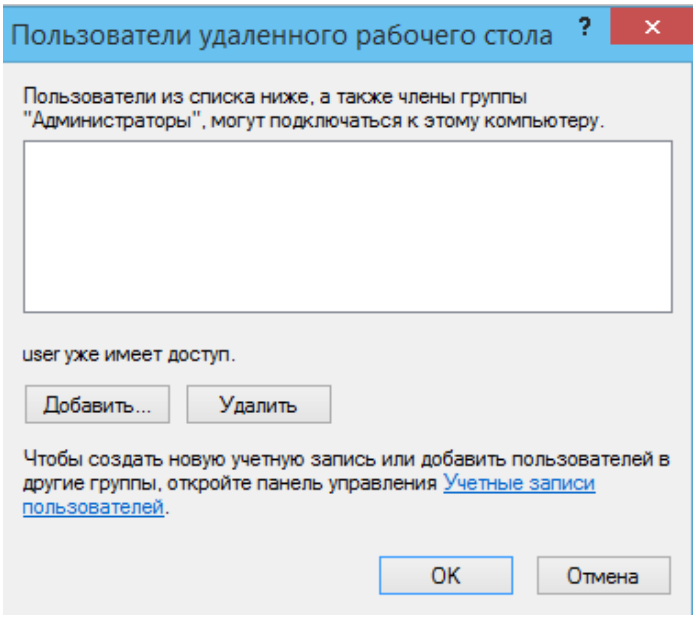


Рис. 13. Добавление пользователей удаленного доступа

Для того, чтобы подключиться к компьютеру с использованием удаленного доступа, войдите в компьютер-клиент (win 8.1), перейдите в меню Пуск – Все программы – Стандартные – Подключение к удаленному рабочему столу (рис. 14). Введите имя компьютера или его ip-адрес. Далее нажмите кнопку «Подключить». Необходимо выполнить вход в систему, после чего можно работать с компьютером с помощью удаленного доступа.

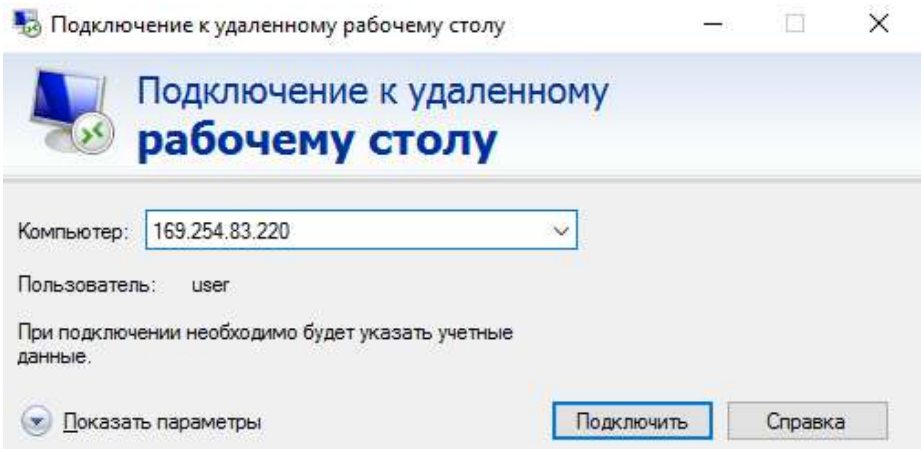


Рис. 14. Подключение к удаленному рабочему столу

4. Задание на лабораторную работу

1. Изучить теоретические сведения.
2. Создать рабочую группу из двух компьютеров, назвать её своим кафедральным именем (717_gdv).
3. Настроить общий доступ и проверить его работу, папку назвать своим полным именем.
4. Настроить удаленный доступ и проверить его работу.
5. Написать отчет по проделанной работе и защитить его у преподавателя.

5. Контрольные вопросы

1. Что такое одноранговая сеть?
2. Каковы достоинства и недостатки одноранговых сетей?
3. Что нужно сделать, чтобы создать рабочую группу?
4. Какое условие должно выполняться, чтобы компьютеры могли взаимодействовать?
5. Какую команду необходимо ввести в командной строке для просмотра компьютеров рабочей группы?
6. Что такое удаленный доступ?
7. Как настроить удаленный доступ?
8. Существуют ли альтернативные способы создания рабочей группы в операционных системах Windows? Если да, то какие?
9. Как просмотреть компьютеры рабочей группы в графическом интерфейсе?
10. Как присоединить гостевую ОС к рабочей группе?

Лабораторная работа № 9
Настройка домена на примере Active Directory

1. Цель работы

Целью данной работы является получение навыков работы в локальных компьютерных сетях с ОС Windows с доменной структурой и управления пользователями и компьютерами домена с помощью групповых политик безопасности домена.

2. Краткие теоретические сведения

Доменом называется отдельная область безопасности в компьютерной сети Microsoft Windows.

В домене один или несколько компьютеров являются серверами. Администраторы сети используют серверы для контроля безопасности и разрешений для всех компьютеров домена. Это позволяет легко изменять настройки, так как изменения автоматически производятся для всех компьютеров.

Пользователи домена должны указывать пароль или другие учетные данные при каждом доступе к домену. Если пользователь имеет учетную запись в домене, он может войти в систему на любом компьютере. Для этого не требуется иметь учетную запись на самом компьютере.

В домене могут быть тысячи компьютеров. Компьютеры могут принадлежать к различным локальным сетям. В каждом домене действует своя политика безопасности и свои отношения безопасности с другими доменами. Если несколько доменов связаны доверительными отношениями и имеют одни и те же схему, конфигурацию и глобальный каталог, их называют деревом доменов. Несколько деревьев доменов могут быть объединены в лес.

Под групповой политикой понимается совокупность параметров и настроек системы, определяющая конкретное окружение пользователя. Администратор может использовать механизм групповых политик для

централизованного управления средой пользователей. Политика безопасности позволяет единообразно конфигурировать большое количество субъектов безопасности. Например, определить уровень доступа к системному реестру или задать порядок осуществления аудита событий.

Папка Мои документы традиционно рассматривается как место хранения пользовательских документов. Посредством механизма групповой политики администратор может задать перенаправление всех обращений пользователей к этой папке на некоторый сетевой ресурс.

Параметры групповой политики хранятся в виде объектов групповой политики (Group Policy Object, GPO). Эти объекты хранятся в каталоге подобно другим объектам. Различают два вида объектов групповой политики – объекты групповой политики, создаваемые в контексте службы каталога, и локальные объекты групповой политики.

Локальные объекты групповой политики (Local Group Policy Object, LGPO) создаются в процессе установки операционной системы Windows и используются, если компьютер не включен в состав домена. Как только компьютер подключается к домену, компьютер и пользователь, работающий на нем, подпадают под действие объектов GPO, определенных в контексте данного домена.

Любой объект групповой политики может быть привязан к некоторому сайту, домену или подразделению, тогда параметры данного объекта групповой политики будут распространяться на все объекты службы каталога, зарегистрированные в данном контейнере. Один объект групповой политики может быть привязан к множеству контейнеров. Так же несколько объектов групповой политики могут быть привязаны к одному контейнеру.

Множество параметров, определяемых в рамках объекта групповой политики, разделено на две части: конфигурирование компьютера и конфигурирование среды пользователя. Конфигурирование компьютера предполагает определение значений для параметров, влияющих на формирование окружения любых пользователей, регистрирующихся на

данном компьютере. Конфигурирование среды пользователя дает возможность управлять процессом формирования окружения конкретного пользователя, независимо от того, на каком компьютере он регистрируется в сети. Категории параметров групповой политики организованы в три контейнера в соответствии со своим назначением:

– Конфигурация программ. В контейнере размещаются категории параметров групповой политики, посредством которых можно управлять перечнем приложений, доступных пользователям.

– Конфигурация Windows. В контейнере размешаются категории параметров групповой политики, определяющие настройки непосредственно самой операционной системы. Содержимое данного контейнера может быть различным, в зависимости от того, определяются параметры групповой политики для пользователя или для компьютера.

Административные шаблоны. Этот контейнер содержит категории параметров групповой политики, применяемых для управления содержимым системного реестра компьютера.

3. Ход работы

3.1. Создание домена

Данная лабораторная работа выполняется на двух виртуальных машинах: под управлением операционных систем Windows 10 и Windows Server 2012. Проверьте, что в параметрах сетевого адаптера виртуальных машин установлен пункт «Внутренняя сеть». Перед началом работы не забудьте сконфигурировать сетевые соединения на обеих виртуальных машинах, а именно задать IP адреса и маски подсети (рис. 1).

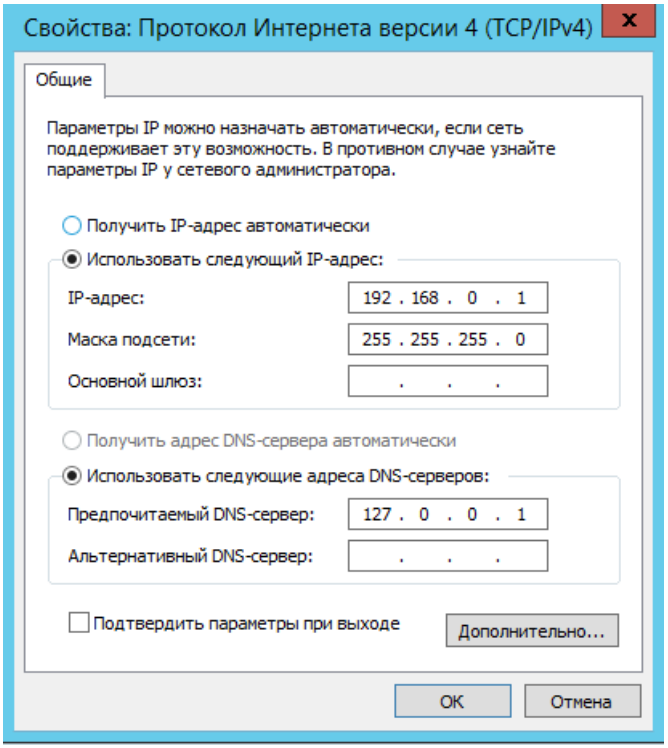


Рис. 1. Настройка IP адреса и маски подсети

Запустите виртуальную машину с ОС Windows Server, войдите в систему от имени администратора. Запустите Диспетчер серверов. Выберите «Добавить роли и компоненты», запустив тем самым «Мастер добавления ролей и компонентов» (рис. 2).

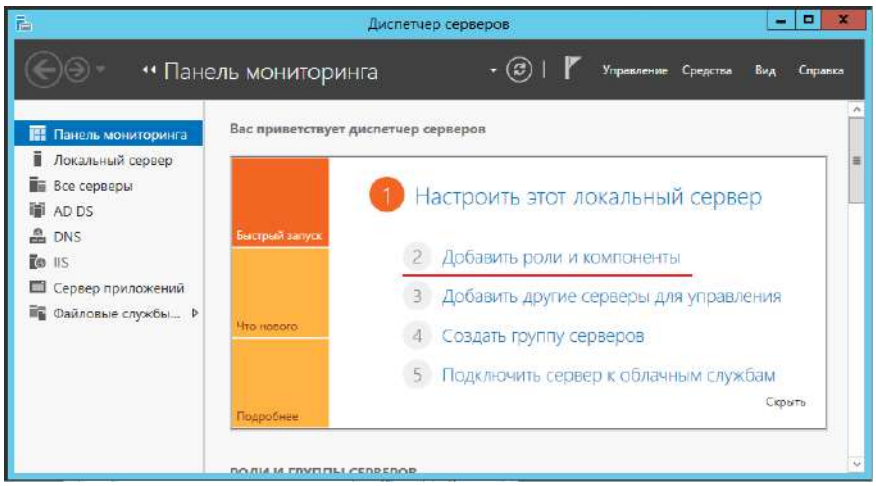


Рис. 2. Диспетчер серверов

1. На первой странице мастер напоминает, что необходимо сделать перед началом добавления роли на сервер. Нажмите «Далее».

2. На втором шаге нужно выбрать «Установка ролей и компонентов» и нажать «Далее».

3. Выберите сервер, на который необходимо установить роль AD и снова нажмите «Далее».

4. На этом шаге нужно выбрать роль, которую мы хотим добавить на компьютер, отметьте галочкой «Доменные службы Active Directory» (Рис. 3). Откроется окно, в котором будет предложено установить службы ролей или компоненты, необходимые для установки роли AD, нажмите кнопку «Добавить компоненты», после чего кликните «Далее».

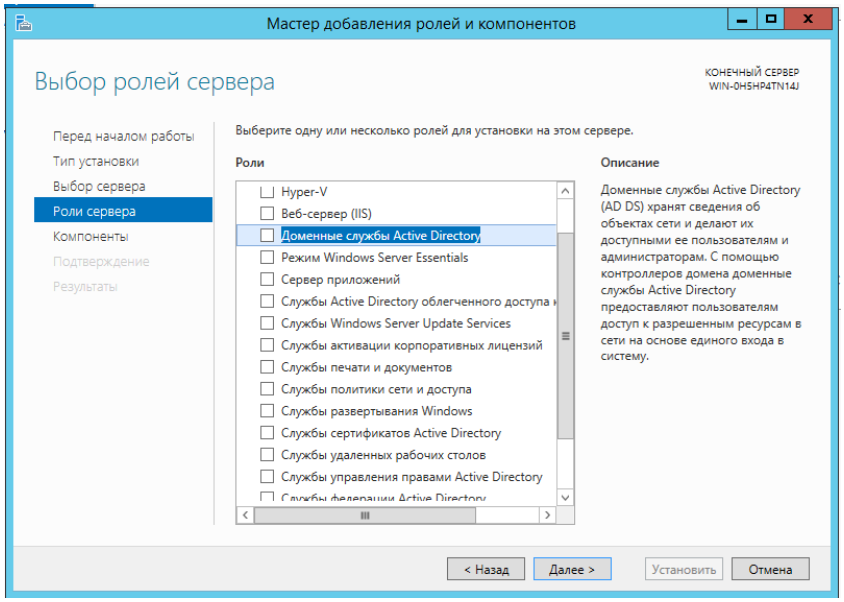


Рис. 3. Мастер добавления ролей и компонентов

5. На шаге выбора компонентов для установки нажмите «Далее».

6. Вы увидите описание роли Доменных служб Active Directory. Прочтите описание роли и пункт «На что обратить внимание», затем нажмите «Далее».

7. Перед установкой будут показаны компоненты, которые будут добавлены на сервер, нажмите «Установить».

8. После того, как установка будет завершена, нажмите «Закрыть» (рис. 4).

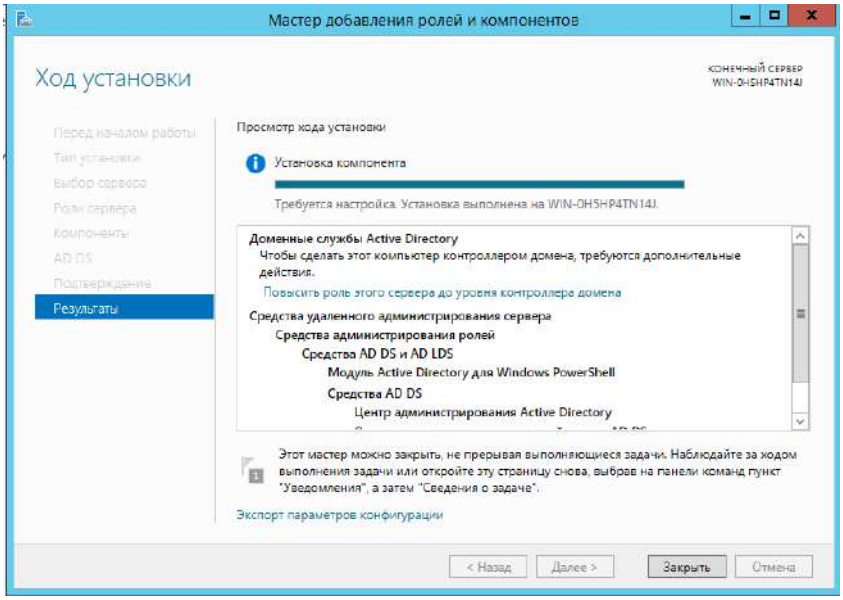


Рис. 4. Установка доменной службы Active Directory

После того, как роль была добавлена на сервер, необходимо настроить доменную службу. Запустите «Мастер настройки доменных служб Active Directory», для чего нажмите на иконку «Уведомления» в диспетчере сервера, затем нажмите «Повысить роль этого сервера до уровня контроллера домена» (рис. 5).

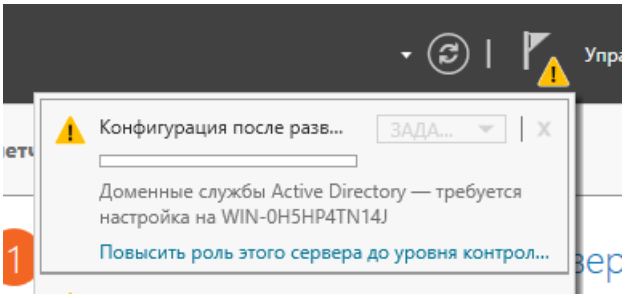


Рис. 5. Повышение роли сервера до уровня контроллера домена

1. Выберите пункт «Добавить новый лес», после этого впишите имя домена в поле «Имя корневого домена». Полное имя домена задается в формате доменных имен сети Интернет, например, headquarters.example.microsoft.com или keva.int. Задайте имя своему домену (например, keva.su) (рис. 6). Нажмите «Далее».

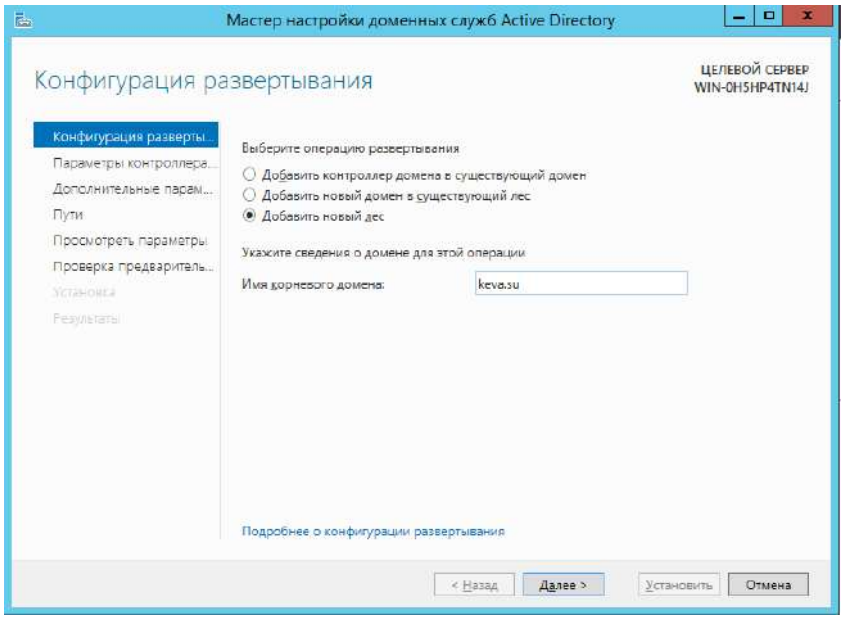


Рис. 6. Добавление нового леса

2. На этом шаге можно изменить совместимость режима работы леса и корневого домена. Оставьте настройки по умолчанию. Задайте пароль для DSRM (Directory Service Restore Mode – режим восстановления службы каталога) и нажмите «Далее».

3. Мастер предупредит, что делегирование для этого DNS-сервера создано не было. Нажмите «Далее».

4. Будет предложено задать NetBIOS имя домена, которое используется младшими версиями операционных систем Microsoft Windows для идентификации домена, оставьте его по умолчанию.

5. Необходимо указать путь к файлу базы данных Active Directory, лог-файлу и путь к папке SYSVOL, которая содержит общие файлы и реплицируется другими контроллерами домена. Оставьте значения по умолчанию.

6. Проверьте, какие параметры были выбраны для установки. Можно просмотреть сценарий Windows PowerShell для развертывания AD DS. Нажмите «Далее».

7. Мастер проверит, соблюдены ли предварительные требования, после чего покажет отчёт. Одно из обязательных требований – это установленный пароль на профиль локального администратора. Внизу можно видеть предупреждение мастера о том, что после нажатия кнопки «Установить» уровень сервера будет повышен до контроллера домена и произойдёт автоматическая перезагрузка. Нажмите «Установить» (рис. 7).

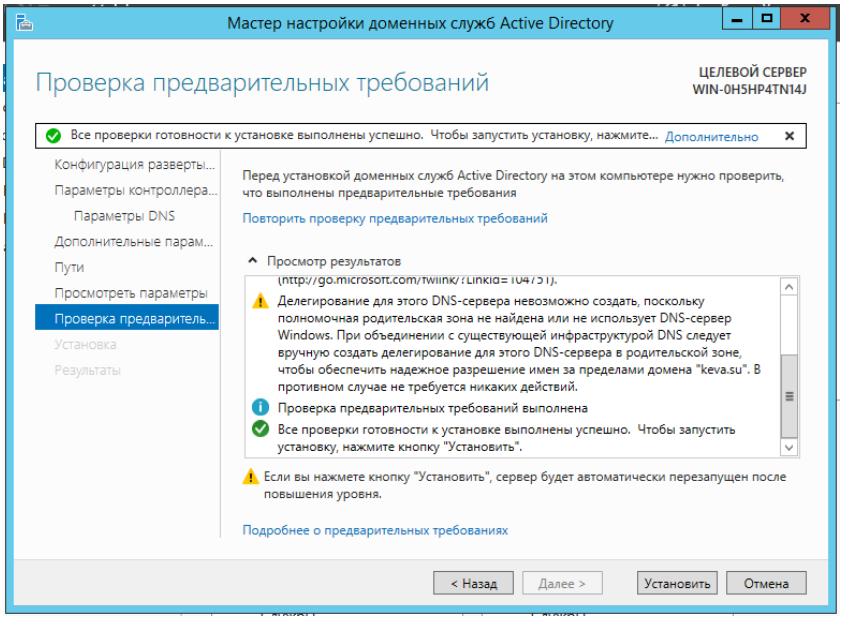


Рис. 7. Мастер настройки доменных служб AD

8. Когда установка будет закончена, компьютер перезагрузится, и вы сможете ввести первый компьютер в домен. Для этого введите логин и пароль администратора домена и нажмите «Войти».

Нужно добавить новых пользователей в домен, после чего можно присоединить компьютер к домену и войти в домен под новым пользователем.

Запустите оснастку «Пользователи и компьютеры Active Directory» (рис. 8), для чего перейдите в Пуск – Панель управления – Система и безопасность – Администрирование – Пользователи и компьютеры Active Directory.

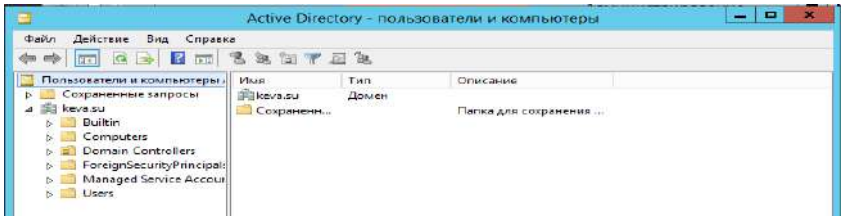


Рис. 8. Оснастка «Пользователи и компьютеры Active Directory»

Выделите название домена и вызовите контекстное меню, в котором выберите (Создать – Подразделение) (рис. 10). Введите имя для подразделения и нажмите «ОК» (рис. 9).

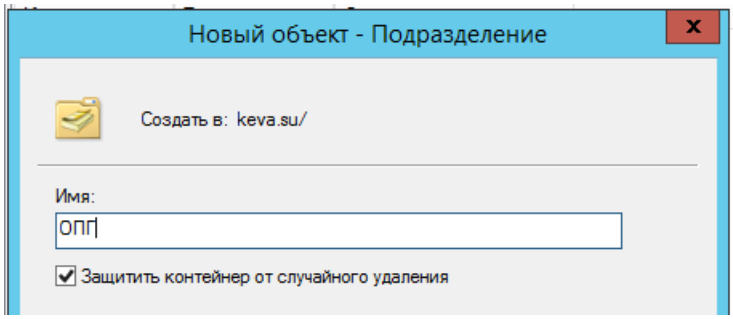


Рис. 9. Создание нового подразделения

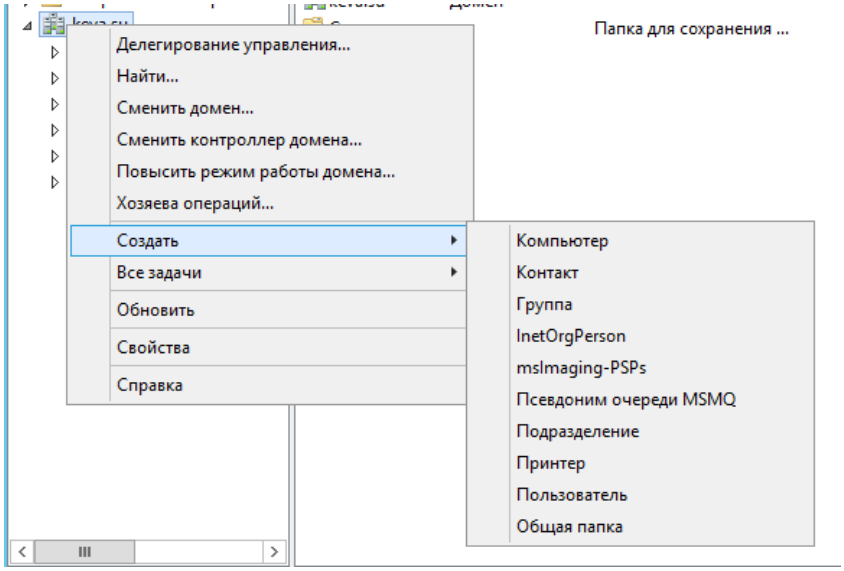


Рис. 10. Путь к Подразделению

Подразделения служат для управления группами компьютеров пользователей. Например, можно разбить пользователей по группам с именами подразделений, соответствующих названиям отделов компании, в

которой они работают (бухгалтерия, отдел кадров, менеджеры и др.).

Создайте учетную запись пользователя в новом подразделении. Для этого в контекстном меню нового подразделения выберите пункт Создать – Пользователь (рис. 11).

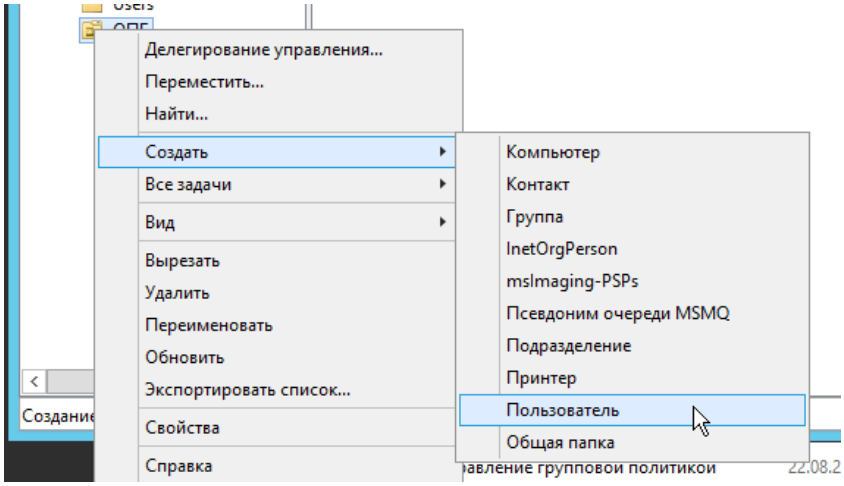


Рис. 11. Контекстное меню

Форма создания нового пользователя представлена на рис. 12.

На следующем шаге мастера создания нового объекта необходимо задать пароль учетной записи пользователя и дополнительные параметры. По умолчанию пароль должен соответствовать требованиям сложности, т.е. содержать три из четырех групп символов: заглавные буквы, строчные буквы, цифры, специальные знаки (. , + – = ? № $ и т.д.). Установите параметр «Требовать смену пароля при следующем входе в систему». Выясните назначение других параметров и установите нужные. Подтвердите создание новой учетной записи.

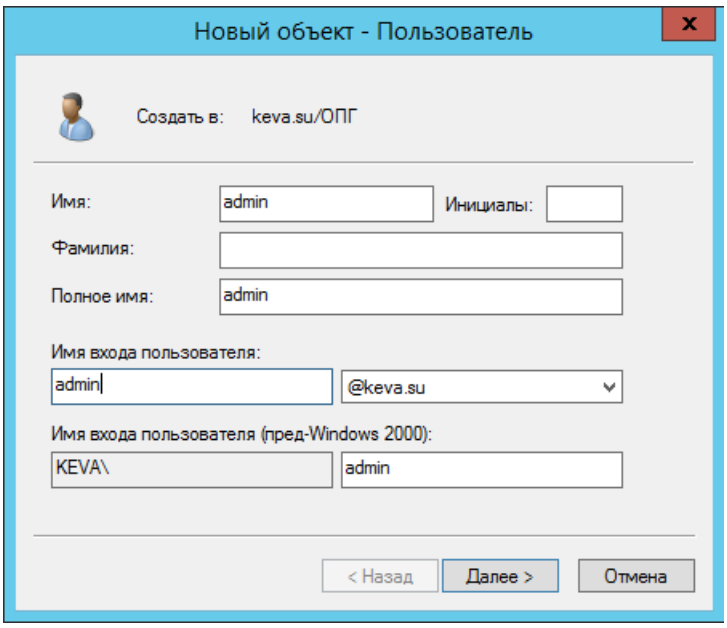


Рис. 12. Создание нового пользователя

Создайте учетную запись группы безопасности в новом подразделении. Для этого в контекстном меню нового подразделения выберите пункт (Создать – Группа). Форма создания группы представлена на рис. 13.

При создании новой группы безопасности необходимо ввести имя, область действия и тип группы. Область действия определяет видимость данной группы в службе каталога. Глобальная группа видна в любом домене службы каталога и ей могут назначаться привилегии доступа к ресурсам других доменов. Локальная группа видна только в своем домене, т.е. ей будут доступны ресурсы только ее домена. Группы безопасности позволяют объединять пользователей и другие группы для назначения им одинаковых привилегий на различные объекты. Группы распространения используются для рассылки сообщений, они не участвуют в разграничении прав доступа.

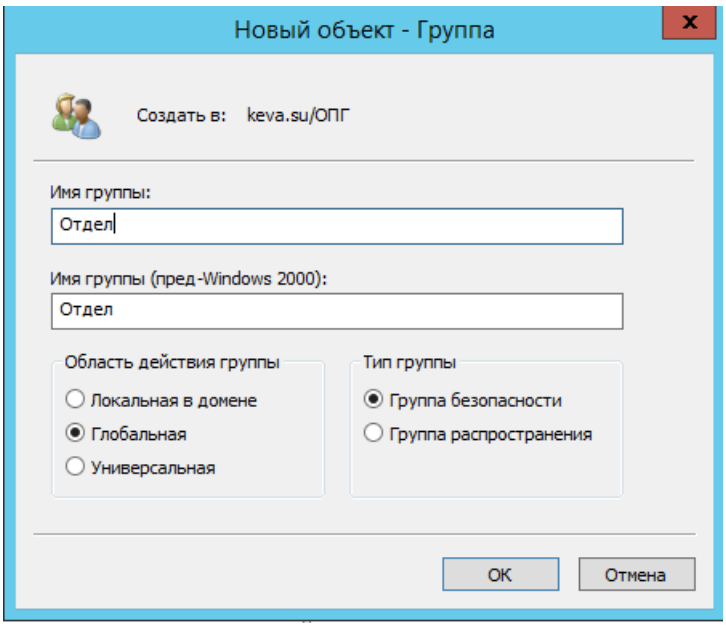


Рис. 13. Создание группы

Теперь нужно ввести компьютер в домен и зайти под новым пользователем. Укажите на клиентском компьютере DNS-адрес. Для этого откройте «Свойства сетевого подключения» (Пуск – Панель управления – Сеть и Интернет – Центр управления сетями и общим доступом – Изменение параметров адаптера), вызовите контекстное меню подключения и выберите «Свойства». Выделите «Протокол Интернета версии 4 (TCP/IPv4)», нажмите кнопку «Свойства», выберите «Использовать следующие адреса DNS-серверов» и в поле «Предпочитаемый DNS-сервер» укажите адрес вашего DNS-сервера. Проверьте, что задан IP-адрес и маска той же подсети, в которой находится сервер (рис. 14).

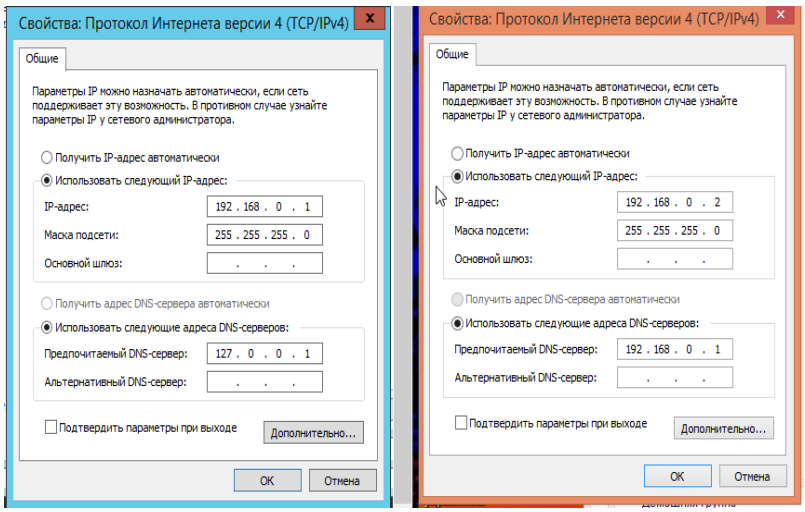


Рис. 14. Настройка IP адресов

Для определения IP адреса машины нужно открыть консоль сочетанием клавиш Win + R и ввести команду ipconfig. Проверить соединение можно командой ping.

Присоедините компьютер к домену. Откройте свойства системы (Пуск – Панель управления – Система и безопасность – Система – Дополнительные параметры системы). Выберите вкладку «Имя компьютера» и нажмите «Изменить». Выберите «Компьютер является членом домена» и введите имя домена (рис. 15). После этого необходимо ввести логин и пароль пользователя с правами присоединения к домену (обычно администратора домена). Если вы всё указали правильно, то появиться приветственное сообщение «Добро пожаловать в домен ...». Для того чтобы завершить присоединение, необходима перезагрузка.

После перезагрузки войдите в систему под доменной учётной записью пользователя, которая была создана ранее.

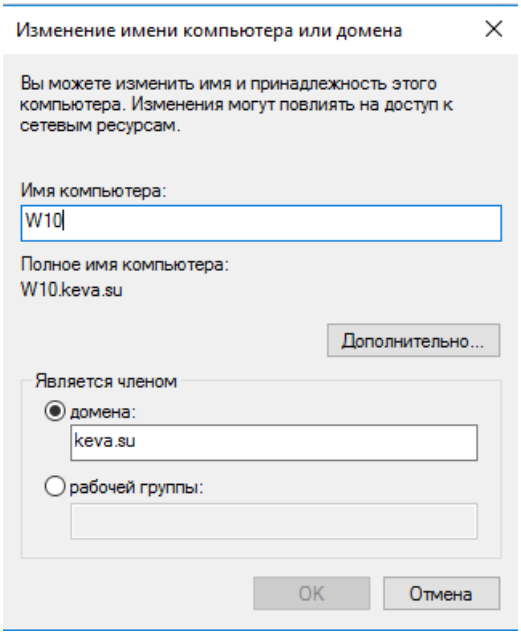


Рис. 15. Присоединение компьютера к домену

Войдите в систему Windows Server под учетной записью Администратора. Нажмите «Пуск» и перейдите в окно Управления групповой политикой (рис. 16).

Для создания нового объекта групповой политикой нажмите правой кнопкой на «Объекты групповой политики», выберите «Создать» и укажите имя объекта (рис. 17).

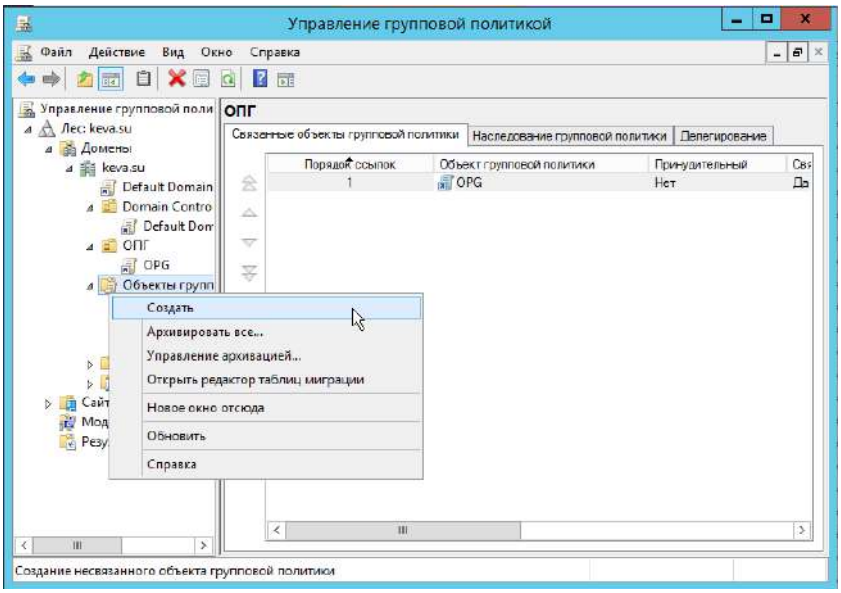


Рис. 16. Вид окна управления групповой политикой

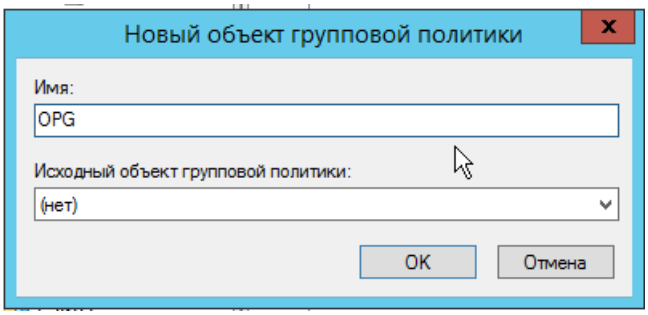


Рис. 17. Создание объекта групповой политики

Теперь необходимо привязать данный объект групповой политики к созданному контейнеру. Для этого нажмите правой кнопкой на созданное подразделение и выберите «Связать существующий объект групповой политики…» (рис. 18), затем выберите созданный ранее объект в списке (рис. 19) и нажмите «ОК».

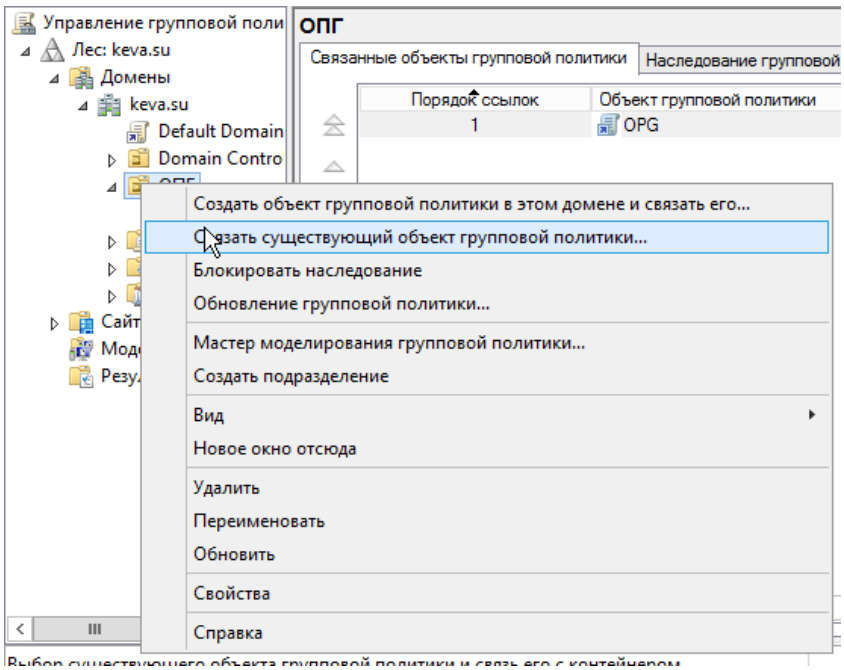


Рис. 18. Привязка объекта групповой политики

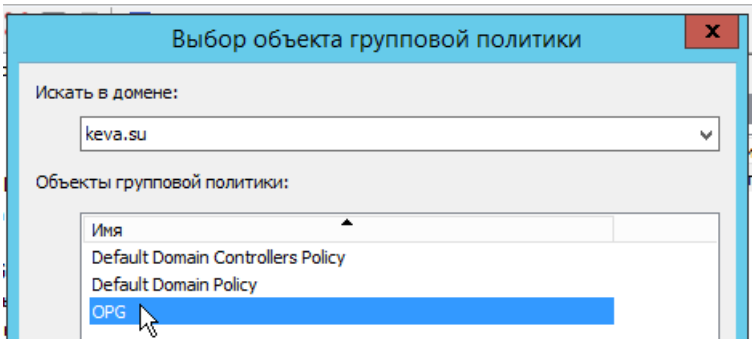


Рис. 19. Выбор объекта групповой политики

Выбранный объект должен появиться в списке связанных объектов групповой политики. Для редактирования параметров, определяемых данным объектом, нажмите на него правой кнопкой и выберите «Изменить» (рис. 20).

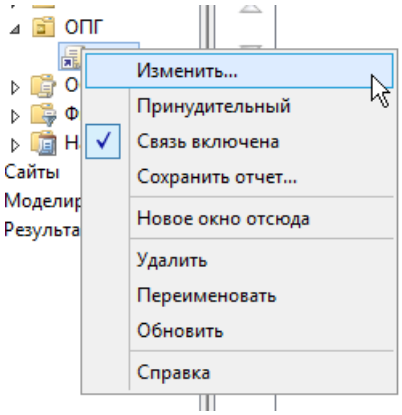


Рис. 20. Контекстное меню объекта

3.2. Установка параметров безопасности

Ограничение на параметры парольной системы защиты задаются в контексте «Конфигурация компьютера». Выберите Конфигурация Windows – Параметры безопасности – Политики учетных записей – Политика паролей (рис. 21).

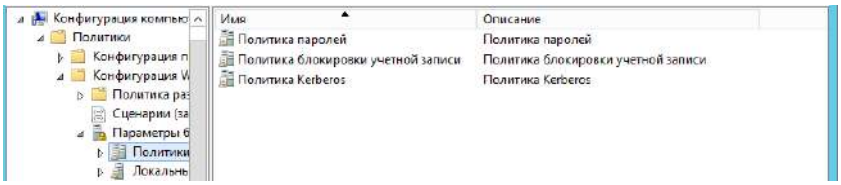


Рис. 21. Политики учетных записей

В данном разделе объекта групповой политики определяются следующие параметры:

– «Минимальный срок действия пароля» задает периодичность смены пароля;

– «Минимальная длина пароля» определяет минимальное количество знаков пароля;

– «Максимальный срок действия пароля» определяет интервал времени, через который разрешается менять пароль;

– «Пароль должен отвечать требованиям сложности» определяет требования к составу групп знаков, которые должен включать пароль;

– «Хранить пароли, используя обратимое шифрование» задает способ хранения пароля в базе данных учетных записей;

– «Вести журнал паролей» определяет количество хранимых устаревших паролей пользователя.

Укажите необходимые значения данных параметров. Ознакомьтесь с параметрами из группы Параметры безопасности.

3.3. Политика ограниченного использования программ

Объекты групповой политики позволяют запретить запуск определенных программ на всех компьютерах, на которые распространяется

действие политики. Для этого необходимо в объекте групповой политики создать политику ограниченного использования программ и создать необходимые правила.

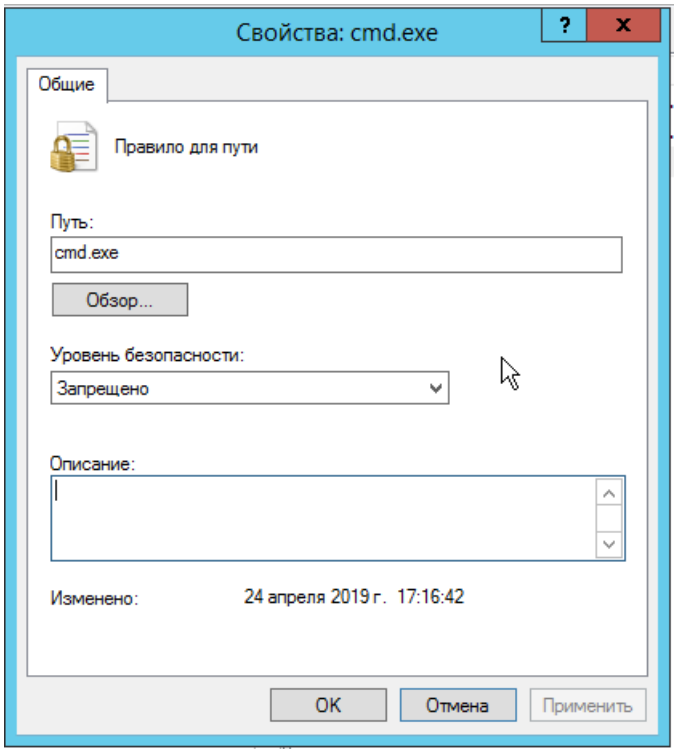


Рис. 22. Окно создания правила для пути политики ограниченного использования программ

Выберите раздел Конфигурация пользователя – Политики – Конфигурация Windows – Параметры безопасности – Политики ограниченного использования программ. Нажмите правой кнопкой на «Политики ограниченного использования программ», далее заходим в “Дополнительные правила” и жмем ПКМ и выбираем “Создать правило для пути (рис. 22-23).

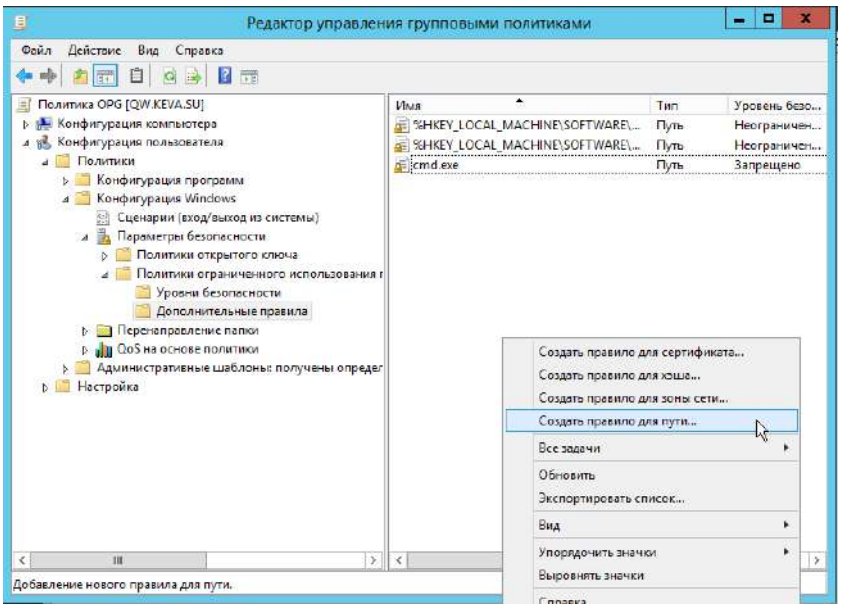


Рис. 23. Создание правило для пути

После обновления объекта групповой политики на рабочей станции, политика ограниченного использования программ вступит в действие и запуск программ, соответствующих правилам, будет невозможен.

4. Задание на лабораторную работу

1) Изучить теоретические сведения.
2) Задать серверу роль контроллера домена.
3) Присоединить рабочую станцию к домену.
4) Создать новый объект групповой политики и привязать его к созданному подразделению.
5) С помощью нового объекта групповой политики выполнить следующие действия:
– установить на рабочей станции приложение;
– задать ограничения на параметры парольной системы защиты;
– запретить запуск определенных программ на компьютере пользователя;
– настроить перенаправление папки «Мои документы» на одну из сетевых папок сервера;
– установить несколько административных шаблонов, запрещающих пользователю какие-либо действия
6) На рабочей станции проверить работу настроек, которые заданы в групповой политике.
7) Написать отчет и защитить его у преподавателя.

5. Контрольные вопросы

1. Что такое домен?
2. Сколько компьютеров может находиться в домене?
3. Что понимается под групповой политикой?
4. В чем различие между локальными политиками безопасности и групповыми политиками домена?

5. Какова структура объекта групповой политики, в какой последовательности применяются разделы объекта групповой политики?
6. Каково назначение административных шаблонов в групповой политике, как создать новый административный шаблон?
7. Для кого чего можно применять режимы планирования и ведения журналов?
8. Для чего нужен журнал паролей?
9. Что содержится в контейнере Конфигурация программ?
Что содержится в контейнере Конфигурация Windows?

ЛАБОРАТОРНАЯ РАБОТА №10

АУТЕНТИФИКАЦИЯ В ОПЕРАЦИОННЫХ СИСТЕМАХ ПРИ ПОМОЩИ ФИЗИЧЕСКОГО ОБЪЕКТА

В лабораторной работе рассмотрены утилиты и приложения, позволяющие производить аутентификацию в операционной системе (ОС) при помощи физического объекта – eToken. При этом пароль для входа в операционную систему хранится на физическом объекте, а для доступа к нему используется PIN-код на eToken. Для подключения eToken к компьютеру используется USB-порт.

Рассматриваемые утилиты и приложения:

– утилита управления eToken – позволяет устанавливать качество PIN-кода к нему;

– eToken Network Logon – позволяет использовать eToken для хранения аутентификационных данных для входа в ОС.

Ход работы

1. Базовые действия с eToken

Запустите виртуальную ОС и войдите под учётной записью «Администратор». Подключите eToken к USB-порту. Запустите утилиту «eToken Properties»: «Пуск – Программы – eToken – eToken Properties» (или через значок «eToken PKI Client» на панели уведомлений). Вид основного окна представлен на рис. 1.

Рисунок 1 – Вид основного окна утилиты «eToken Properties»

Смените PIN-код. Используемый по умолчанию PIN-код: «1234567890». При смене PIN-кода необходимо соблюдать требования, предъявляемые к его качеству. Достижение отметки 100% означает, что введённый PIN-код отвечает установленным требованиям (рис. 2).

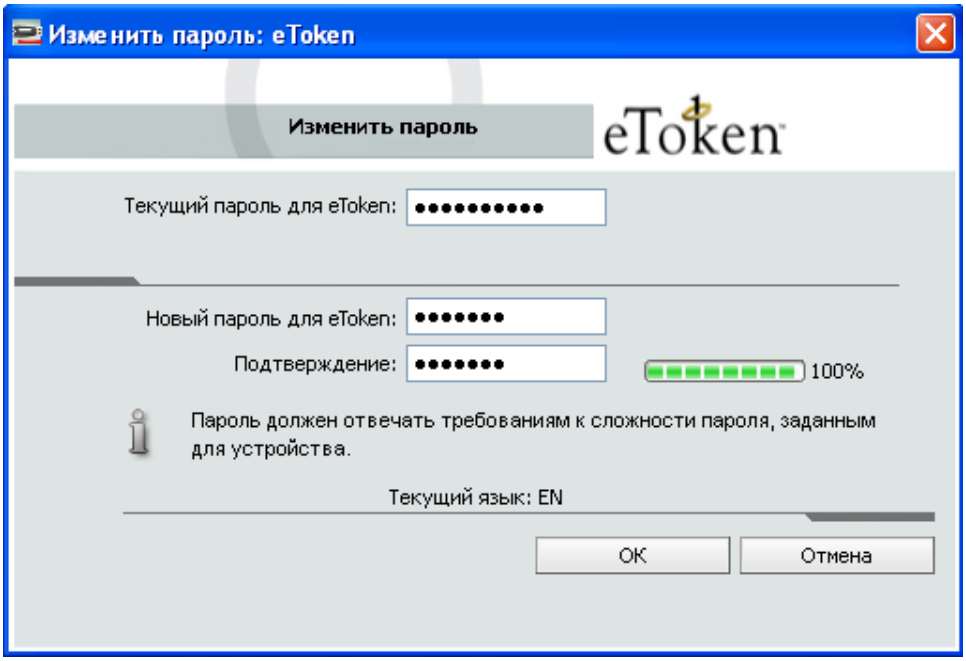


Рисунок 2 – Смена PIN-кода

Переименуйте eToken (рис. 3). Для возможности простого определения принадлежности eToken необходимо присвоить ему уникальный в системе идентификатор пользователя (login), которому выдаётся eToken. При первой операции с eToken необходимо ввести PIN-код.

Измените режим интерфейса на «Подробный вид» (значок на панели инструментов). В данном режиме предоставляется доступ к дополнительным настройкам и функциям по работе с подключенными eToken (рис. 4). В основном окне режима «Подробный вид» предоставляется информация о выбранном eToken.

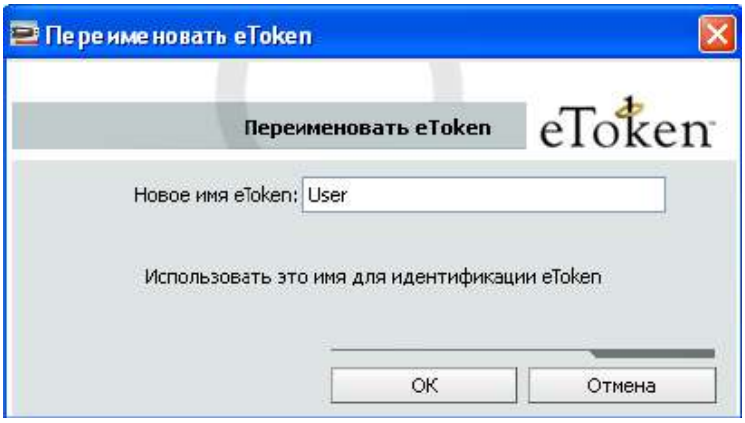


Рисунок 3 – Переименование eToken

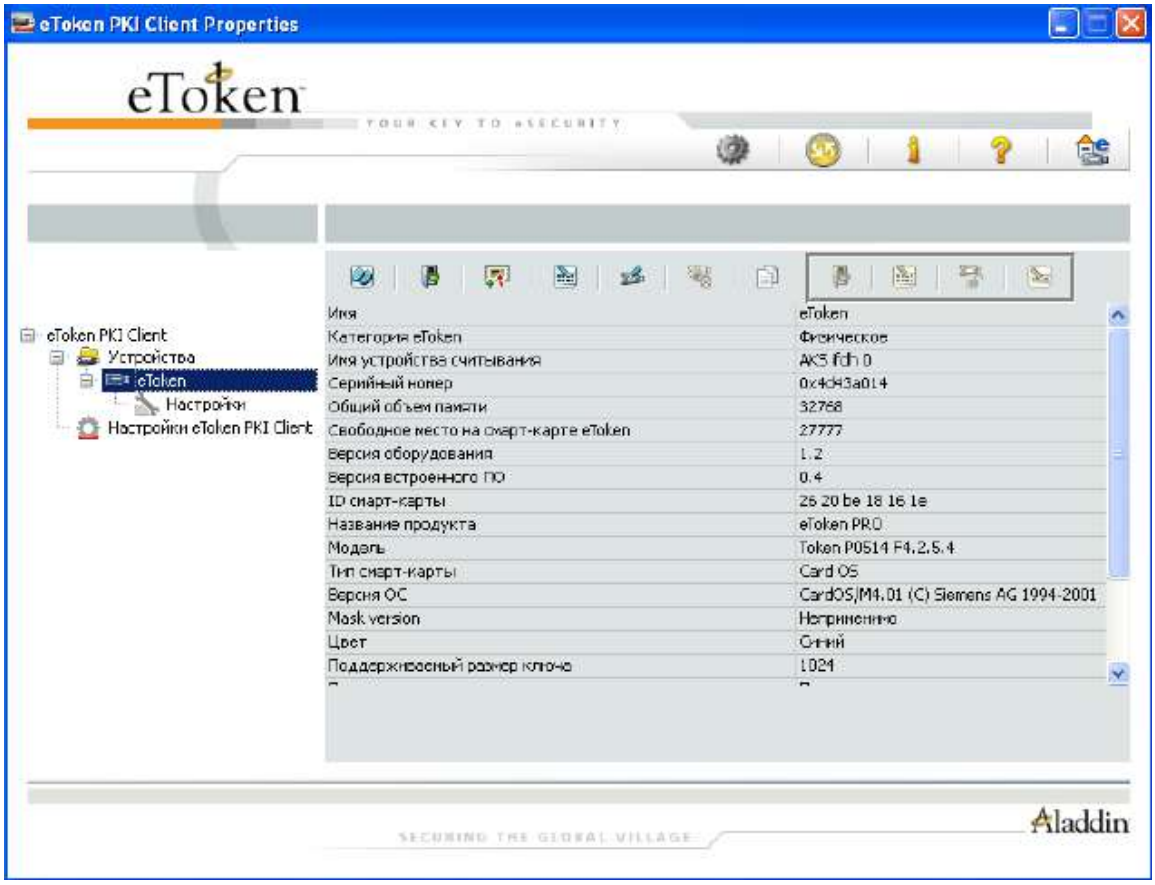


Рисунок 4 – Вид основного окна для eToken в режиме «Подробный вид»

2. Установка требований к качеству PIN-кода eToken

В разделе «Настройки eToken PKI Client» возможна установка требований к качеству PIN-кода eToken, которые будут записаны на него при форматировании (рис. 5). Просмотр требований, сохранённых на eToken, возможен в разделе «Настройки» выбранного eToken.

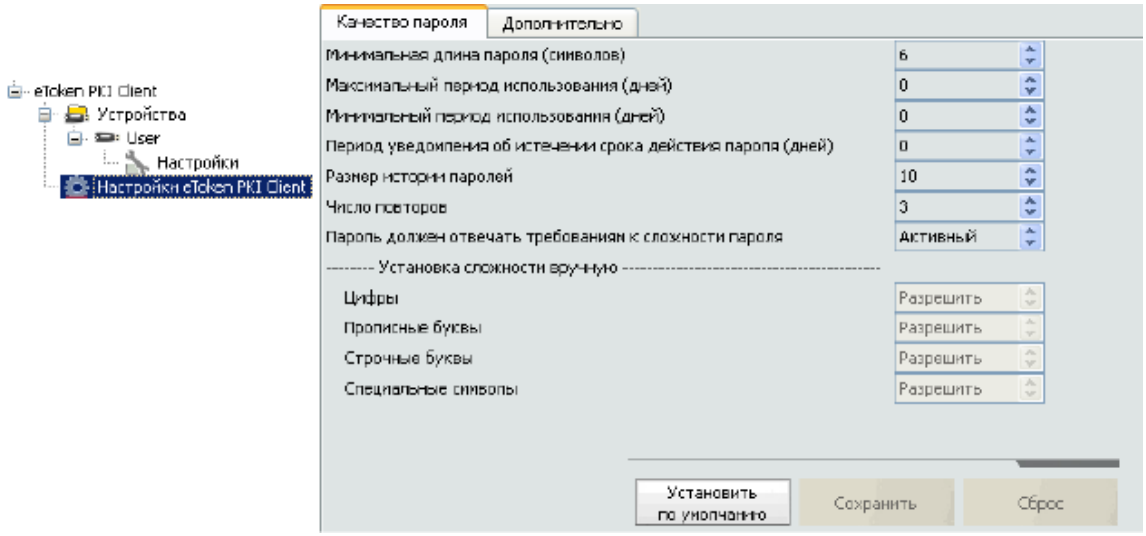


Рисунок 5 – Настройка параметров качества PIN-кода eToken

3. Администрирование eToken

В режиме «Подробный вид» выберите подключенный eToken и на панели инструментов выберите «Инициализировать eToken». В окне «Параметры инициализации eToken» (рис. 6) установите PIN-код eToken или требование к обязательной смене пароля при первом использовании (если оставите PIN-код по умолчанию), а также PIN-код администратора eToken. Также можно установить максимальное количество ошибок ввода соответствующих PIN-кодов и имя eToken. Отформатируйте eToken. **Внимание!** При форматировании есть возможность указать ключ форматирования («Дополнительно» – «Изменить ключ инициализации»). **Не изменяйте** настройки этой вкладки, так как при незнании ключа форматирования нельзя восстановить его в первоначальном состоянии, что приводит к неработоспособности eToken.

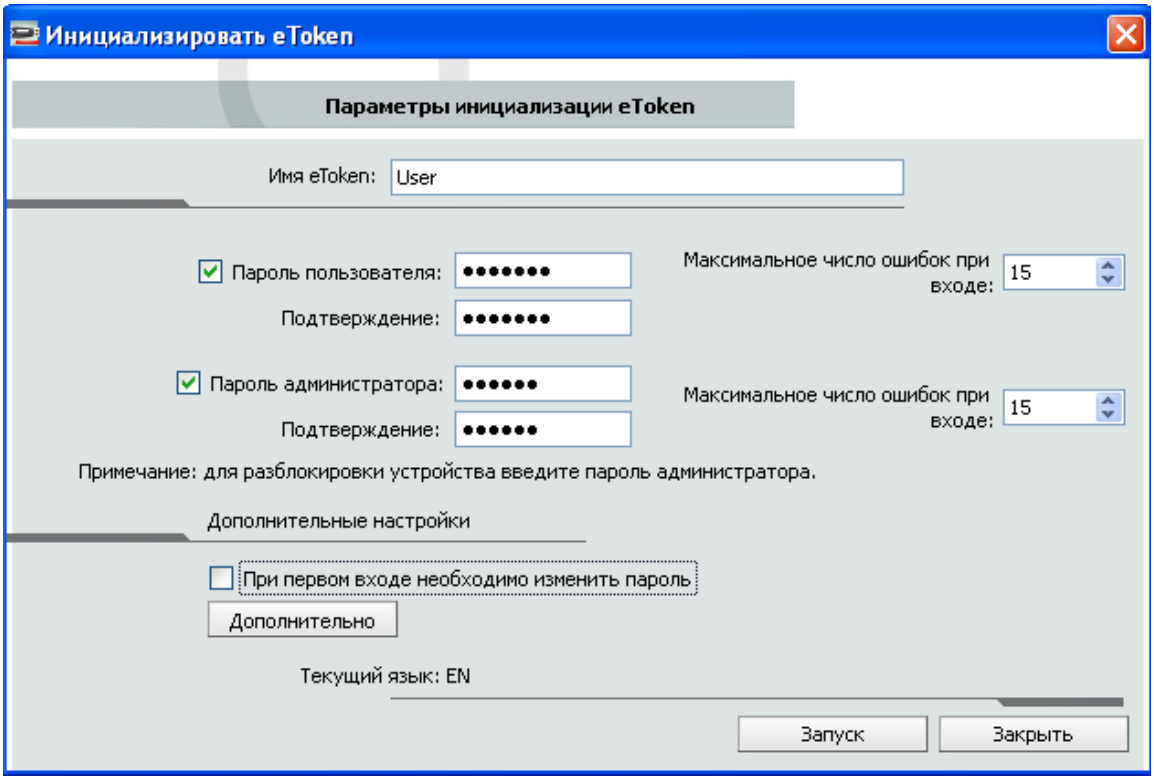


Рисунок 6 – Параметры инициализации eToken

Выберите подключенный eToken. На панели инструментов выберите значок «Вход с правами администратора». Введите PIN-код администратора (рис. 7). Администратору предоставляются дополнительные функции. На панели инструментов выберите значок «Установить пароль пользователя». Эта функция позволяет администратору задать новый PIN-код eToken, если пользователь забыл свой текущий PIN-код.

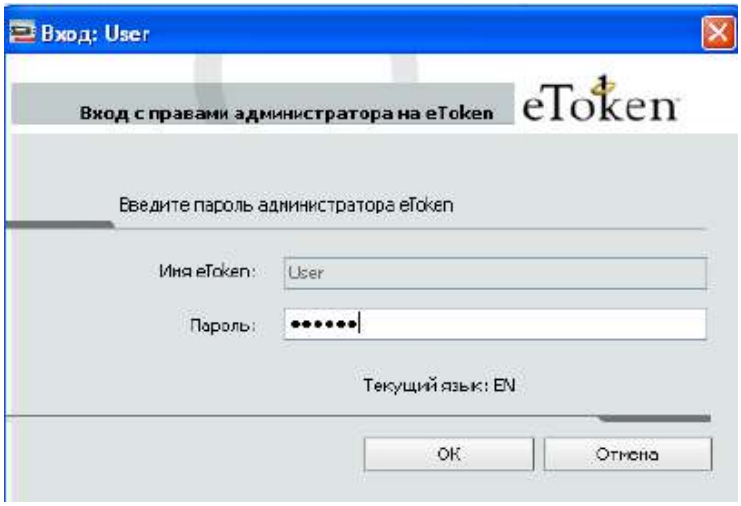


Рисунок 7 – Ввод пароля администратора

Настройки интерфейса утилиты «Свойства eToken» можно изменять через «Групповые политики», используя соответствующий административный шаблон. Откройте оснастку gpedit.msc и добавьте административный шаблон eTokenPKIClient.adm (расположен на «Рабочем столе»). В появившемся разделе «eToken PKI Client Settings» можно разрешать или запрещать доступ к любой настройке рассматриваемой утилиты. Например, запретите доступ к режиму «Подробный вид» (значение 0 настройки «OpenAdvancedView» параметра «Access Control» раздела «UI Access Control List», рис. 8). Для проверки внесённых изменений перезапустите утилиту «Свойства eToken».

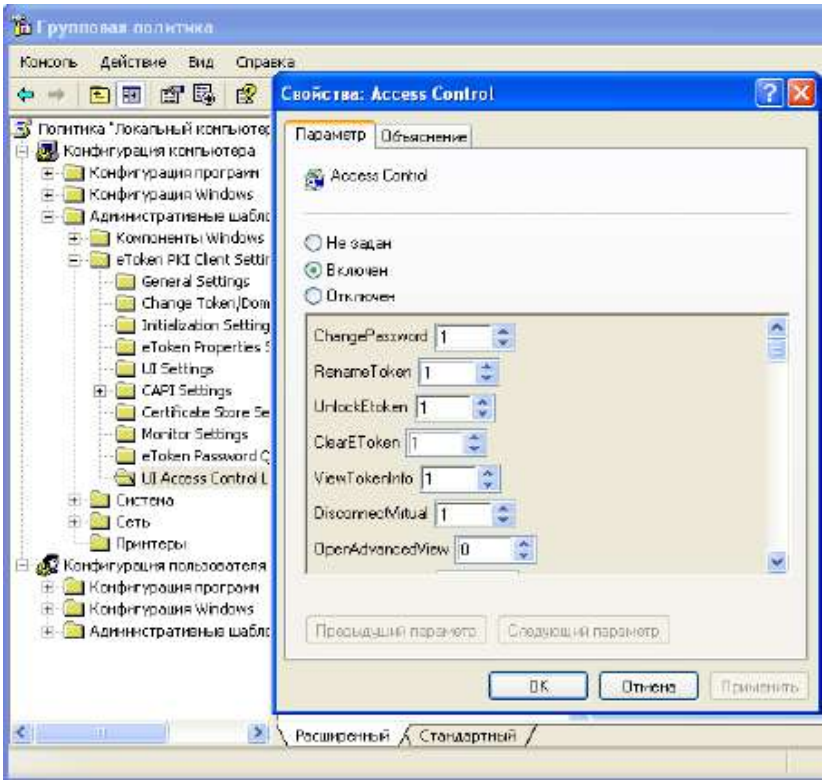


Рисунок 8 – Запрет доступа к режиму «Дополнительно»

4. Аутентификация в ОС при помощи eToken

Запустите утилиту для создания профиля входа в операционную систему: «Пуск – Программы – eToken – eToken Network Logon – eToken Network Logon Profile Wizard». Нажмите «Далее». Введите логин пользователя (например, «User») и название рабочей станции (либо домена), для которых создаётся профиль (рис. 9). Нажмите «Далее».

Рисунок 9 – Ввод информации пользователя для входа в ОС

Введите и подтвердите пароль для входа в ОС, принадлежащий выбранному пользователю (рис. 10). Дважды нажмите «Далее». Введите PIN-код eToken для подтверждения записи на него созданного профиля.

Рисунок 10 – Ввод пароля для входа в ОС

Завершите текущий сеанс пользователя и отключите eToken. При появлении «окна приветствия» Windows подключите eToken. Появится окно, изображённое на рис. 11. Введите PIN-код eToken и нажмите кнопку «OK». С eToken будет считана необходимая аутентификационная информация и произведён вход в ОС. После входа в ОС отключите eToken – в этом случае сеанс пользователя блокируется. Подключите eToken и разблокируйте сеанс.

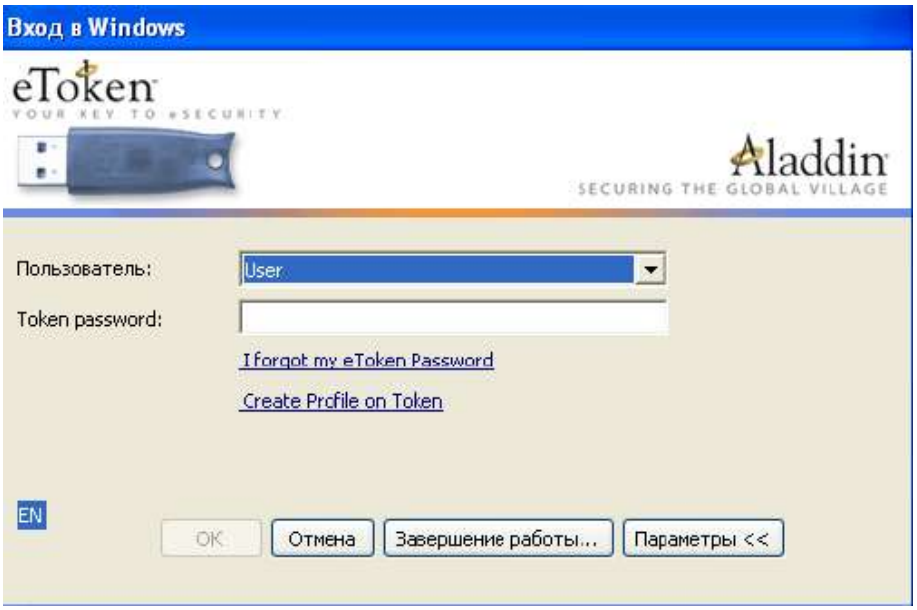


Рисунок 11 – Двухфакторная аутентификация при помощи eToken

Сменить пароль для входа в ОС можно, используя встроенные в ОС средства. Нажмите Ctrl-Alt-Del и выберите «Смена пароля…». В появившемся окне (рис. 12), кроме нового пароля и его подтверждения необходимо ввести PIN-код eToken для записи на него нового пароля.

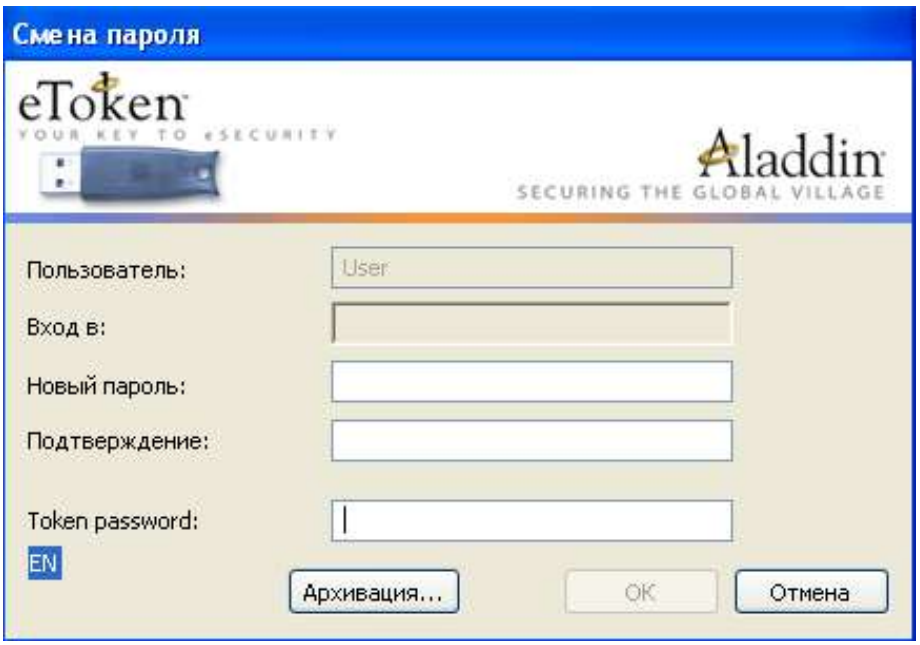


Рисунок 12 – Смена пароля для входа в ОС

Сменить пароль также можно при помощи утилиты «eToken Network Logon Profile Wizard». В окне (рис. 13) выберите существующий на eToken профиль. В окне (рис. 14) выберите создание нового пароля и включите параметр обновления пароля в хранилище ОС («Update domain password in directory»). Введите текущий и новый пароли. Если текущий пароль уже есть на eToken, то включите параметр «Read current domain password from eToken» и утилита автоматически считает его из существующего профиля.

Рисунок 13 – Выбор существующего на eToken профиля

Рисунок 14 – Смена пароля для входа в ОС

Для удаления существующего на eToken профиля нужно в окне (рис.15) выбрать «Remove an existing profile». Удалите существующий профиль.

Рисунок 15 – Выбор двухфакторной аутентификации

5. Аутентификация в ОС на основе случайного пароля

Создайте новый профиль для входа в ОС, выбрав задание случайного пароля определённой длины (рис. 16). Тогда пароль для входа в ОС будет храниться только на eToken, иметь высокую сложность, не будет известен пользователю, уменьшая возможность подбора или разглашения пароля. После создания профиля завершите сеанс пользователя. Отключите eToken. При попытке стандартного входа в ОС (через Ctrl-Alt-Del) старый пароль пользователя будет отклонён, т.к. произошла смена пароля на случайный с заданной длиной. Войдите в ОС с использованием eToken.

Рисунок 16 – Задание случайного пароля для входа в ОС

Сменить случайный пароль для входа в ОС пользователь может, выбрав «Смена пароля…» при нажатии Ctrl-Alt-Del (рис. 17). В этом случае достаточно ввести PIN-код eToken, а новый пароль для входа в ОС будет сгенерирован случайным образом. Длина случайного пароля будет задана в соответствии с настройками.

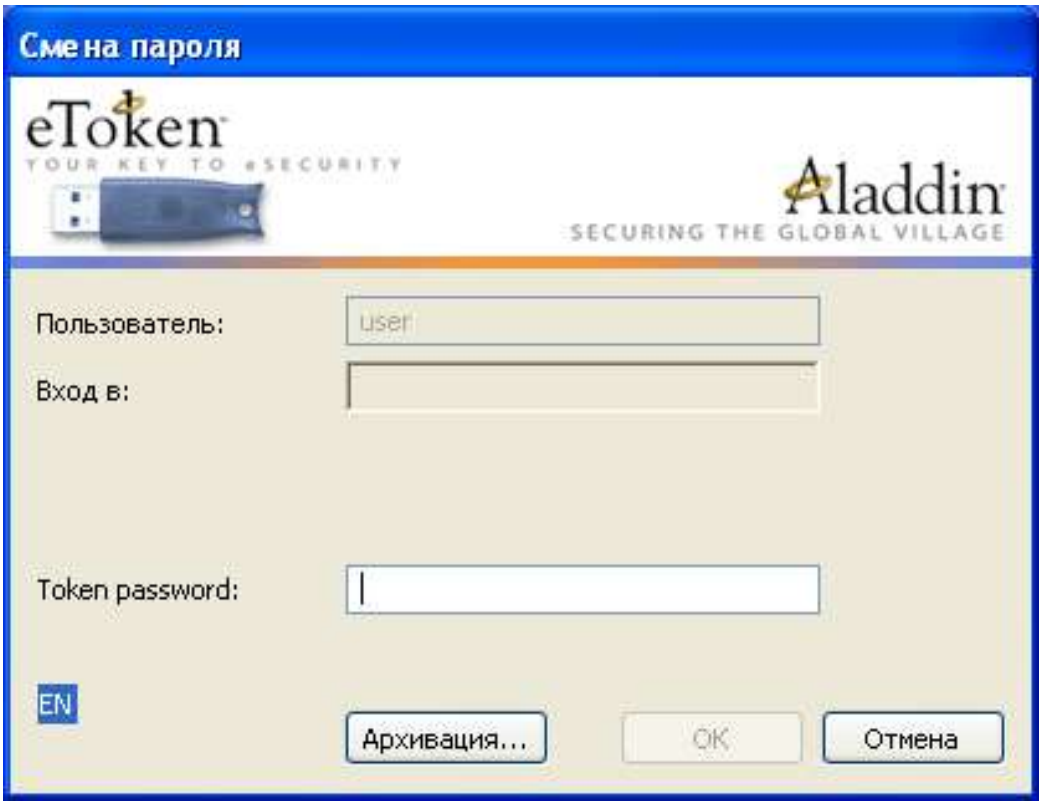


Рисунок 17 – Смена случайно заданного пароля для входа в ОС

6. Администрирование eTokenNetworkLogon

Настройки рассматриваемой утилиты можно изменять через «Групповые политики», используя соответствующий административный шаблон. Под учётной записью «Администратор» откройте gpedit.msc, добавьте административный шаблон «C:\Program Files\Aladdin\eToken\eTNLogon\eTokenNetworkLogon.adm». В разделе «eTokenNetworkLogon» можно разрешать или запрещать доступ к любой настройке, а также включать и отключать функции рассматриваемой утилиты. Например, запретите стандартный вход в ОС через Ctrl-Alt-Del (значение 0 параметра «Allow Standard Windows Logon») – будет разрешён вход только с использованием eToken (рис. 18). Завершите сеанс пользователя. Попытайтесь воспользоваться стандартным методом входа в ОС.

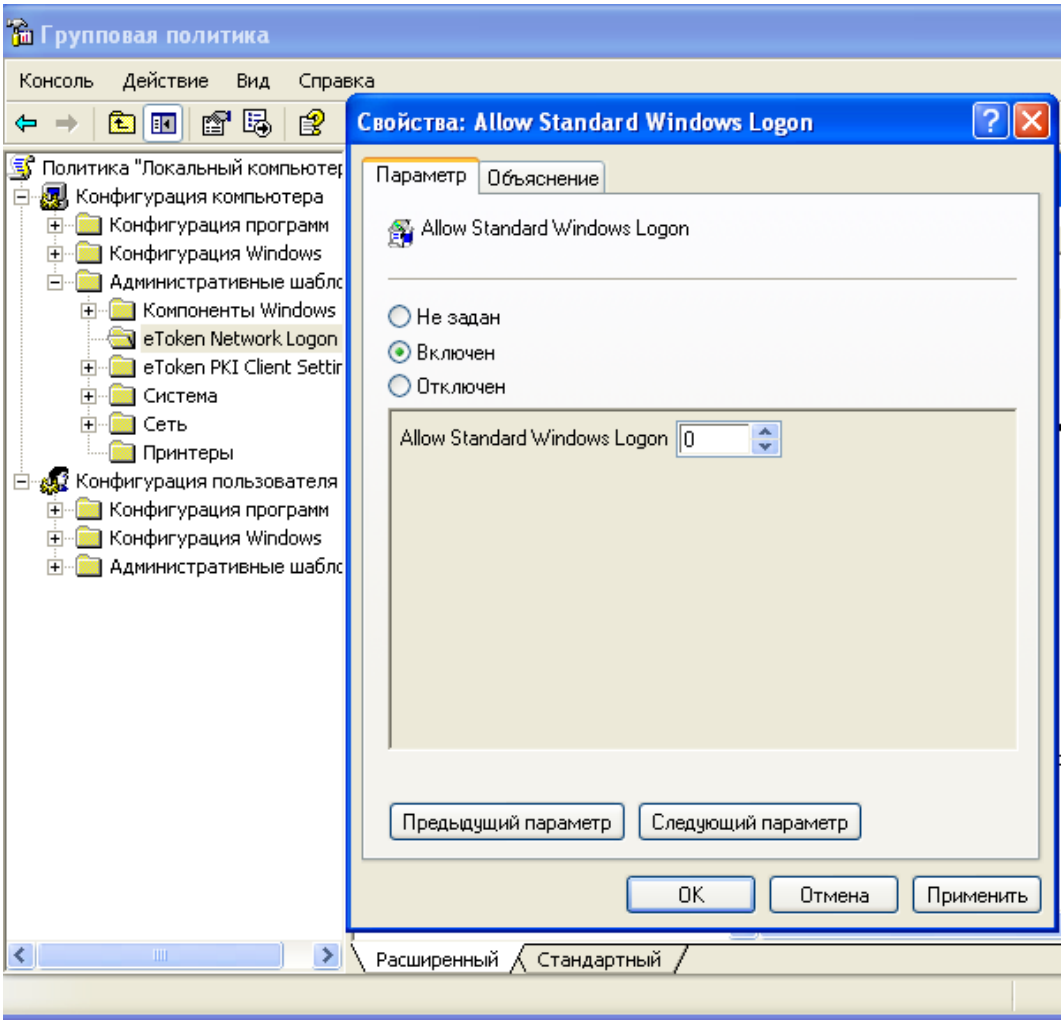


Рисунок 18 – Запрет стандартного входа в ОС

Для входа с правами администратора создайте для учётной записью «Администратор» новый профиль на eToken при помощи функции «Create profile on Token» (рис. 19).

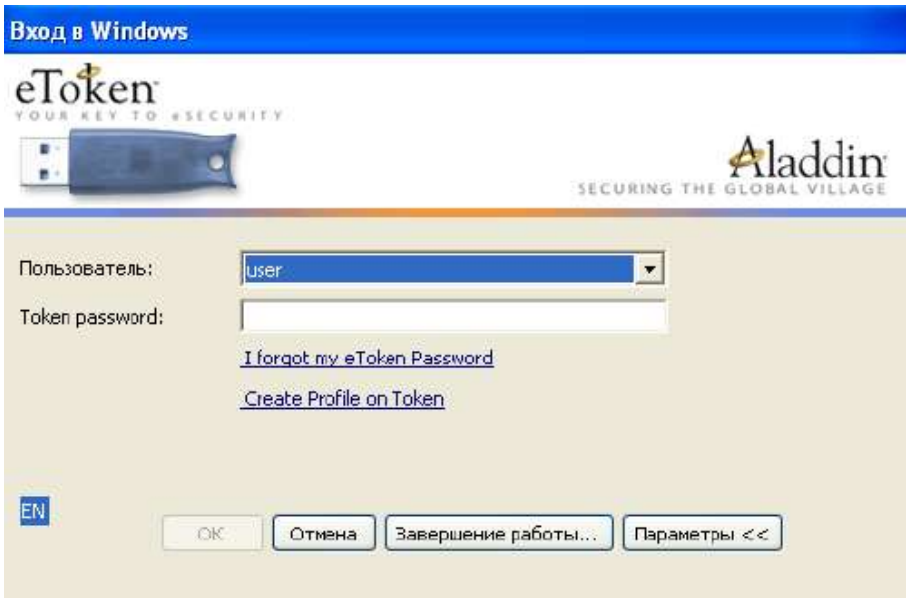


Рисунок 19 – Функции по работе с eToken, доступные до входа в ОС

Задание

1. Создайте пользователя с именем, совпадающим с Вашим именем в кафедральной сети.

2. Установите требования к качеству PIN-кода eToken в соответствии с Вашим вариантом (табл. 1).

3. Отформатируйте eToken, присвоив ему имя созданного пользователя и установив пароль, соответствующий требованиям п. 2.

4. Создайте профиль для входа в ОС созданного пользователя.

5. Продемонстрируйте преподавателю процедуру смены пароля для входа в ОС в соответствии с параметрами, указанными в Вашем варианте.

Таблица 1 – Варианты заданий

Вар.	Требования к качеству PIN-кода	Параметры входа в ОС
1	Мин. длина пароля – 8 символов. Макс. срок действия пароля – 30 дней.	Ввод нового пароля вручную. Ввод текущего пароля вручную.
2	Мин. длина пароля – 12 символов. Количество хранимых последних паролей – 5.	Ввод нового пароля вручную. Считывание текущего пароля с eToken.
3	Мин. длина пароля – 12 символов. Пароль должен содержать только буквы обоих регистров.	Ввод нового пароля вручную. Считывание текущего пароля с eToken.
4	Макс. срок действия пароля – 30 дней. Пароль должен содержать все типы символов.	Генерация случайного нового пароля длиной 10 символов. Ввод текущего пароля вручную.
5	Макс. срок действия пароля – 40 дней. Количество хранимых последних паролей – 8.	Генерация случайного нового пароля длиной 10 символов. Считывание текущего пароля с eToken.
6	Мин. длина пароля – 10 символов. Пароль должен содержать только буквы обоих регистров и числа.	Генерация случайного нового пароля длиной 10 символов. Ввод текущего пароля вручную.
7	Мин. длина пароля – 12 символов. Пароль может содержать все типы символов.	Генерация случайного нового пароля длиной 15 символов. Ввод текущего пароля вручную.

8	Макс. срок действия пароля – 30 дней. За сколько дней пользователь должен быть предупреждён о смене пароля – 3 дня.	Генерация случайного нового пароля длиной 15 символов. Считывание текущего пароля с eToken.
9	Количество хранимых последних паролей – 7. Пароль должен содержать только буквы обоих регистров и числа.	Изменение пароля через Ctrl-Alt-Del.
10	Количество хранимых последних паролей – 9. Пароль должен содержать все типы символов.	Изменение случайно заданного пароля через Ctrl-Alt-Del.

Контрольные вопросы

1. Какой PIN-код для eToken используется по умолчанию?
2. Каким образом можно узнать размер свободной памяти на eToken?
3. Какие дополнительные возможности предоставляются администратору eToken?
4. Какие можно установить требования к качеству PIN-кода eToken?
5. Где хранятся требования к качеству PIN-кода eToken, используемые при смене этого PIN-кода?
6. Опишите отличия двухфакторной аутентификации при использовании eToken от однофакторной.
7. Что включает профиль входа в операционную систему, создаваемый приложением eToken Network Logon?
8. С использованием каких способов может происходить смена пользователем пароля на вход в операционную систему?
9. Каким образом происходит смена пользователем случайно установленного пароля для входа в операционную систему?
10. Каким образом настраивается доступность для пользователя различных функций eToken Properties и eToken Network Logon?

ЛАБОРАТОРНАЯ РАБОТА №11

РАЗГРАНИЧЕНИЕ ДОСТУПА К УСТРОЙСТВАМ

Целью данной работы является практическое изучение принципов разграничения доступа к устройствам на основе программного продукта DeviceLock.

В данной работе рассмотрены приложения, позволяющие администратору компьютера или домена контролировать доступ пользователей к дисководам, CD/DVD – приводам, другим сменным устройствам, адаптерам WiFi и Bluetooth, а также к USB, FireWire, инфракрасным, COM и LPT-портам.

Контроль доступа может выполняться на двух уровнях: уровне интерфейса (порта) и уровне типа (съёмное устройство, принтеры, жёсткие диски и т.д). Некоторые устройства проверяются на обоих уровнях, в то время как другие – только на одном: либо на уровне интерфейса (порта), либо на уровне типа.

DeviceLock состоит из трёх частей:

– агента (DeviceLock Service). Агент устанавливается на каждый компьютер, автоматически запускается и обеспечивает защиту устройств на компьютере-клиенте;

– сервера (DeviceLock Enterprise Server). Это дополнительный необязательный компонент, используемый для централизованного сбора и хранения данных теневого копирования и журналов аудита;

– консоли управления. Это интерфейс контроля, который системный администратор использует для удалённого управления любой системой, на которой установлен агент.

Рассматриваемые утилиты и приложения:

– консоль управления DeviceLock Management Console. С её помощью можно просматривать и изменять разрешения и правила аудита, устанавливать DeviceLock Service, а также просматривать журналы аудита и теневого копирования для отдельных компьютеров.

Ход работы

1. Настройка DeviceLock Management Console

Войдите под учётной записью «Администратор». Запустите «DeviceLock Management Console»: «Пуск – Программы – DeviceLock» (рис. 1). Доступ к консоли можно также получить через «MMC», добавив оснастку «DeviceLock Management Console».

Подключите консоль «DeviceLock Management Console» к управляемому компьютеру. Для этого в контекстном меню «Сервис DeviceLock» выберите «Подключиться…» (рис. 2). Дополнительно включите настройку «Подключаться к локальному компьютеру при запуске» для автоматического подключения сервиса.

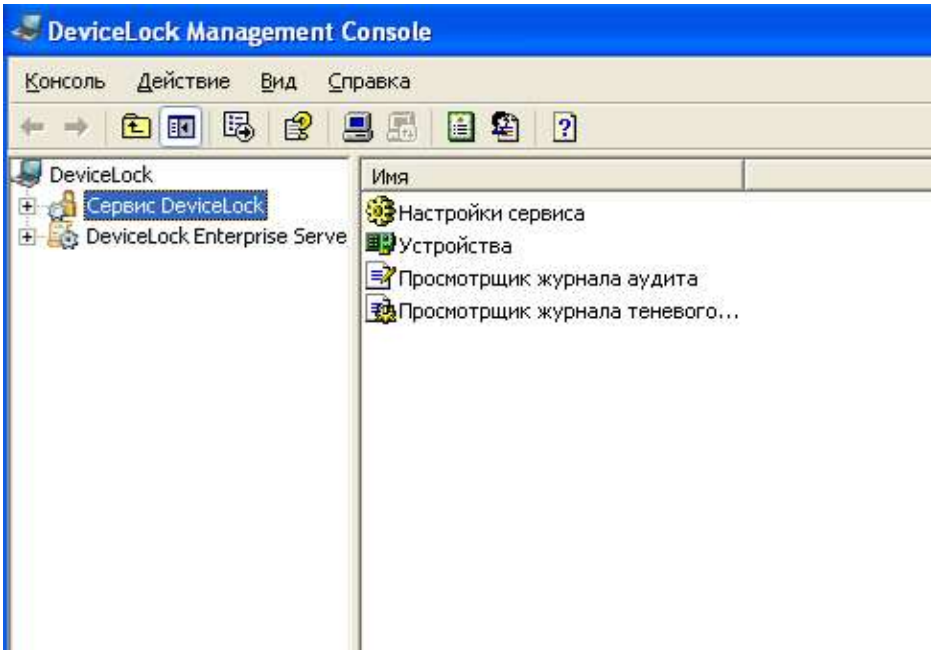


Рисунок 1 – «DeviceLock Management Console»

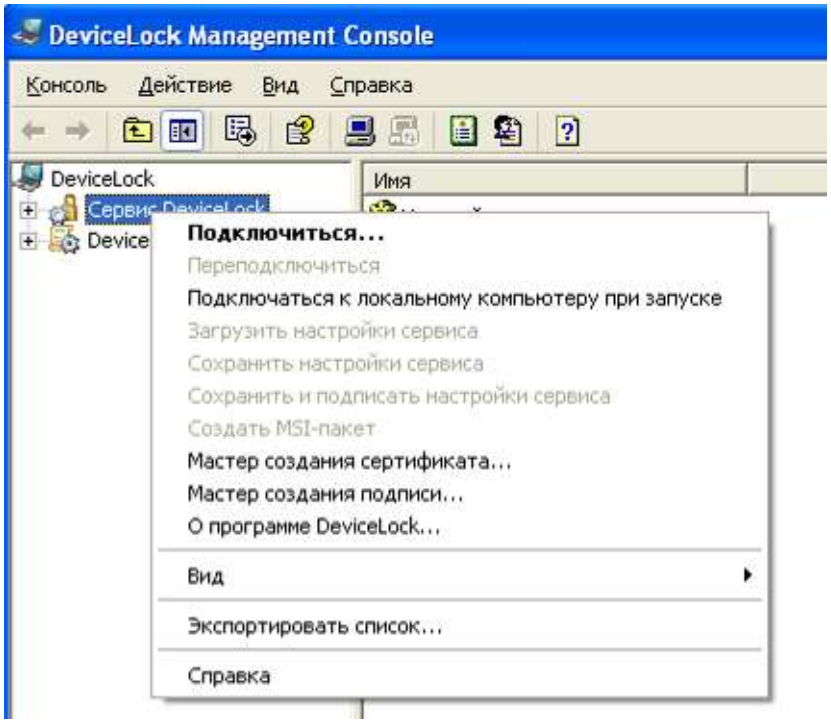


Рисунок 2 – Подключение консоли DeviceLock

Перейдите во вкладку «Настройка сервиса – Администраторы DeviceLock». Добавьте в качестве администратора DeviceLock учётную запись «Администратор» (рис. 3). В данной вкладке можно добавить и других пользователей с возможностью ограничения доступа к оснастке (полный доступ, изменение, только чтение). Пользователи, не внесённые в список, не будут иметь доступ к оснастке управления разграничением доступа к устройствам.

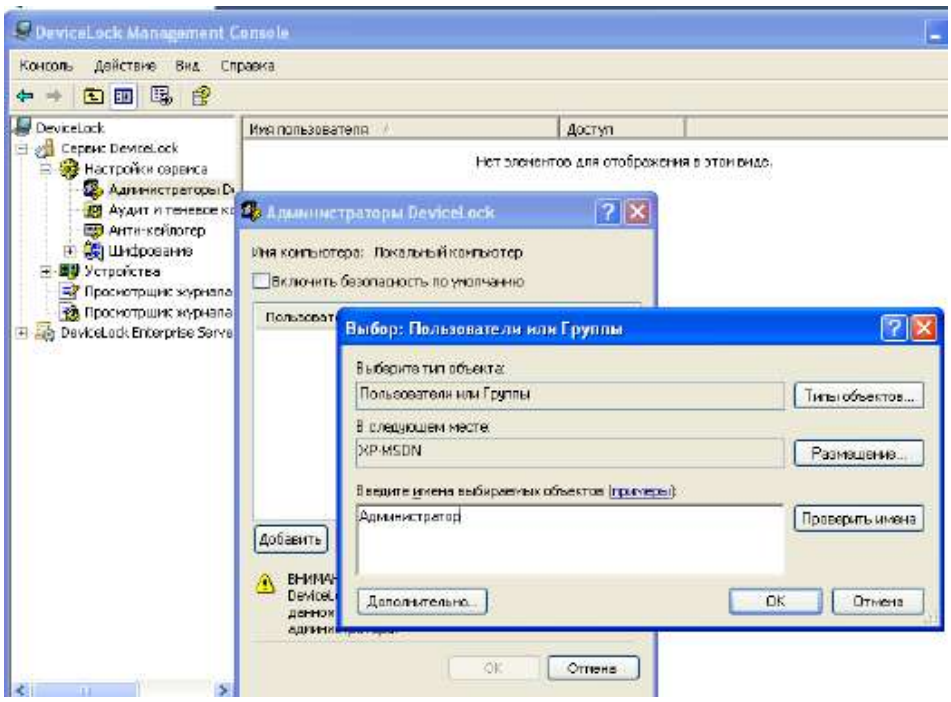


Рисунок 3 – Добавление администратора DeviceLock

2. Разграничение доступа к устройствам

Когда пользователь пытается получить доступ к устройству, DeviceLock перехватывает запрос на уровне ядра ОС. В зависимости от типа устройства и интерфейса подключения (например, USB), DeviceLock проверяет права пользователя в соответствующем списке управления доступом (ACL). Если у пользователя отсутствуют права доступа к данному устройству, будет возвращено сообщение об ошибке – «доступ запрещён».

Перейдите в раздел «Устройства – Разрешения» (рис. 4)

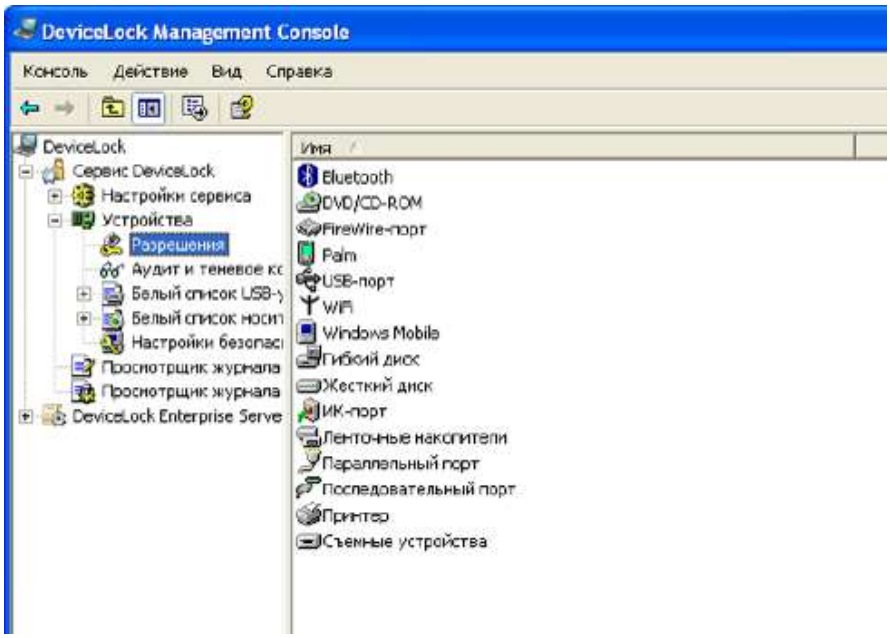


Рисунок 4 – Разрешения для устройств

Запретите доступ учётной записи «user» к приводу DVD/CD-ROM (рис. 5). Если на ПК установлено несколько CD/DVD-приводов, то можно воспользоваться белым листом устройств, для того чтобы выбрать определённый носитель.

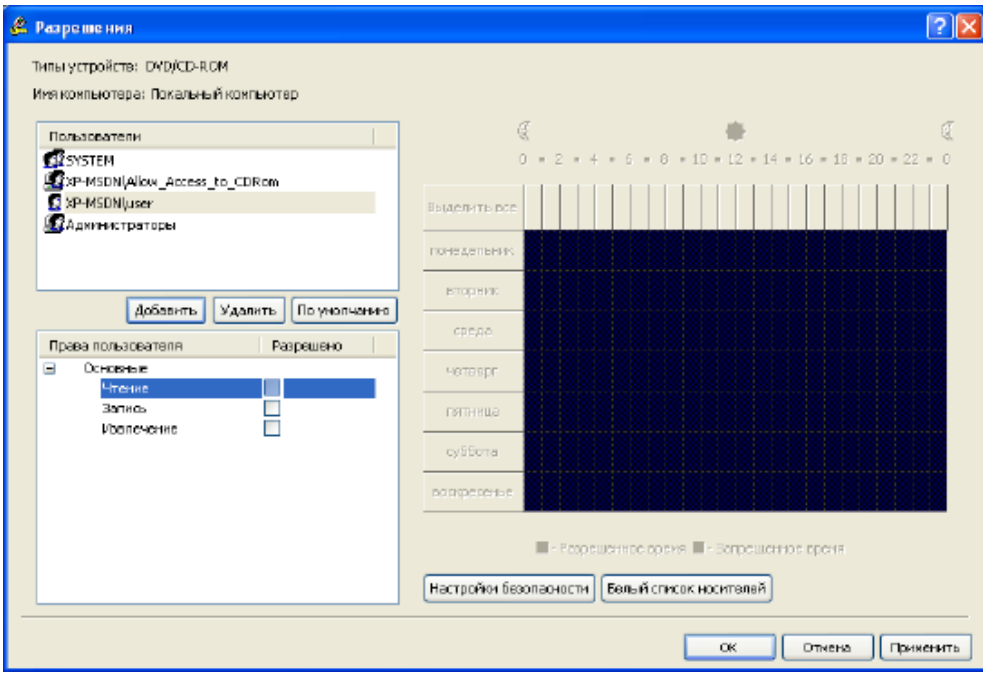


Рисунок 5 – Разрешения для DVD/CD-ROM

Войдите под учётной записью «user». Убедитесь что доступ к CD/DVD – приводу запрещен.

Под учётной записью «Администратор» разрешите пользователю «user» только чтение файлов со съёмных носителей (рис. 6).

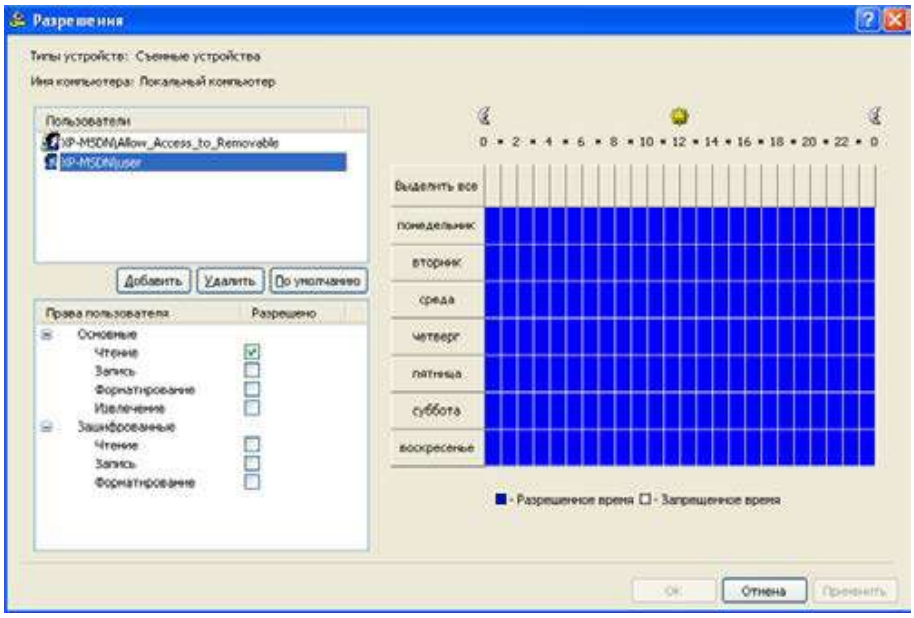


Рисунок 6 – Разрешения для съемных устройств

Примечания:

– если пользователь входит в какую-либо группу и у этой группы стоит полный доступ к устройству, то режим только чтение не будет работать (это связано с тем, что разрешения суммируются);

– если учётную запись не добавить в разрешения, то доступ ей будет запрещён.

Войдите под учётной записью «user».

Подключите съёмный носитель и убедитесь, что запись на него невозможна.

DeviceLock предоставляет возможность разграничения доступа к устройствам по дням недели и времени суток.

Войдите под учётной записью «Администратор» и установите пользователю «user» полный доступ к съёмным устройствам в будние дни с 8:00 до 17:00 либо на время занятий (рис. 7).

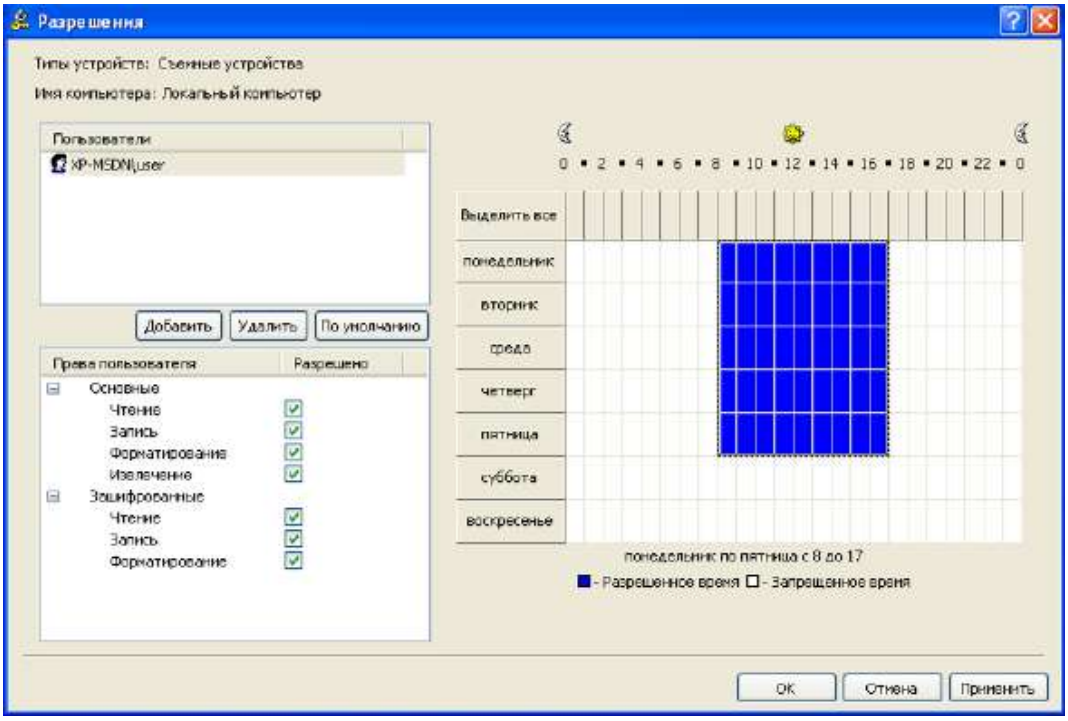


Рисунок 7 – Разграничения доступа к устройствам по дням недели и времени суток

Войдите под учётной записью «user». Подключите съёмный носитель и убедитесь, что доступ к нему разрешён.

Под учётной записью «Администратор» измените системное время на воскресенье.

Войдите под учетной записью «user» и проверьте запрет доступа к съёмному носителю.

3. Белый список устройств

Под учётной записью «Администратор» запретите доступ к USB-порту учётной записи «user» (рис. 8).

В случае с USB-устройствами DeviceLock в первую очередь проверит разрешения на уровне интерфейса (USB-порта), открыт или нет доступ к USB-порту. Затем, поскольку «Windows» определяет USB-флэш как съёмное устройство, DeviceLock также проверит ограничения на уровне типа устройства (съёмное устройство). Под учётной записью «user» проверьте запрет доступа к съёмному носителю.

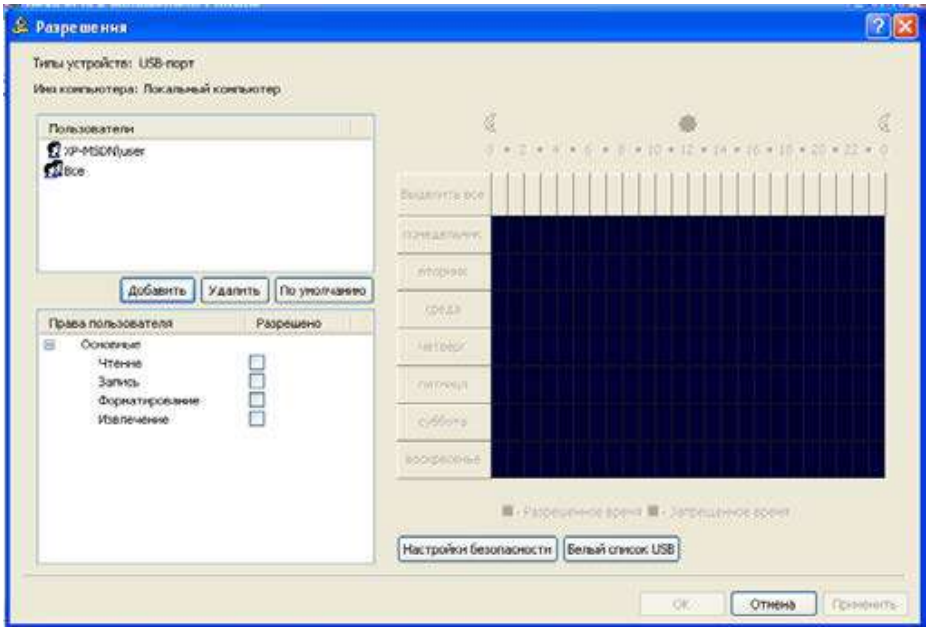


Рисунок 8 – Разрешения для USB-порта

Так как разграничению доступа подвергаются все USB-устройства, возникает необходимость делать исключения для USB-устройств, разрешённых к использованию в организации.

Исключения можно указывать двумя способами:

– через «Настройки безопасности» (рис. 9);

– через «Белый список» на основе идентификации модели или конкретного экземпляра устройства.

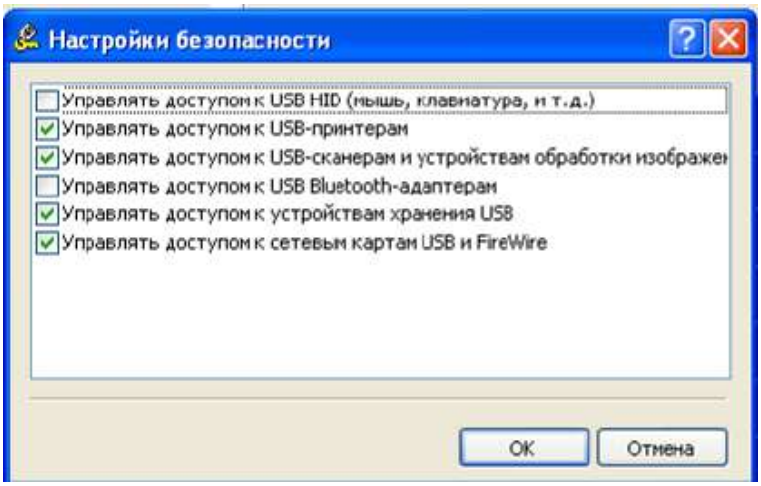


Рисунок 9 – Настройки безопасности

Если в «Настройках безопасности» включить настройки управления каким-либо классом устройств, то к устройствам этого класса применяется разграничение доступа. Если настройка отключена, то использовать устройства данного класса могут все пользователи.

При использовании белого списка есть два варианта идентификации устройств:

1) Device Model – описывает все устройства одной и той же модели. Каждое устройство идентифицируется по комбинации идентификатора производителя (VID) и продукта (PID).

Комбинация VID и PID описывает конкретную модель, но не конкретное устройство. Это значит, что все устройства данной модели данного производителя будут распознаны как одно устройство.

2) Unique Device – описывает конкретное уникальное устройство. Каждое устройство идентифицируется по комбинации идентификатора производителя (VID), продукта (PID) и серийного номера.

Устройство может быть добавлено в белый список как уникальное устройство только в том случае, если производитель присвоил ему серийный номер на этапе изготовления.

Перед тем как устройство может быть авторизовано через белый список, оно должно быть добавлено в базу данных. Перейдите во вкладку «Устройства – Белый список USB», в контекстном меню выберите «Управление». В появившемся окне (рис. 10) перейдите в «Базу данных USB-устройств».

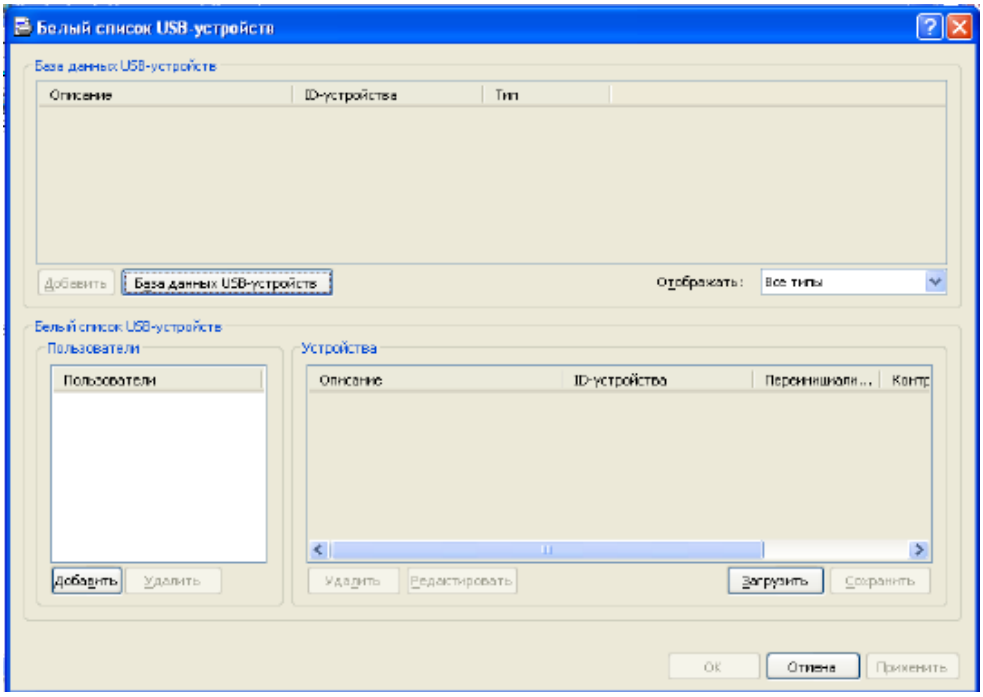


Рисунок 10 – Белый список USB-устройств

Добавьте в «Базу данных устройств» те USB-устройства, к которым необходимо разрешить доступ, выбрав устройство и нажав кнопку «Добавить» (рис. 11).

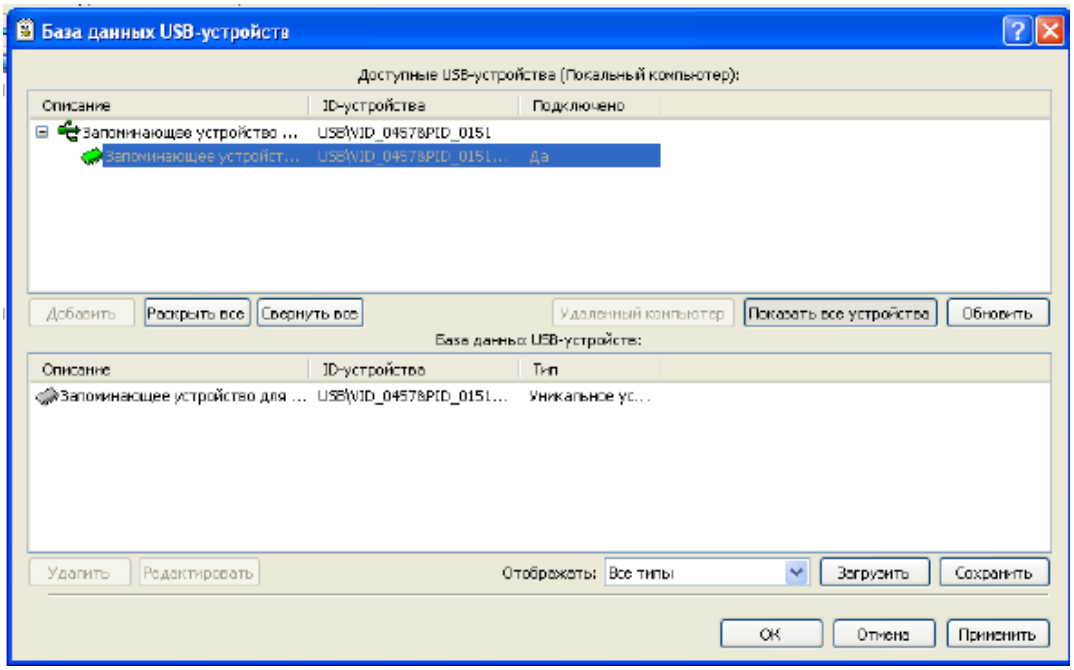


Рисунок 11 – База данных USB-устройств

Разрешите пользователю «user» доступ к USB-устройству из базы данных. Для этого добавьте учётную запись «user» и из «Базы данных USB-устройств» выберите необходимые устройства (рис. 12).

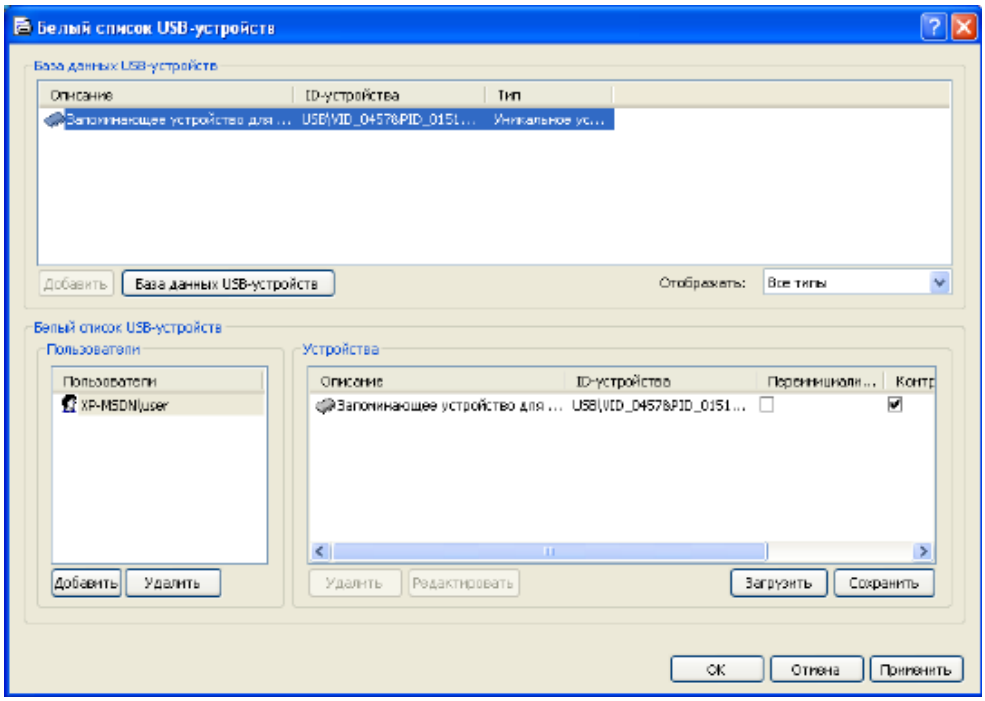


Рисунок 12 – Добавление устройства в белый список пользователя

4. Аудит использования устройств

Кроме функции контроля доступа, DeviceLock позволяет осуществлять протоколирование и аудит использования устройств пользователями на локальном компьютере.

Чтобы включить протоколирование действий пользователя, необходимо установить соответствующие права аудита.

1) Чтение/запись – протоколируются попытки пользователя читать/записывать данные. Для типов устройств «Bluetooth, FireWire-порт, ИК-порт, Параллельный порт, последовательный порт, USB-порт и WiFi».

2) Печать – протоколируются попытки пользователя посылать документы на принтеры. Применимо только к типу «Принтер».

3) Выполнение – протоколируются попытки пользователя удаленно выполнить код на стороне устройства. Применимо только к типу «Windows Mobile».

4) Чтение/запись не файлов – протоколируются попытки пользователя читать/записывать не файловые объекты (календарь, контакты, задачи и т.п.). Применимо только к типам «Windows Mobile» и «Palm».

Существует возможность протоколировать успешный доступ к устройствам и ошибки доступа:

1) «Аудит разрешений» – все попытки доступа, которые были разрешены DeviceLock, т.е. пользователю был предоставлен доступ к устройству.

2) «Аудит запретов» – все попытки доступа, которые были заблокированы DeviceLock, т.е. пользователю был запрещён доступ к устройству.

Перейдите в раздел «Устройства – Аудит и теневое копирование». Примените к съёмным устройствам аудит для пользователя «user» (рис. 13).

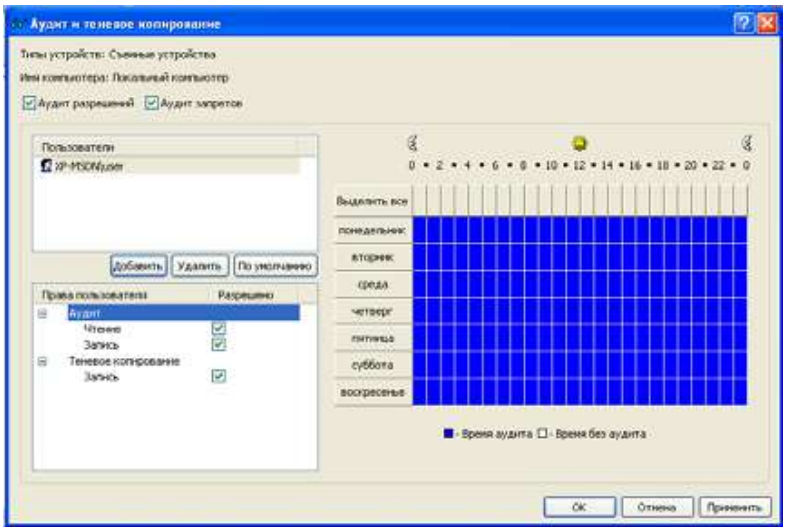


Рисунок 13 – Настройка аудита для съёмных устройств

Убедитесь, что пользователю «user» разрешён доступ к съёмным устройствам. Войдите под учётной записью «user», подключите съёмное устройство и скопируйте на него образцы рисунков «Windows» из каталога «*\Мои документы\Мои рисунки\Образцы рисунков».

Войдите под учётной записью «Администратор».

Доступ к результатам аудита можно получить во вкладке «Просмотрщик журнала аудита» (рис. 14).

Журналы аудита могут храниться как в стандартных журналах ОС «Windows», так и в журналах DeviceLock. Перейдите во вкладку «Настройка сервиса – Аудит и теневое копирование» (рис. 15).

Опция – «Тип журнала аудита» устанавливает вид журнала и может принимать три значения:

- «Журнал событий» – данные аудита записываются только в стандартный журнал «Windows», хранящийся на локальном компьютере;
- «Журнал DeviceLock» – данные аудита записываются только в собственный защищённый журнал, отсылаемый на DeviceLock Enterprise Server для централизованного хранения;
- «Журнал событий и DeviceLock» –запись в оба журнала.

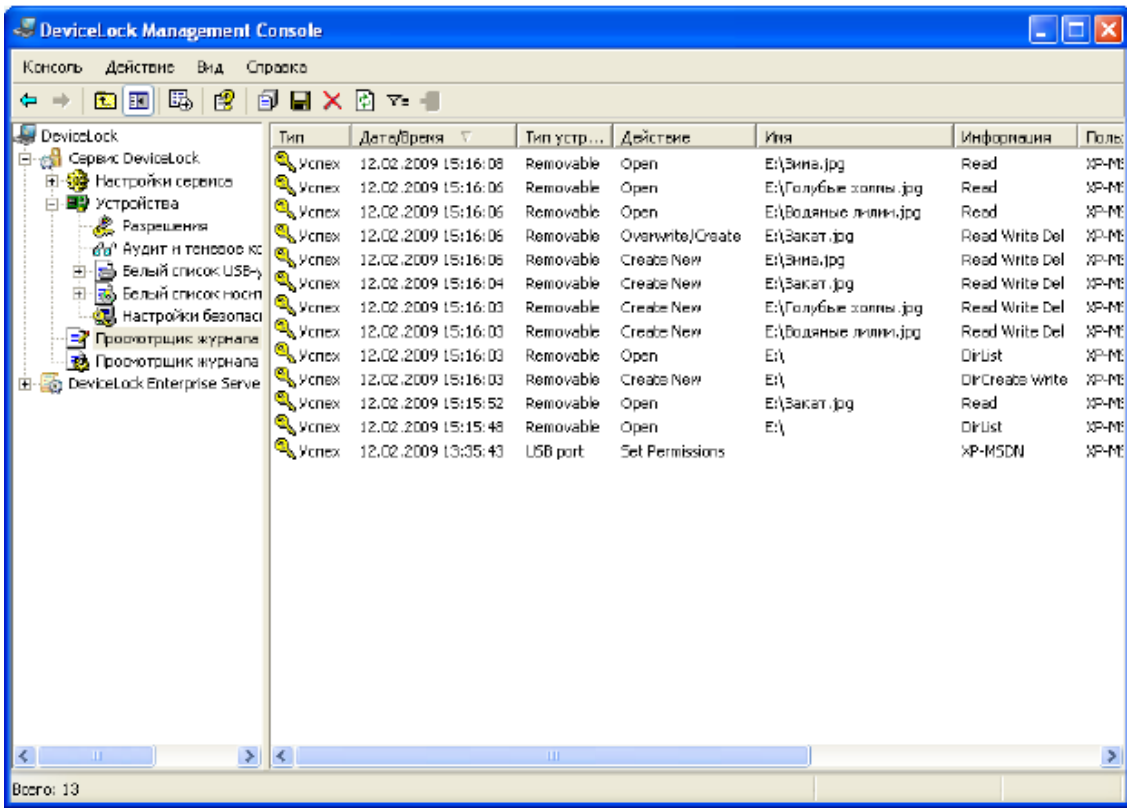


Рисунок 14 – Просмотрщик журнала аудита

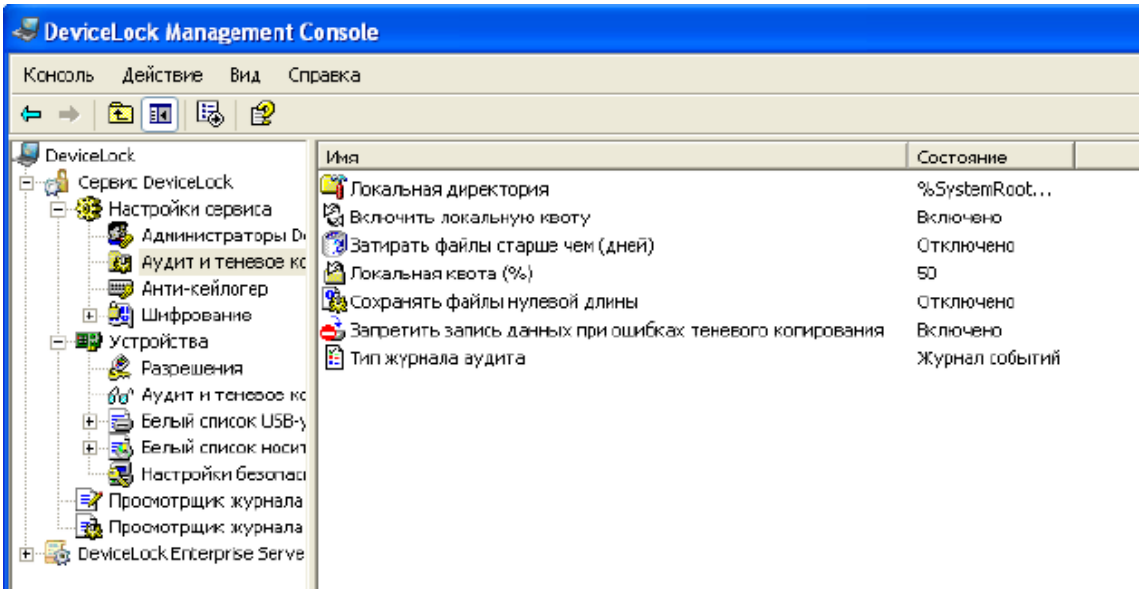


Рисунок 15 – Вкладка «Настройка сервиса – Аудит и теневое копирование»

Для того чтобы просмотреть журнал аудита через стандартный журнал «Windows», запустите консоль управления «Пуск – Выполнить – MMC». В ней добавьте оснастку «Просмотр событий». Вкладка «DeviceLock Log» предоставляет журнал аудита (рис. 16).

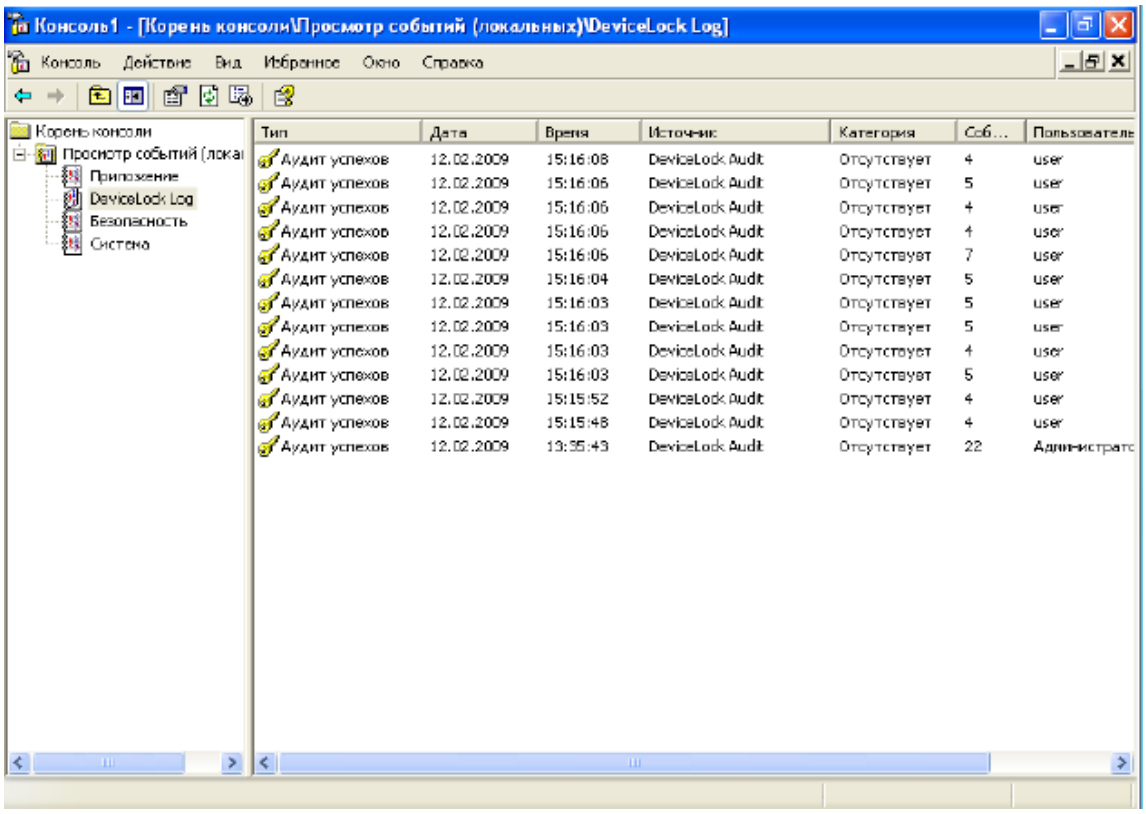


Рисунок 16 – Вкладка «Devicelock Log»

5. Теневое копирование файлов

Теневое копирование позволяет сохранять копии всех файлов, которые пользователь копирует на съёмные носители или отправляет

на печать. Сохранённые файлы могут быть в дальнейшем проанализированы на предмет наличия в них конфиденциальной информации.

Перейдите в раздел DeviceLock «Устройства – Аудит и теневое копирование». Включите для пользователя «user» теневое копирование файлов на съёмные устройства (рис. 17).

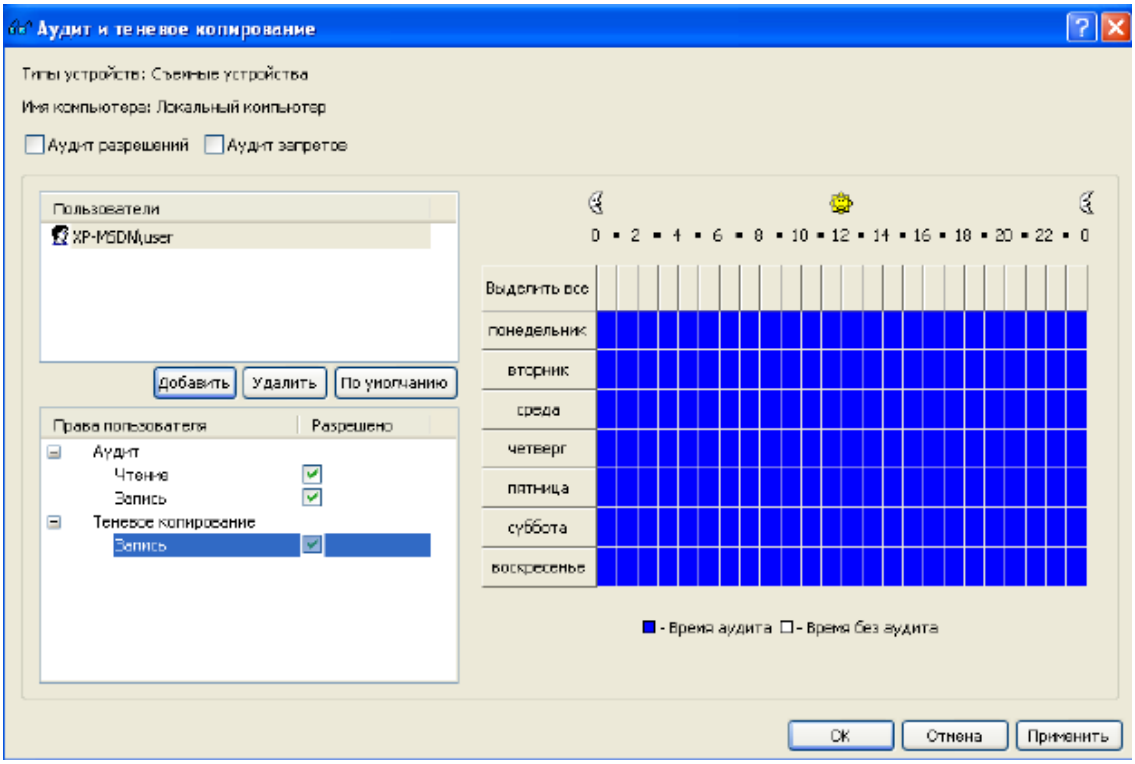


Рисунок 17 – Включение теневого копирования для съёмных устройств

Под учётной записью «user» подключите съёмное устройство и скопируйте на него текстовый или графический файл.

Под учётной записью «Администратор» откройте раздел DeviceLock «Просмотрщик журнала теневого копирования» (рис. 18).

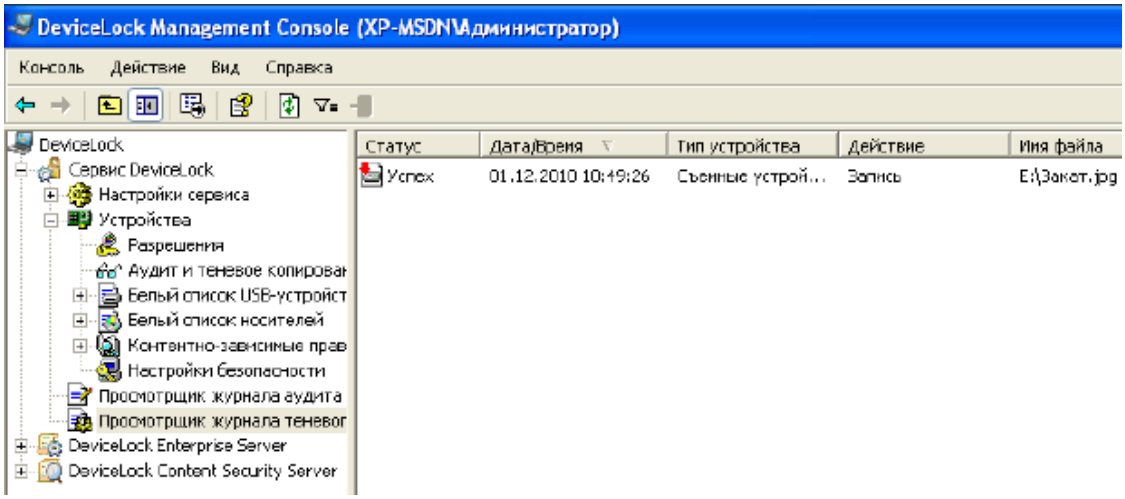


Рисунок 18 – Просмотрщик журнала теневого копирования

Откройте появившуюся в журнале запись. Это позволит увидеть содержимое файла, скопированного пользователем «user» на съёмное устройство.

Выбор места хранения теневых копий файлов возможен в разделе «Настройки сервиса – Аудит и теневое копирование – Локальная директория» (рис. 19).

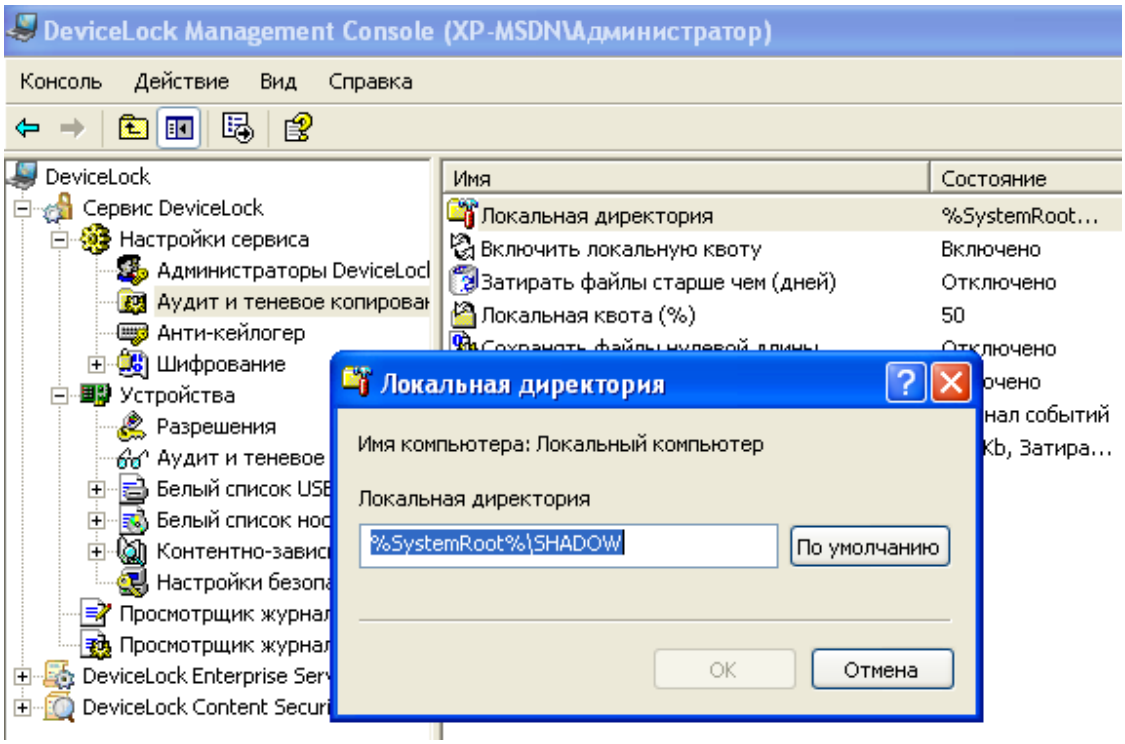


Рисунок 19 – Каталог хранения для теневого копирования

Задание

Учётной записи «user» установите разрешения в соответствии с вариантом.

Вариант 1

DVD/CD-ROM	Принтер	Жёсткий диск
Только чтение. Добавьте один носитель в белый список. Полный доступ к виртуальным приводам	Доступ по будням. Аудит печати и запретов доступа	Полный доступ. Аудит чтения и записи

Вариант 2

Съёмные устройства	USB-порт	WIFI
Чтение и извлечение	Аудит всех событий	Доступ по будням

Вариант 3

Съёмные устройства	USB-порт	DVD/CD-ROM
Чтение и извлечение	Запрет доступа к сканерам, принтерам, устройствам хранения usb. Добавьте 3 устройства в белый список	Доступ только по будням с 17 до 19 часов. Аудит записи и разрешений

Вариант 4

WindowsMobile	Съёмные устройства	USB-порт
Только чтение. Аудит всех событий	Запрет доступа вне рабочего времени	Только чтение. Добавить в белый список 2 устройства

Вариант 5

Параллельный порт	Жёсткий диск	Съёмные устройства
Запрет доступа.	Доступ по будням с 8 до 20 часов.	Чтение и извлечение. Аудит всех событий.

Вариант 6

DVD/CD-ROM	WindowsMobile	Съёмные устройства
Только чтение. Аудит всех событий.	Доступ без ограничений. Аудит всех событий.	Чтение и извлечение. Аудит всех событий вне рабочего времени.

Вариант 7

Последовательный порт	USB-порт	Принтер
Запрет доступа вне рабочего времени. Доступ к модемам, подключаемым через данный порт, без ограничений.	Запрет доступа. Добавить 4 устройства в белый список.	Доступ с 8 до 18 часов. Аудит всех событий.

Вариант 8

Bluetooth	Параллельный порт	WindowsMobile
Доступ без ограничений.	Доступ по будням.	Доступ без ограничений. Аудит записи.

Вариант 9

DVD/CD-ROM	USB-порт	Жёсткий диск
Только чтение.	Чтение, извлечение. Добавить в белый список 3 устройства.	Аудит всех событий.

Вариант 10

FireWire-порт	WIFI	Съёмные устройства
Только чтение. Аудит записи и запретов.	Доступ в рабочее время. Аудит чтения и записи.	Запрет доступа. Аудит запретов.

Контрольные вопросы

1. Существует ли возможность разграничения доступа к управлению приложением DeviceLock?
2. В чём отличие уровня интерфейса от уровня типа устройств?
3. Какие функции разграничения доступа к ресурсам предоставляет DeviceLock?
4. Каким образом можно исключить классы USB-устройств (например, мыши, клавиатуры и т.п.) из механизма разграничения доступа?
5. Для чего используются белые списки?
6. К каким классам устройств могут быть созданы белые списки?
7. Какие варианты идентификации устройства применяются в белом списке?
8. Для чего используется база данных устройств?
9. Где могут храниться журналы аудита работы с устройствами?
10. Для чего используется теневое копирование файлов?

ЛАБОРАТОРНАЯ РАБОТА № 12

МАНДАТНЫЙ МЕХАНИЗМ РАЗГРАНИЧЕНИЯ ДОСТУПА К ФАЙЛОВЫМ ОБЪЕКТАМ

Целью данной работы является практическое изучение мандатного механизма разграничения доступа на основе программного продукта Secret Net 5.1 (автономный вариант).

Ход работы

1. Настройка категорий конфиденциальности

Доступ пользователя к информации, содержащейся в конфиденциальном файле, осуществляется при условии, если пользователю назначен соответствующий уровень допуска. Набор уровней допуска, применяемых в системе, совпадает с набором категорий конфиденциальности ресурсов.

Запустите «Локальные параметры безопасности» под учетной записью «Администратор»: «Пуск – Все программы – Secret Net 5 – Локальная политика безопасности», перейдите в группу «Параметры Secret Net 5 Настройка подсистем – настройка подсистем».

Параметр «Полномочное управление доступом: название уровней конфиденциальности» настройте, как показано на рис. 1.

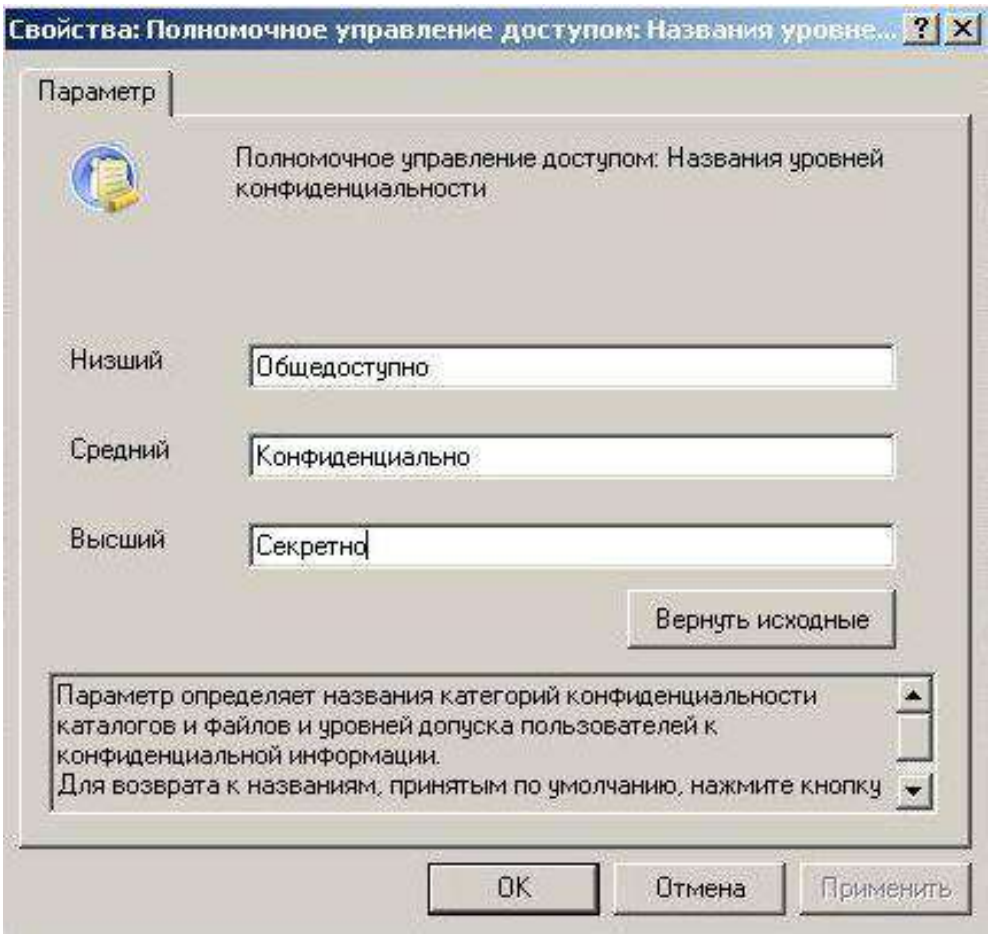


Рисунок 1 – Параметр «Название уровней конфиденциальности»

2. Настройка субъектов доступа

Запустите «Управление компьютером» под учётной записью «Администратор»: «Пуск – Все программы – Secret Net 5 – Управление компьютером», перейдите в группу «Локальные пользователи и группы – Пользователи».

Далее настройте права администратора. Для этого в свойствах учётной записи «Администратор» перейдите на вкладку Secret Net 5. В группе «Доступ» установите следующие значения (рис. 2).

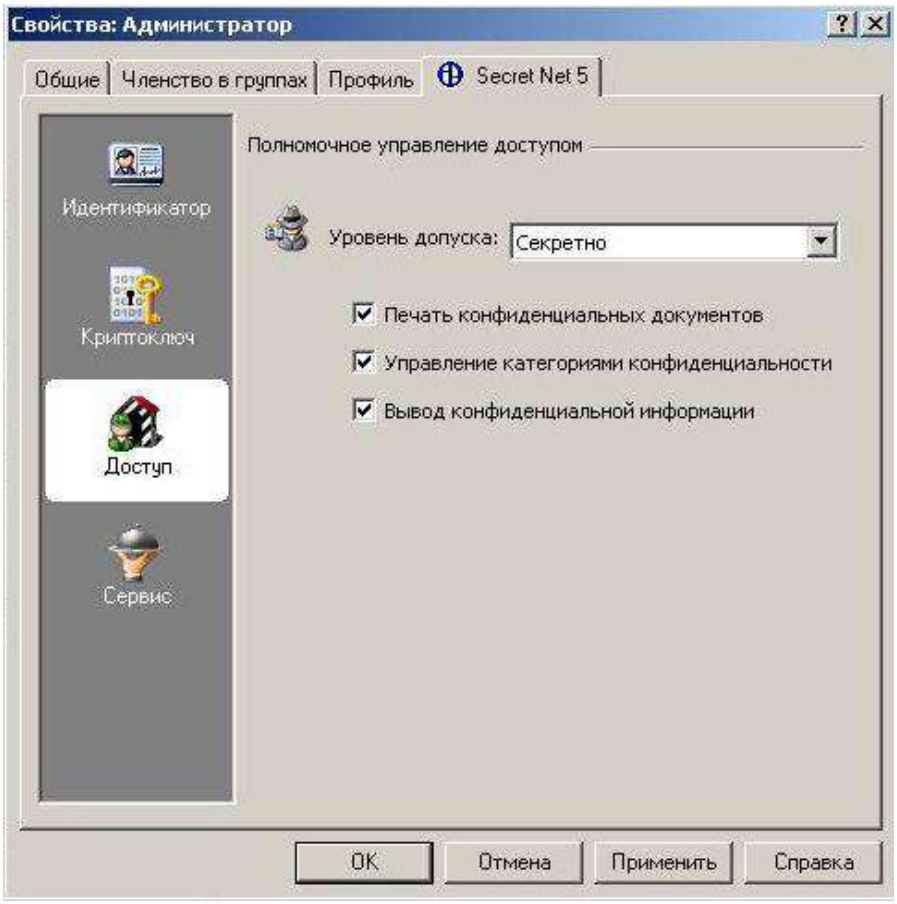


Рисунок 2 – Настройка прав доступа пользователя «Администратор»

– Управление категориями конфиденциальности – пользователь может изменять категории конфиденциальности каталогов и файлов в рамках своего уровня допуска; управлять режимом наследования категорий конфиденциальности каталогов.

– Печать конфиденциальных документов – используется для разрешения пользователю выводить на принтер конфиденциальные документы. Привилегия применяется при включенном режиме контроля печати конфиденциальных документов.

– Вывод конфиденциальной информации – пользователю разрешается выводить конфиденциальную информацию на внешние носители.

После чего вернитесь в оснастку «Локальные пользователи и группы – Пользователи». Создайте пользователя, выбрав «Новый пользователь» в контекстном меню или в меню «Действие». Настройте учётную запись как показано на рис. 3 и нажмите кнопку «Создать».

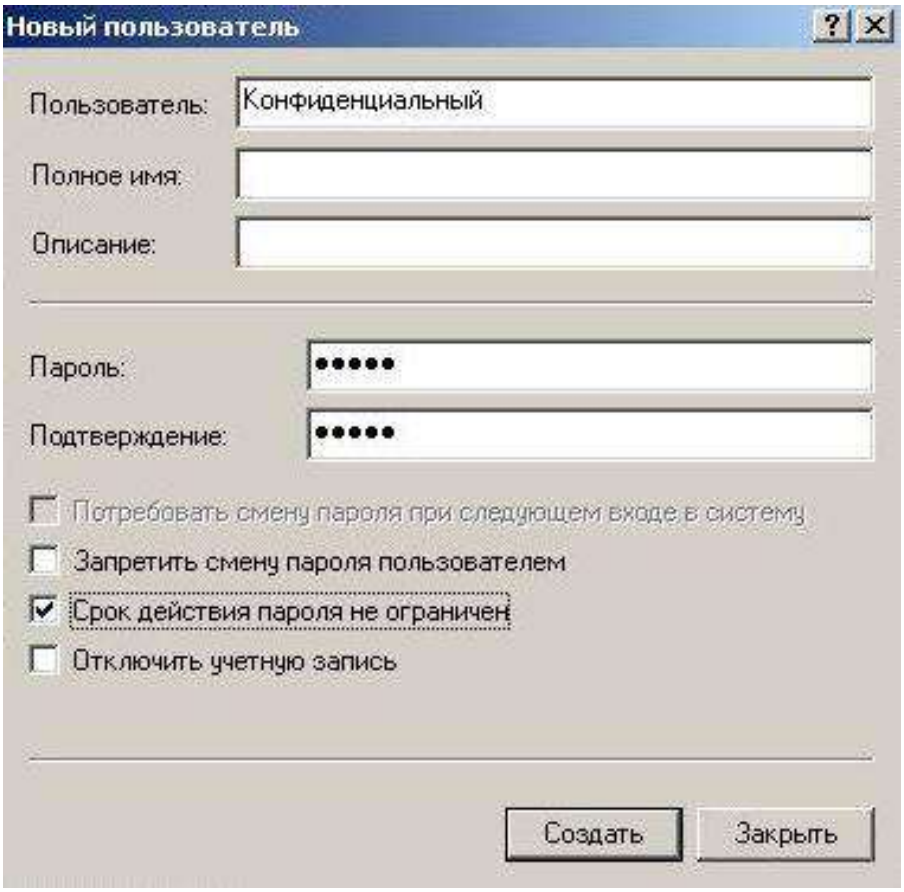


Рисунок 3 – Создание пользователя

По аналогии создайте пользователя «Секретный».

Для настройки прав доступа перейдите в группу «Пользователи», выделите пользователя «Конфиденциальный». В контекстном меню выберите «Свойства». В группе «Доступ» настройте параметры как показано на рис. 4, предоставив право вывода информации на внешние носители и печать конфиденциальных документов.

Для пользователя «Секретный» выберите уровень допуска «Секретно», запретив вывод на внешние носители и печать конфиденциальных документов (рис. 5).

Для применения настроек завершите сеанс и повторно войдите под учётной записью «Администратор».

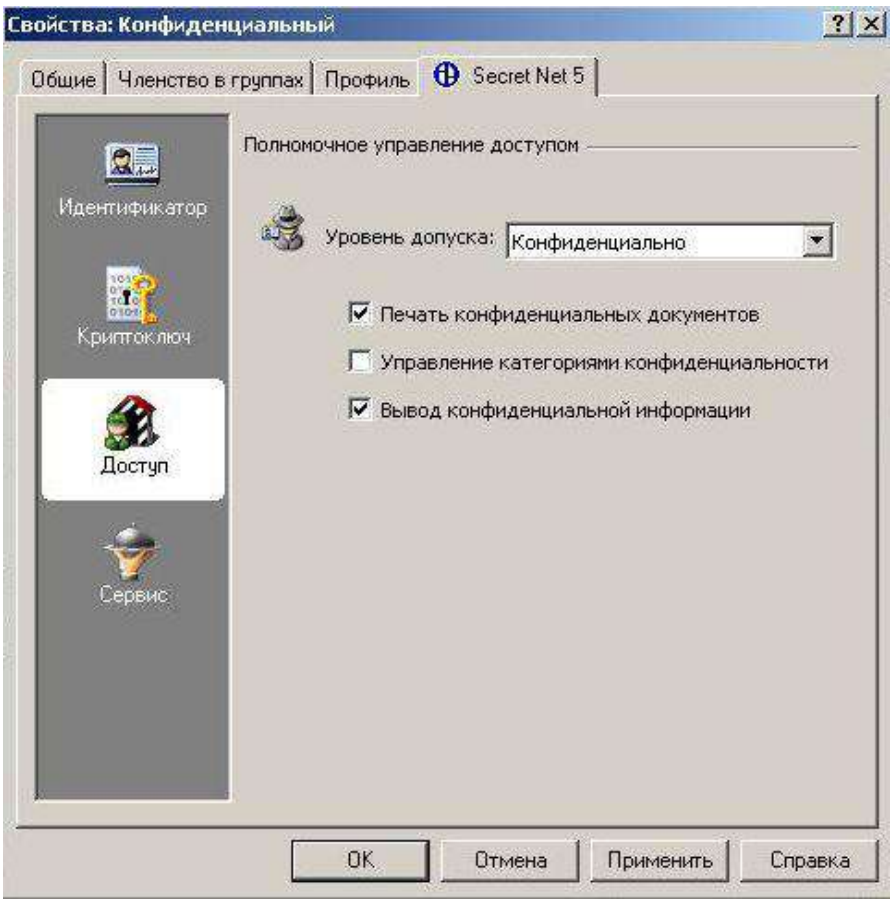


Рисунок 4 – Настройка прав доступа пользователя «Конфиденциальный»

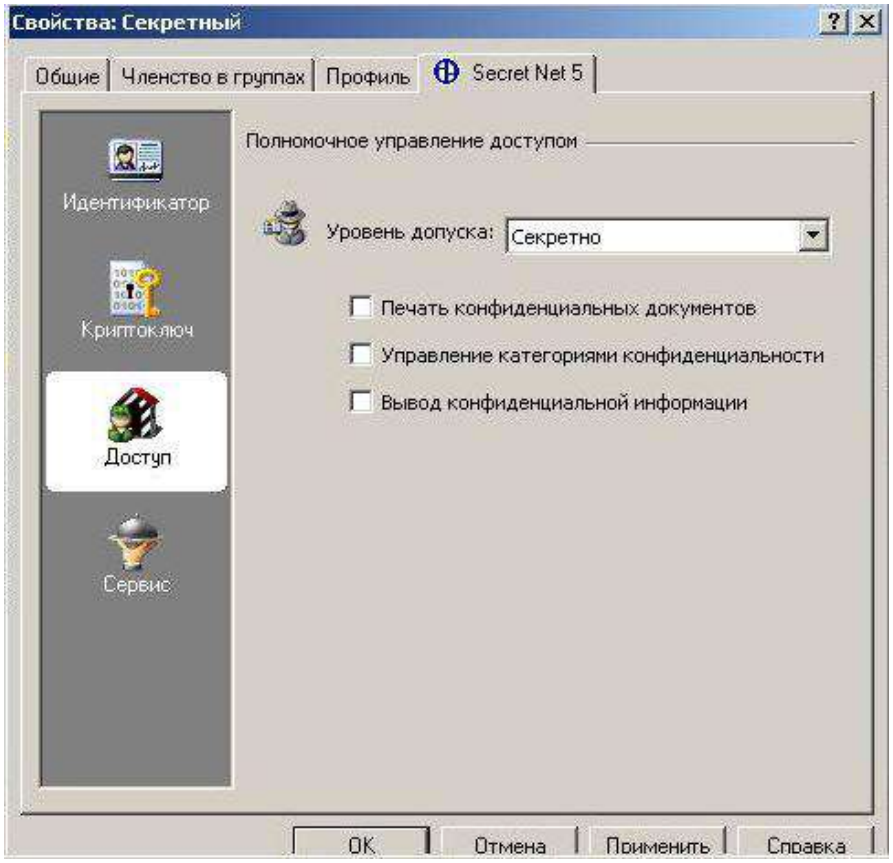


Рисунок 5 – Настройка прав доступа пользователя «Секретный»

3. Настройка объектов доступа (данные)

В механизме полномочного управления доступом используются следующие категории конфиденциальности:

– неконфиденциально (в нашем случае «общедоступно»);

– конфиденциально;

– строго конфиденциально (в нашем случае «секретно»).

Категория конфиденциальности относится к атрибутам ресурса (каталога или файла). Повышение категорий конфиденциальности нужных ресурсов осуществляется пользователями в пределах своих уровней допуска. В механизме полномочного управления доступом используется принцип наследования файлами категории конфиденциальности каталога.

Присвоение новым файлам категории конфиденциальности каталога может выполняться автоматически или по запросу. Включение и отключение режима автоматического присвоения категории осуществляется в диалоговом окне настройки свойств каталога (параметр «Автоматически присваивать новым файлам», рис. 6).

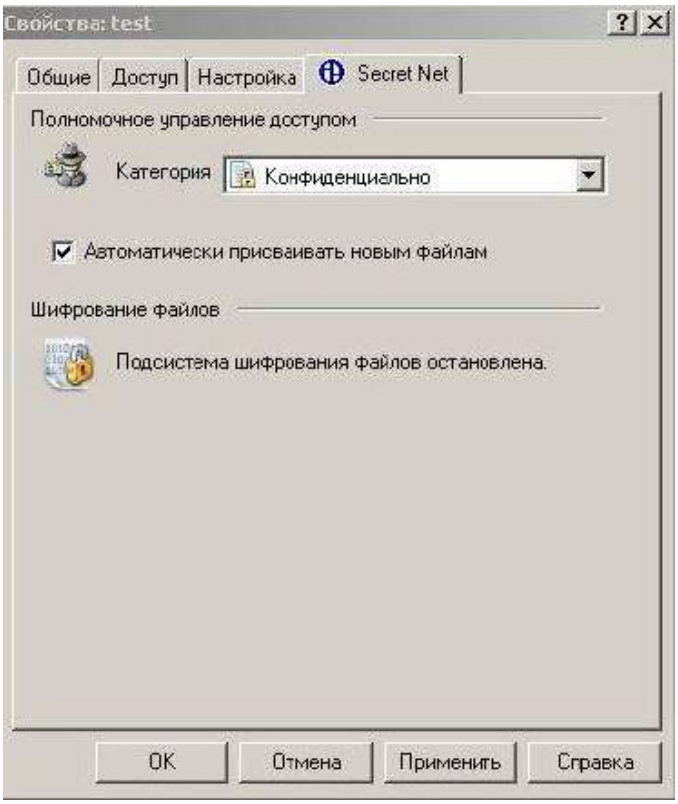


Рисунок 6 – Выбор категории конфиденциальности ресурса

Присвоение ресурсам категорий конфиденциальности выполняется уполномоченными пользователями, имеющими привилегию «Управление категориями конфиденциальности». Категория конфиденциальности может быть присвоена только ресурсам, расположенным на дисках с файловой системой NTFS.

Для изменения категории конфиденциальности каталога или файла в режиме мандатного разграничения доступа необходимо обладать привилегией «Управление категориями конфиденциальности». Если у пользователя нет такой привилегии, то он может только повысить категорию конфиденциальности файла, но не выше своего уровня допуска или уровня конфиденциальности сеанса.

В проводнике вызовите контекстное меню каталога «D:\temp» и выберите «Свойства». В окне «Свойства» откройте вкладку «Secret Net» (рис. 6).

Укажите для каталога следующие значения параметров:

– выберите в раскрывающемся списке поля «Категория» категорию «Конфиденциально»;

– установите режим автоматического присвоения категории конфиденциальности файлам каталога, включив параметр «Автоматически присваивать новым файлам».

Нажмите кнопку «ОК».

Если каталог содержит файлы и подкаталоги, на экране появится диалоговое окно, предлагающее изменить категории конфиденциальности вложенным файлам и каталогам (рис. 7).

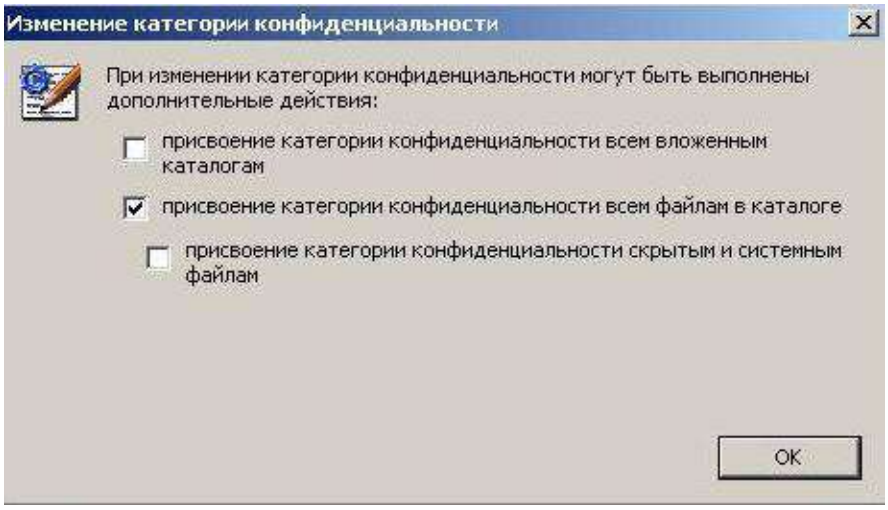


Рисунок 7 – Изменение категории конфиденциальности вложенных каталогов и файлов

Изменение категории конфиденциальности файла производится аналогично.

Пользователю разрешается доступ к файлу, если уровень допуска пользователя не ниже категории конфиденциальности файла. Например, пользователю с уровнем допуска «Конфиденциально» разрешается выполнять чтение файлов с категориями «Конфиденциально» и «Общедоступно», но запрещено открывать файлы с категорией «Секретно». Уровень допуска «Секретно» предоставляет возможность открывать файлы с любой категорией конфиденциальности.

Если категория допуска пользователя выше, чем метка конфиденциальности каталога с документами, то пользователь может открывать документы, но изменять и сохранять в этой же папке не сможет, также запрещено создавать и удалять документы в папках, категория конфиденциальности которых меньше категории допуска пользователя.

Войдите под учётной записью «user» (уровень допуска «Общедоступно»). Попытайтесь открыть файл «D:\temp\Конф.txt». Операционная система выдаст ошибку доступа к этому файлу (рис. 8). Попытайтесь удалить этот файл. Операционная система выдаст ошибку удаления этого файла (рис. 9). Попытайтесь скопировать файл в общедоступный каталог (например, «Рабочий стол»). Операционная система выдаст ошибку копирования файла (рис. 10). Попытайтесь создать новый файл в каталоге «test». Операционная система выдаст ошибку создания файла (рис. 11).

Таким образом, под учётной записью с уровнем допуска «Общедоступно» запрещены любые действия с файловыми объектами уровня «Конфиденциально» (пользователь не может работать с документами, чья категория конфиденциальности выше его уровня допуска).

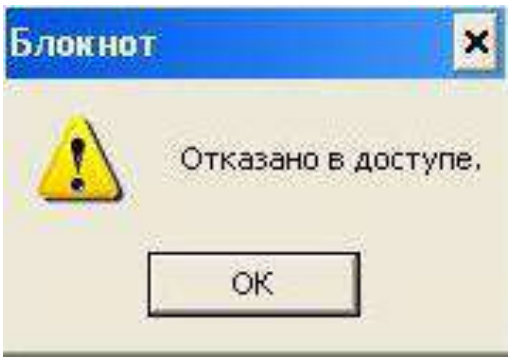


Рисунок 8 – Ошибка доступа к конфиденциальному файлу

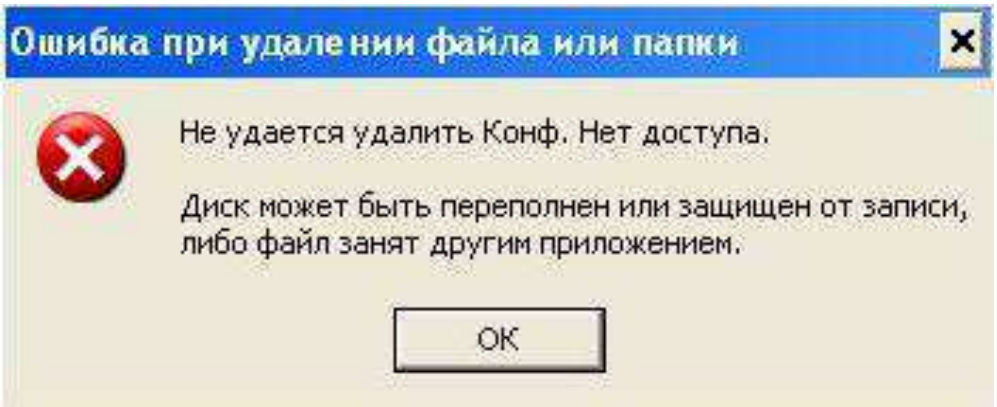


Рисунок 9 – Ошибка удаления конфиденциального файла

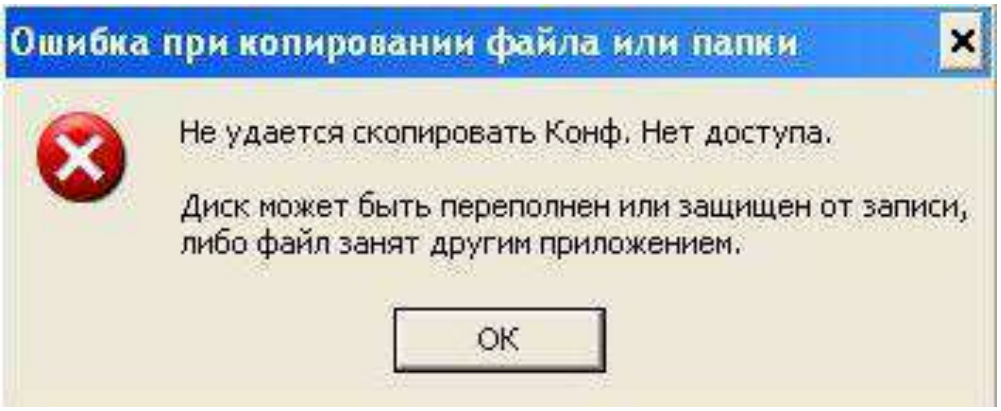


Рисунок 10 – Ошибка копирования конфиденциального файла

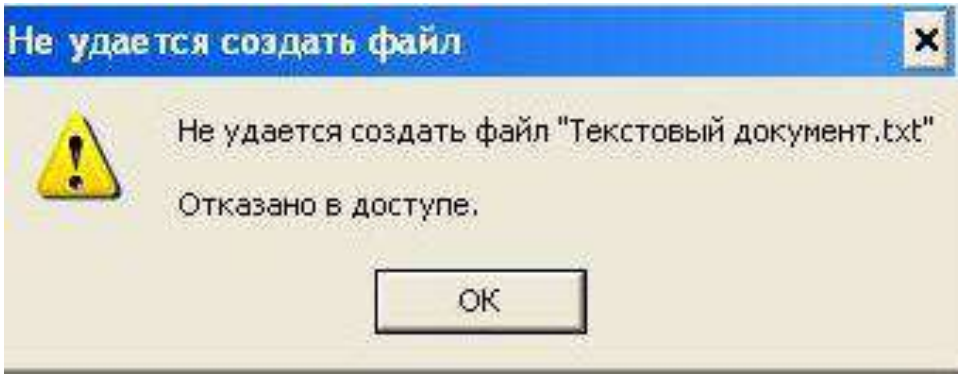


Рисунок 11 – Ошибка создания файла в конфиденциальном каталоге

Войдите под учётной записью «Секретный». Попытайтесь открыть файл «D:\temp\Конф.txt» – будет выдано окно с предложением о повышении уровня конфиденциальности приложения (рис. 12). Работа с файлом будет разрешена только после повышения уровня. Скопируйте файл в общедоступный каталог (например, «Рабочий стол»). Посмотрите уровень конфиденциальности у скопированного файла. После копирования был присвоен уровень «Общедоступно». Попытайтесь скопировать данные из файла «D:\temp\Конф.txt» в любой файл с меткой «Общедоступно». Уровень конфиденциальности у общедоступного файла не изменился.

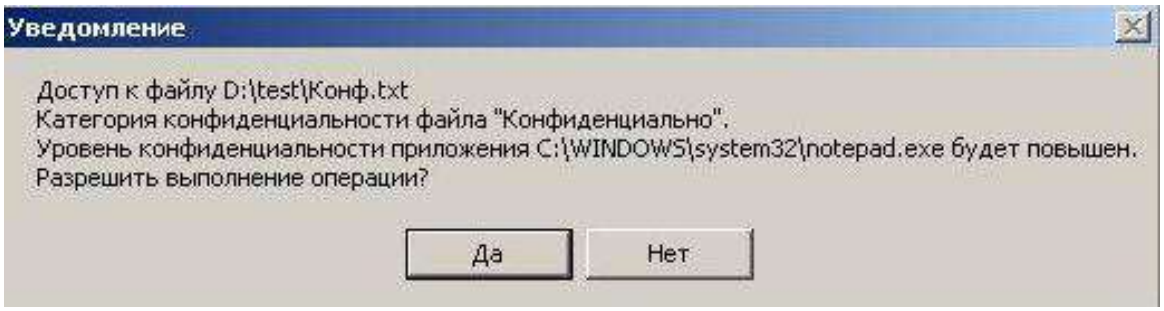


Рисунок 12 – Повышение уровня конфиденциальности приложения

Таким образом, возможность копирования конфиденциальных файлов в общедоступный каталог или самих конфиденциальных данных в общедоступный файл может привести к утечке информации.

При таком подходе ответственность за конфиденциальность информации лежит на пользователях, которым разрешён доступ к информации.

4. Контроль потоков данных

4.1. Включение контроля потоков данных

Запретить пользователям возможность понижения уровня конфиденциальности информации можно при помощи контроля потоков данных.

Войдите под учётной записью «Администратор». Запустите «Локальные параметры безопасности»: «Пуск – Все программы – Secret Net 5 – Локальная политика безопасности», перейдите в группу «Параметры Secret Net – Настройки подсистем». Выберите параметр «Полномочное управление доступом: Режим работы» и включите контроль потоков.

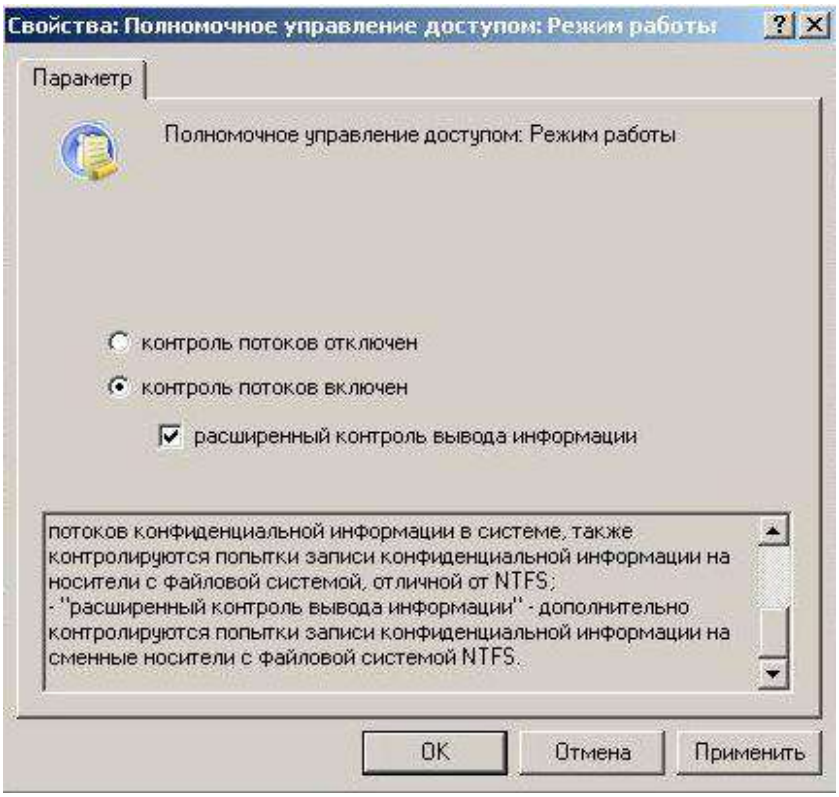


Рисунок 13 – Включение контроля потоков данных

4.2. Работа с конфиденциальными файлами при более высоком уровне сеанса

Перезагрузите операционную систему для применения настроек и войдите под учётной записью «Секретный». При входе появляется предложение выбрать уровень сеанса, определяющего, с каким уровнем конфиденциальности файлов будет проходить работа (рис. 14). Выберите уровень сеанса «Секретно».

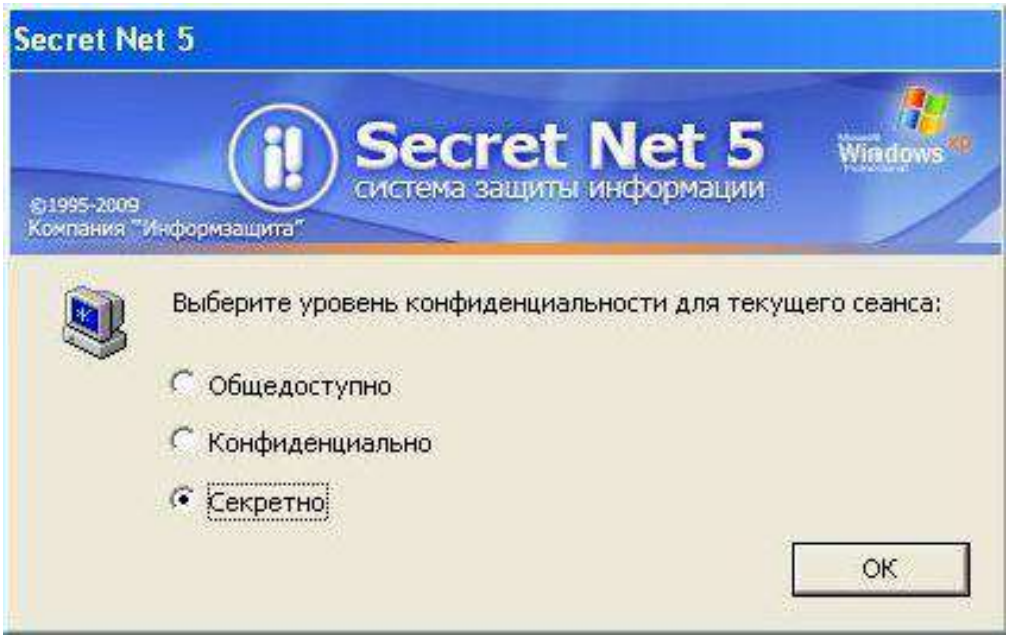


Рисунок 14 – Выбор уровня конфиденциальности сеанса

Откройте файл «D:\temp\Конф.txt». Попытайтесь удалить этот файл, изменить и сохранить его, скопировать в общедоступный каталог (например, «Рабочий стол»). Попытайтесь создать новый файл в каталоге «test». Таким образом, если включен контроль потоков данных, то при уровне сеанса более высоком, чем уровень конфиденциальности файла, все действия, кроме чтения, запрещены.

Измените файл «D:\temp\Конф.txt» и попытайтесь его сохранить под другим именем или в другой каталог. Сохранение будет невозможно (рис. 15), т.к. уровень сеанса выше, чем уровень конфиденциальности каталогов.

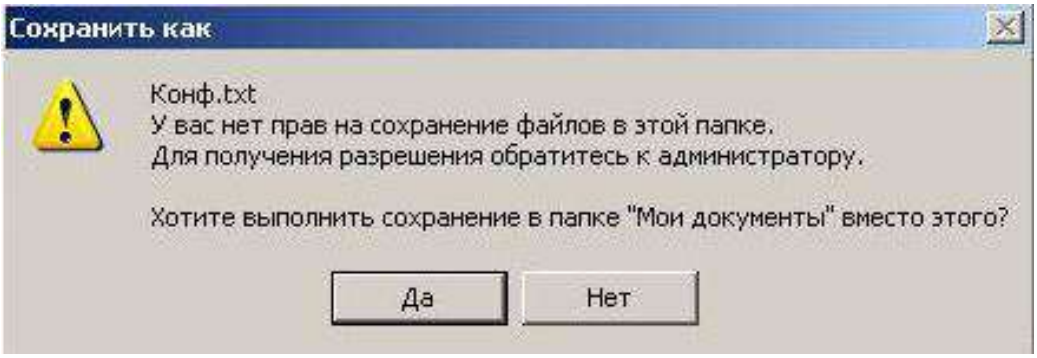


Рисунок 15 – Ошибка сохранения информации при контроле потоков в каталог с меньшим уровнем конфиденциальности, чем уровень сеанса

4.3. Работа с конфиденциальными файлами при равном уровне сеанса

Войдите под учётной записью «Секретный» и выберите уровень сеанса «Конфиденциально».

Откройте файл «D:\temp\Конф.txt». Измените и сохраните этот файл, создайте новый файл в каталоге «test». Попытайтесь

скопировать его в общедоступный каталог (например, «Рабочий стол»).

Скопируйте текст из файла «Конф.txt» в файл «Общее.txt» и попытайтесь сохранить файл «Общее.txt». Произойдёт отказ в доступе из-за попытки понизить уровень конфиденциальности информации. Сохраните файл «Общее.txt» в конфиденциальный каталог «test».

Измените какую-либо настройку операционной системы (например, отображение вкладки «Безопасность»: измените параметр «Использовать простой общий доступ к файлам» в разделе «Панель управления – Свойства папки»). Перезапустите вкладку «Свойства папки» и проверьте состояние параметра. Попытайтесь запустить «Outlook». Изменения настроек операционной системы и приложений записываются в общедоступные файлы, поэтому их сохранение не происходит.

Таким образом, если включен контроль потоков данных, то при уровне сеанса, равном уровню конфиденциальности файла, все действия разрешены, кроме копирования информации в файлы с более низким уровнем конфиденциальности.

Попытайтесь скопировать файл «D:\temp\Конф.txt» на сменный носитель. Копирование не удастся, т.к. данному пользователю не было представлено право копирования конфиденциальной информации на сменный носитель.

4.4. Работа при уровне сеанса «Общедоступно»

Войдите под учётной записью «Секретный» и выберите уровень сеанса «Общедоступно».

Попытайтесь открыть, удалить файл «D:\temp\Конф.txt», скопировать его в общедоступный каталог (например, «Рабочий стол») и на сменный носитель. При уровне сеанса «Общедоступно» любой доступ к конфиденциальной информации запрещён. В то же время доступ к общедоступной информации неограничен: запустите «Outlook», скопируйте общедоступный файл на сменный носитель.

Таким образом, за счёт подхода, основанного на контроле потоков данных, исключается возможность утечки конфиденциальной информации.

4.5. Копирование конфиденциальных файлов на сменный носитель

Войдите под учётной записью «Конфиденциальный». При первом входе необходимо настроить операционную систему, что возможно только при сеансе «Общедоступно», поэтому доступ к конфиденциальной информации запрещён (рис. 16).

Завершите сеанс и снова войдите под учётной записью «Конфиденциальный», выбрав уровень сеанса «Конфиденциально».

Скопируйте файл «D:\temp\Конф.txt» на сменный носитель. При

копировании появится предупреждение о потере файлом уровня конфиденциальности (рис. 17). Несмотря на потерю конфиденциальности, копирование будет разрешено, т.к. пользователю было предоставлено вывода конфиденциальной информации на сменные носители (рис. 4).

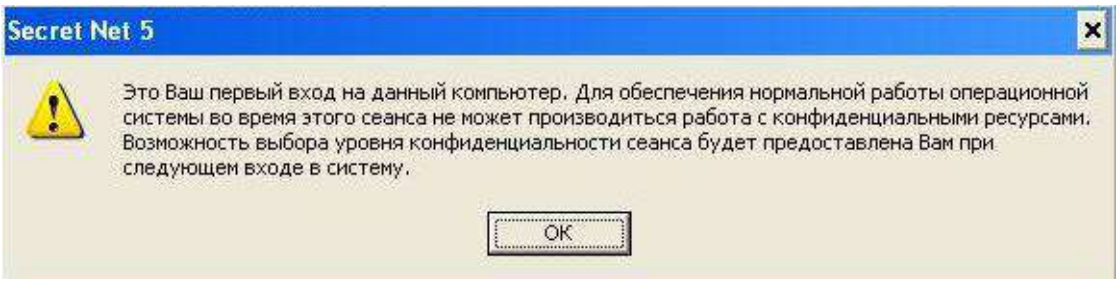


Рисунок 16 – Первый вход в операционную систему

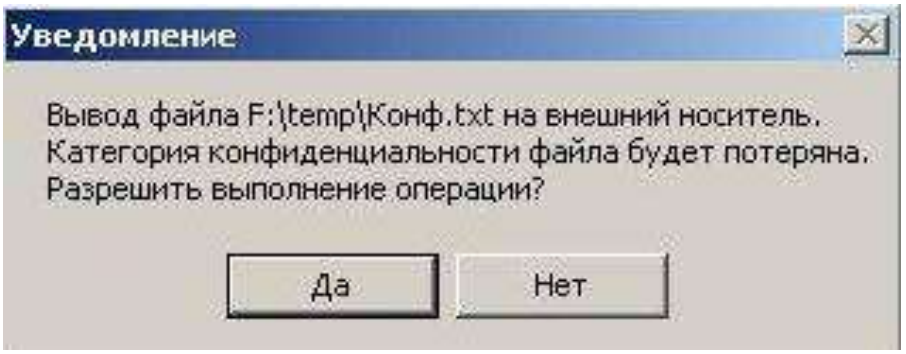


Рисунок 17 – Предупреждение о потере файлом конфиденциальности при копировании на сменный носитель

Задание

1. В соответствии с табл. 1 от имени администратора присвойте каталогам (находящимся в корне диска D:\) категории конфиденциальности.
2. В каждом каталоге создайте 2-4 документа от имени пользователя, допуск которого соответствует категории конфиденциальности каталога.
3. Проверьте возможность доступа к созданным документам.

Таблица 1 – Варианты заданий

Вари-ант	Каталог и его категория конфиденциальности		
	доступно	конфиденциально	секретно
1	D:\БД\Заказы	D:\БД\Поставщики	D:\БД\Клиенты
2	D:\Договоры\ Спонсоры	D:\Договоры\Инве-сторы	D:\Договоры\ Партнёры

3	D:\Документация\Отчёты	D:\Документация\ Приёмные документы	D:\Документация\ Информация о сотрудниках
4	D:\Подразделения\Отдел сбыта	D:\Подразделения\ Отдел кадров	D:\Подразделения \Финансовый отдел
5	D:\Файлы\ Пользователи	D:\Файлы\Опытные пользователи	D:\Файлы\ Администраторы
6	D:\БД\ Поставщики	D:\БД\Заказы	D:\БД\Клиенты
7	D:\Договоры\ Партнёры	D:\Договоры\ Спонсоры	D:\Договоры\ Инвесторы
8	D:\Подразделения\Отдел кадров	D:\Подразделения\ Финансовый отдел	D:\Подразделения \Отдел сбыта
9	D:\Файлы\ Опытные пользователи	D:\Файлы\ Пользователи	D:\Файлы\ Администраторы
10	D:\Документация\Приёмные документы	D:\Документация\ Отчёты	D:\Документация\ Информация о сотрудниках

Контрольные вопросы

1. На чём основан принцип действия мандатного механизма разграничения доступа?
2. Разрешается ли пользователю доступ к файлу, если уровень допуска пользователя выше категории конфиденциальности файла?
3. Что означает функция «Вывод конфиденциальной информации»?
4. Перечислите категории конфиденциальности по умолчанию.
5. Какой параметр предоставляет возможность управлять категориями конфиденциальности?
6. Можно ли присвоить категорию конфиденциальности ресурсу, расположенному на диске с файловой системой FAT32?
7. Поясните параметр «Автоматически присваивать новым файлам».
8. Для чего нужен контроль потоков данных?
9. При каком уровне сеанса пользователь может изменять настройки операционной системы и приложений?
10. Какие права предоставляются пользователю при доступе к конфиденциальной информации, уровень которой ниже уровня сеанса?

Лабораторная работа № 13

Применение криптопровайдеров на автоматизированном рабочем месте

Цель работы

Целью данной лабораторной работы является получение практических навыков по установке и настройке криптопровайдеров СКЗИ «Signal-COM CSP» и СКЗИ «КриптоПро»

СКЗИ "Signal-COM CSP"

СКЗИ "Signal-COM CSP" предназначено для генерации и управления ключевой информацией, шифрования, выработки значения хеш-функции, формирования и проверки электронной цифровой подписи для областей оперативной памяти и других данных, для защиты данных по протоколам TLS и CMS.

СКЗИ "Signal-COM CSP" реализовано в соответствии с интерфейсом Cryptographic Service Provider (CSP), что позволяет приложениям, использующим стандартные интерфейсы компании Microsoft, работать с российскими криптографическими алгоритмами и протоколами.

СКЗИ "Signal-COM CSP" позволяет выполнять следующие криптографические операции:

- Генерация криптографических ключей.
- Хеширование данных в соответствии с ГОСТ Р 34.11-94.
- Формирование и проверка цифровых подписей в соответствии с ГОСТ Р 34.10-2001.
- Зашифрование и расшифрование данных в соответствии с ГОСТ 28147-89.

Криптографические ключи, используемые в СКЗИ "Signal-COM CSP", подразделяются на *сеансовые* и *парные* (с открытым ключом). Сеансовые ключи используются в симметричных (одноключевых) алгоритмах для зашифрования и расшифрования данных. Они создаются на определенный сеанс работы с СКЗИ "Signal-COM CSP" и уничтожаются после его завершения.

Парные ключи используются в алгоритмах с открытым ключом для формирования цифровых подписей и зашифрования сеансовых ключей. Они состоят из ***закрытого ключа, который должен быть известен только его владельцу***, и *открытого ключа*, который в виде *сертификата* (см. ниже) может и должен распространяться свободно (помещаться в открытые справочники, передаваться по почте и т.д.). С помощью парного закрытого ключа осуществляется формирование цифровой подписи владельца ключа и расшифрование сеансовых ключей.

Парный открытый ключ используется для проверки цифровой подписи, сформированной закрытым ключом, и для зашифрования сеансовых ключей, которые, в свою очередь, используются для зашифрования сообщения в адрес владельца закрытого ключа.

Парные ключи условно подразделяются на *ключи подписи* и *ключи обмена* (ключи зашифрования сеансовых ключей), хотя и те, и другие могут использоваться для формирования цифровой подписи и зашифрования сеансовых ключей. Для обеспечения высокого уровня безопасности рекомендуется использовать одну пару ключей для формирования цифровых подписей и другую пару ключей - для зашифрования сеансовых ключей.

Ход работы

Для установки СКЗИ "Signal-COM CSP" запустите установочную программу SCCSP-X86-RUS.EXE (для 32-битных ОС) или SCCSP-X64-RUS.EXE (для 64-битных ОС) и далее следуйте ее указаниям.

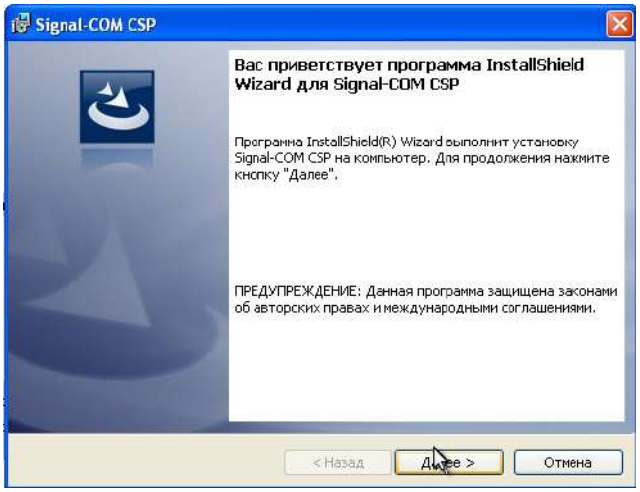


Рисунок 4.1 — Установка СКЗИ "Signal-COM CSP"

Если Вы не ввели ключ продукта (лицензии) при установке СКЗИ "Signal-COM CSP", данное программное обеспечение будет функционировать в течение 30 дней с момента установки. Вы можете ввести ключ продукта позже, воспользовавшись утилитой *Администратор* (см. "Модуль настроек и сервисных функций. Руководство пользователя."), поставляемой в составе дистрибутива СКЗИ "Signal-COM CSP". Продолжайте установку без ввода ключа.

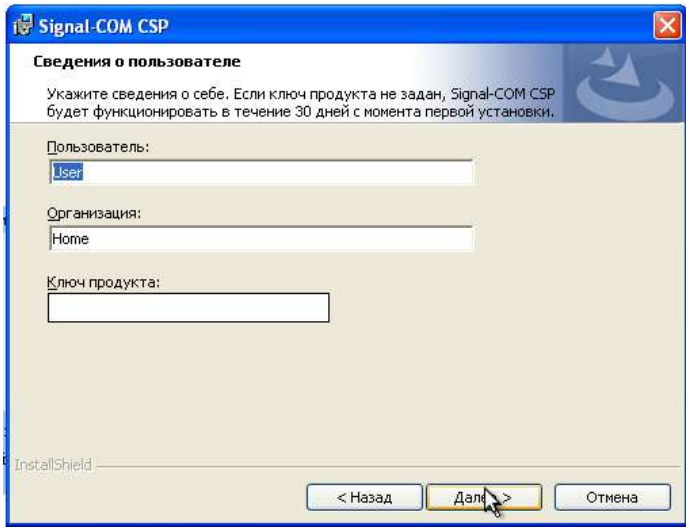


Рисунок 4.2 — Ввод ключа

При выборе вида установки "Обычная" будет установлен стандартный набор компонентов (Signal-COM CSP), в который входят базовые модули криптопровайдера (поддержка российских криптографических алгоритмов в функциях MS CryptoAPI), а также модули поддержки российских криптоалгоритмов в приложениях компании Microsoft: приложения Microsoft Office Word, Excel, PowerPoint, InfoPath и Outlook, Outlook Express (Почта Windows) и др.

При выборе вида установки "Выборочная" пользователь может дополнительно установить компонент Signal-COM TLS, в который входят модули поддержки российских криптоалгоритмов в протоколе TLS (SSL), а также модуль формирования электронных подписей данных HTML-форм (для работы с сервером системы Inter-PRO напрямую с помощью браузера MS Internet Explorer).

Сделайте выборочную установку Signal-COM CSP без установки компонента Signal-COM TLS.

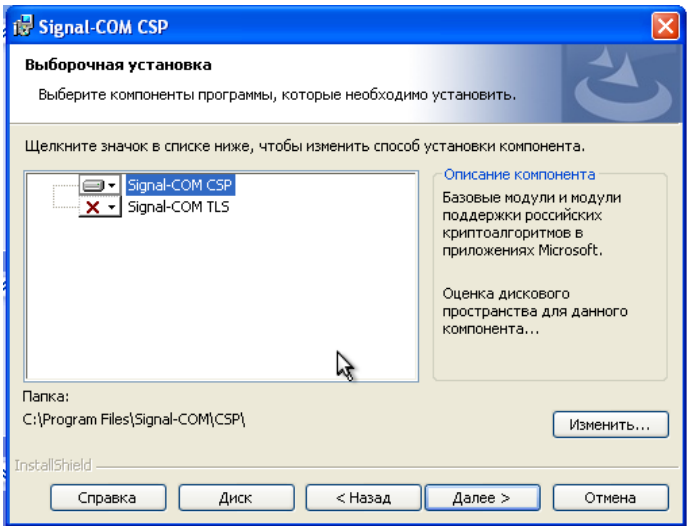


Рисунок 4.3 — Выбор компонентов

После завершения установки необходимо перезагрузить систему для работы с программой.

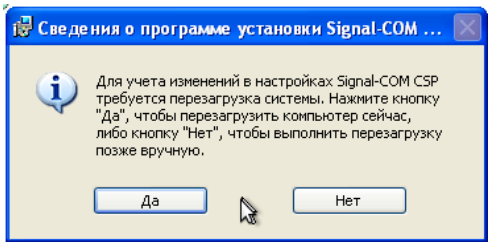


Рисунок 4.4 — Завершение установки

Запустить приложение можно из меню Пуск (Все программы/Signal-COM CSP/Администратор)

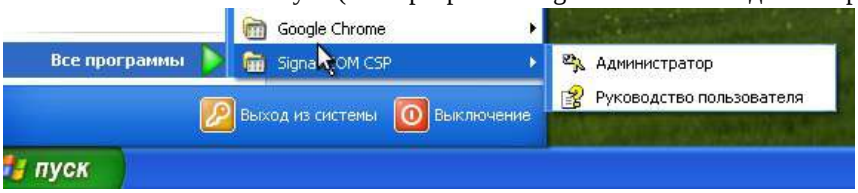


Рисунок 4.5 — Запуск программы из меню Пуск.

На рисунке 4.6 представлено главное окно программы. Закройте его ивыполните установку компонента Signal-COM TLS. Из панели управления (в списке установленных программ необходимо выбрать Signal-COM CSP, открыть контекстное меню и выбрать "Изменить").

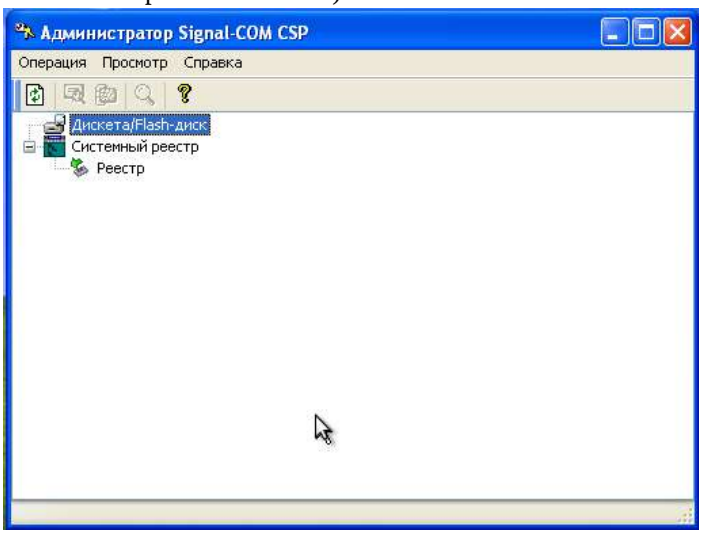


Рисунок 4.6 — Основное окно

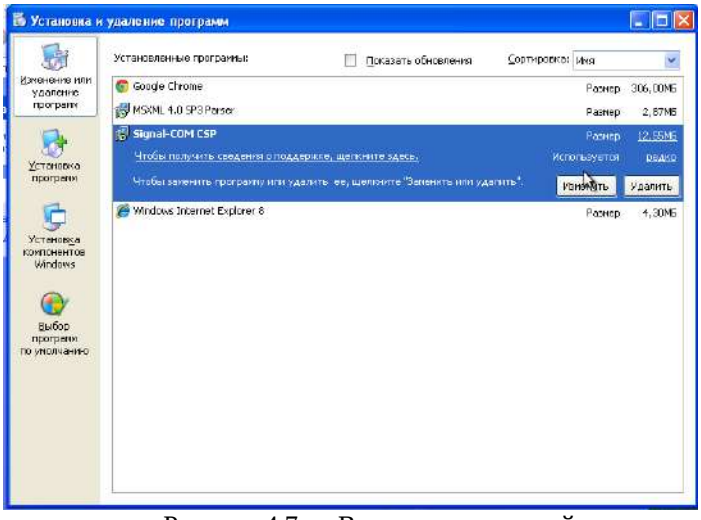


Рисунок 4.7 — Внесение изменений

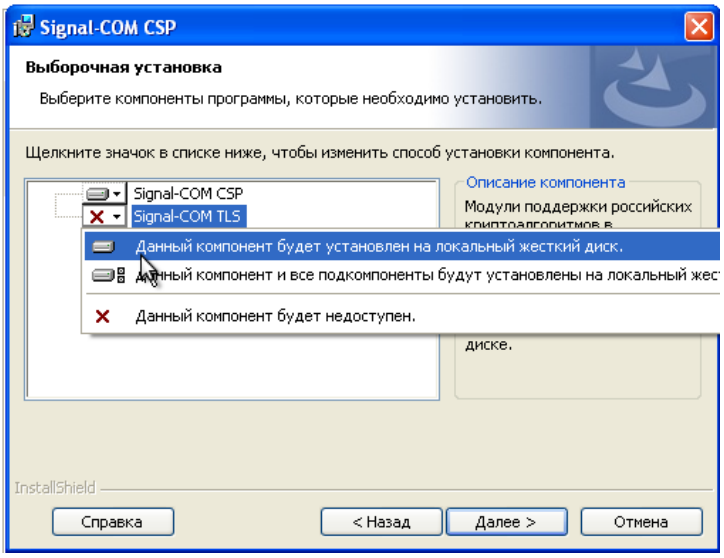


Рисунок 4.8 — Установка Signal-COM TLS

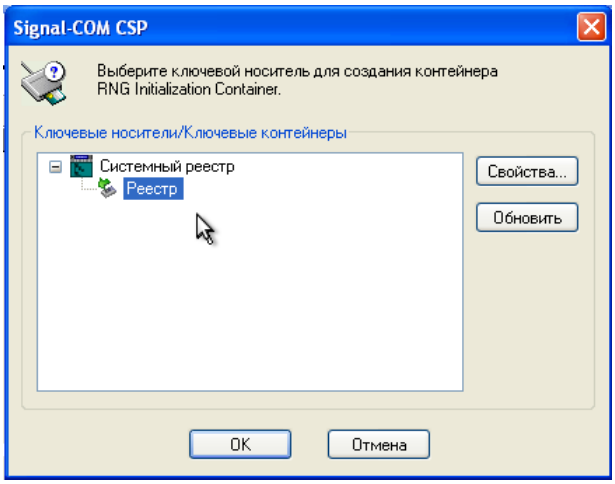


Рисунок 4.9 — Выбор контейнера

При добавлении компонент Signal-COM TLS, вам будет предложено выбрать ключевой носитель (системный реестр) для создания ключевого контейнера, который будет использоваться для инициализации датчика случайных чисел в системных сервисах (обычно серверы), использующих протокол TLS (SSL).

Далее стартует процедура начальной инициализации датчика случайных чисел (ДСЧ), которая требует нажатий клавиатуры или перемещений курсора мыши. .

Для того, чтобы начать использовать СКЗИ "Signal-COM CSP" в каком-либо приложении Windows, как правило, необходимо выполнить следующие действия:

1. Зарегистрировать полученные сертификаты в локальной базе сертификатов;
2. Настроить приложение Windows на работу с полученным пользовательским сертификатом.

СКЗИ "Signal-COM CSP" использует встроенный датчик случайных чисел (ДСЧ), который должен быть инициализирован перед использованием. Инициализация ДСЧ осуществляется двумя способами: с использованием существующего ключевого контейнера или с помощью специальной процедуры.

Перезагрузите систему.

В состав СКЗИ "Signal-COM CSP" входит программа *Администратор*, предназначенная для настройки параметров СКЗИ, а также для выполнения операций с ключевыми контейнерами: копирование, удаление, изменение пароля, импорт и экспорт сертификатов и др. Например, с помощью данной программы можно перенести и зарегистрировать свой личный сертификат для работы на данном компьютере.

Для этого выберем во вкладке «операции» «импорт» ,появится следующее окно(Рисунок 4.10).

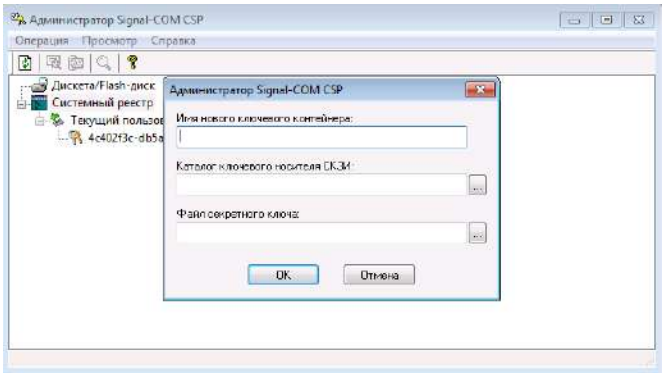


Рисунок 4.10 – Импорт сертификата

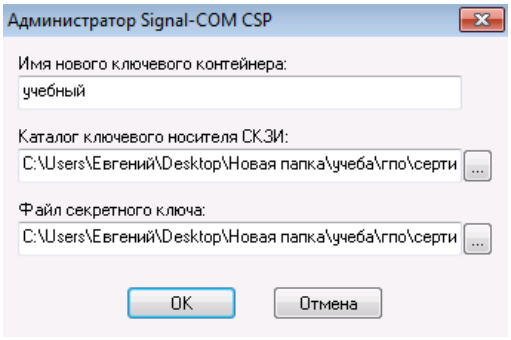


Рисунок 4.11 – Настройка импорта

Далее нажать «Ok» так как отсутствует носитель ,появится ошибка (рисунок 6), пропустим ее так как на данном этапе работы будем считать что требовалось только добавить сертификат, что мы успешно сделали.

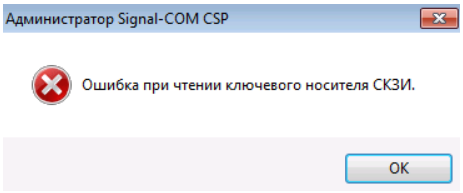


Рисунок 4.12 – Ошибка, вызванная отсутствием ключевого носителя

СКЗИ КриптоПро CSP

Перейдем к изучению СКЗИ КриптоПро CSP. КриптоПро CSP обеспечивает**:**

- информационную безопасность по уровню защиты КС2;
- информационную безопасность по уровню защиты КС3;
- выполнение функций создания и проверки электронной цифровой подписи (ЭЦП), выполнение функций шифрования и имитозащиты;
- формирование электронных сертификатов открытых ключей пользователей;
- аутентификацию программных компонент и пользователя при обмене информацией между ними с использованием модуля поддержки сетевой аутентификации

Установка дистрибутива СКЗИ КриптоПро CSP должна производиться пользователем, имеющим права администратора. Для установки программного обеспечения вставьте компакт-диск в дисковод. Из предлагаемых дистрибутивов выберите дистрибутив, подходящий для Вашей операционной системы, имеющий нужный Вам уровень защищенности и удобный для Вас язык установки. Запустите выполнение установки.

Либо установщик можно скачать с сайта.

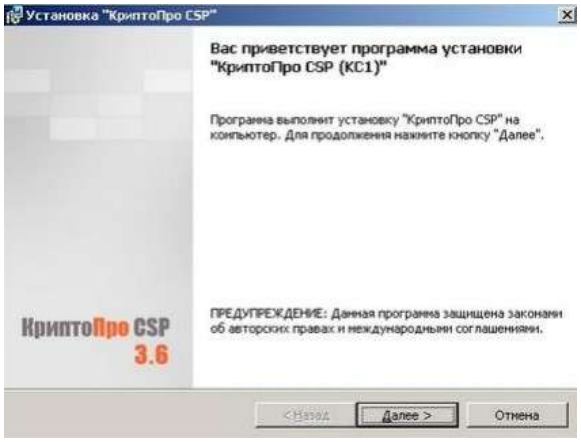


Рисунок 4.13 – Приветственное окно мастера установки

Если мастер установки обнаружит на машине более раннюю версию СКЗИ КриптоПро CSP, то в окне появится информация о замещаемых продуктах:

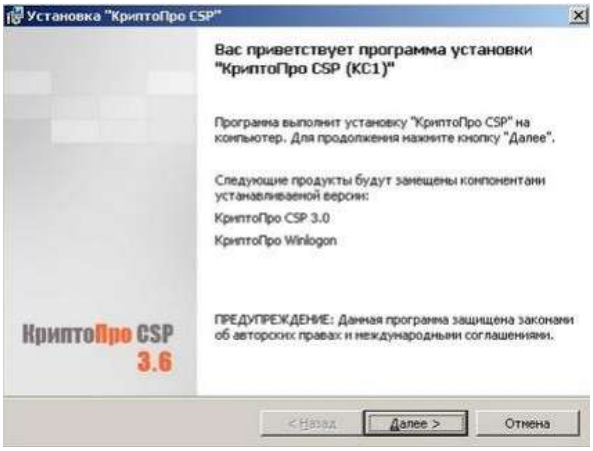


Рисунок 4.14 – Установка с замещением компонентов

Примечание: При установке в режиме замещения компонент важно, чтобы уровень защищенности установленной на компьютере версии СКЗИ КриптоПро CSP совпадал с уровнем защищенности в выбранном Вами для установки дистрибутиве. В противном случае появится сообщение об ошибке и установка завершена не будет:

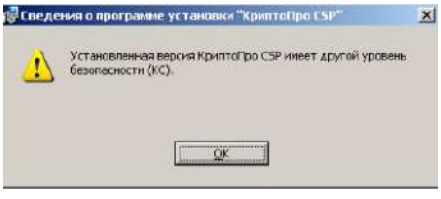


Рисунок 4.15 – Сообщение об ошибке

В этом случае необходимо выбрать установку с дистрибутива, имеющего соответствующего установленному уровню защищенности.

Для дальнейшей установки КриптоПро CSP нажмите «Далее».

Последующая установка производится в соответствии с сообщениями, выдаваемыми программой установки. В процессе установки будет предложено зарегистрировать дополнительные считыватели ключевой информации, дополнительные датчики случайных чисел (для уровней КС2 и КС3) или настроить криптопровайдер на использование службы хранения ключей (для уровня КС1).

Все эти настройки можно произвести как в момент установки криптопровайдера, так и в любой момент после завершения установки через панель свойств КриптоПро CSP.

После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

Панель настройки КриптоПро CSP доступна как отдельный пункт в группе программ «КриптоПро» (Пуск → Программы), а также из оснастки КриптоПро PKI, расположенной в той же группе программ «КриптоПро» (Пуск → Программы).

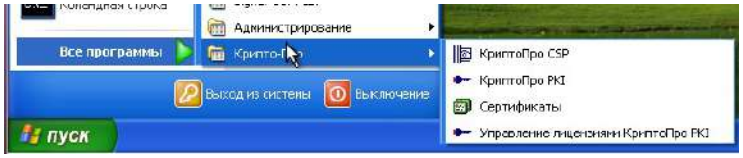


Рисунок 4.16 – Группа программ в меню «Пуск»

В оснастке «Управление лицензиями КриптоПро PKI», расположенной в группе программ «КриптоПро» (меню Пуск → Программы) осуществляется ввод лицензий и просмотр лицензионной информации обо всех установленных продуктах ООО "КРИПТО-ПРО".

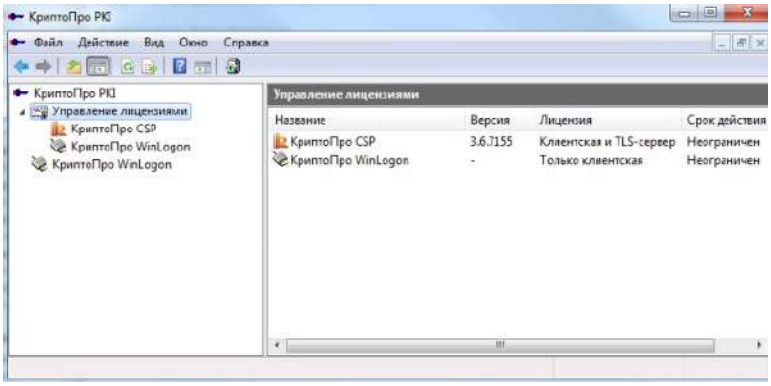


Рисунок 4.17 – КриптоПро PKI

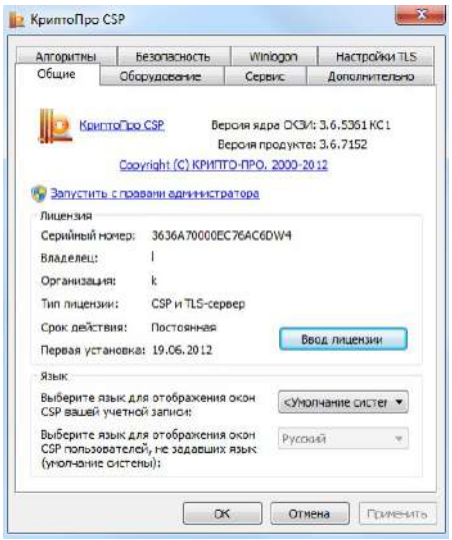


Рисунок 4.18 – КриптоПро CSP

Откройте оснастку «Сертификаты» (Пуск/Программы/Крипто-Про/Сертификаты). В корне консоли представлено две группы сертификатов: пользовательские и локальной машины(Рисунок 4.19).

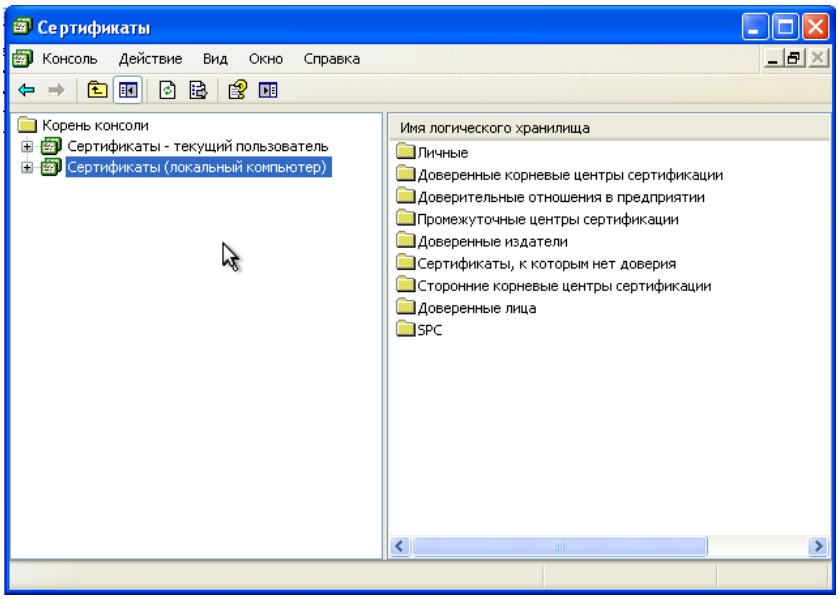


Рисунок 4.19 — оснастка сертификатов

Выберите пункт Действие/Поиск сертификатов. Найдите сертификаты выданные компанией Microsoft. Как видно на рисунке 4.20 поиск можно вести по разным полям. Нас интересует поле «Кем выдан».

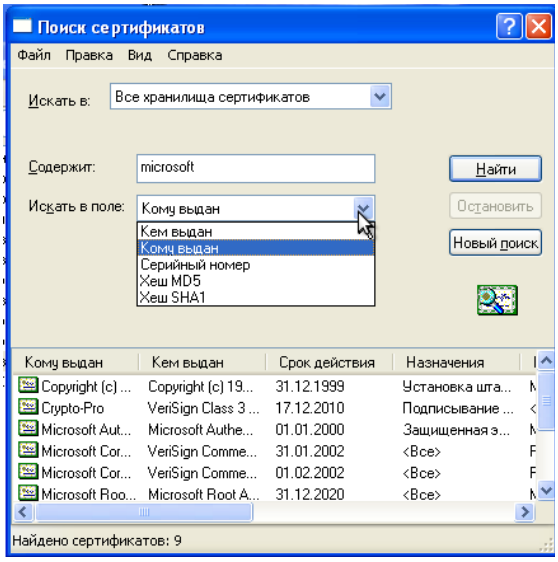


Рисунок 4.20 — Поиск сертификатов.

Просмотрите сведенья о сертификатах сделав двойной клик мыши на интересующем.

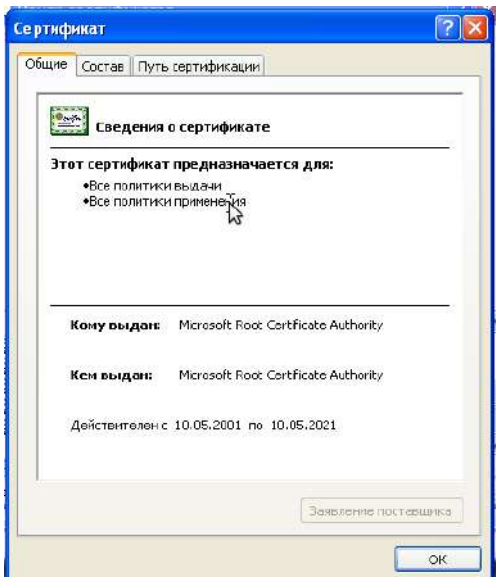


Рисунок 4.21 — Сведения о сертификате

Сделайте экспорт любого из сертификатов, нажав правой кнопкой мыши на сертификате и выбрав соответствующий пункт меню.

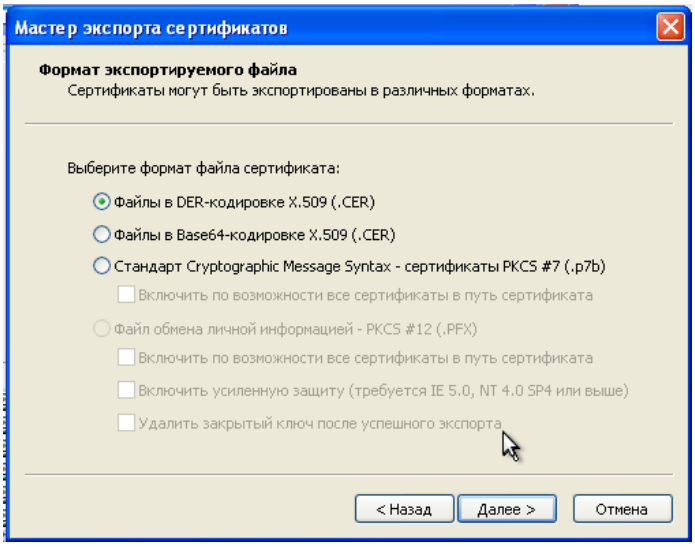


Рисунок 4.22 — Экспорт сертификата

Вам потребуется выбрать формат и ввести имя файла. Сохраните файл на рабочий стол.

Лабораторная работа № 14

Применение средств криптографической защиты информации на автоматизированном рабочем месте

1 Теоретическая часть

VeraCrypt – бесплатное программное обеспечение с открытым исходным кодом для шифрования файлов и дисков, использующая шифрование «на лету». Программа была создана на основе исходного кода программы TrueCrypt, которая когда-то была популярна, но проект был закрыт. На рисунке 1 показан общий вид интерфейса программы.

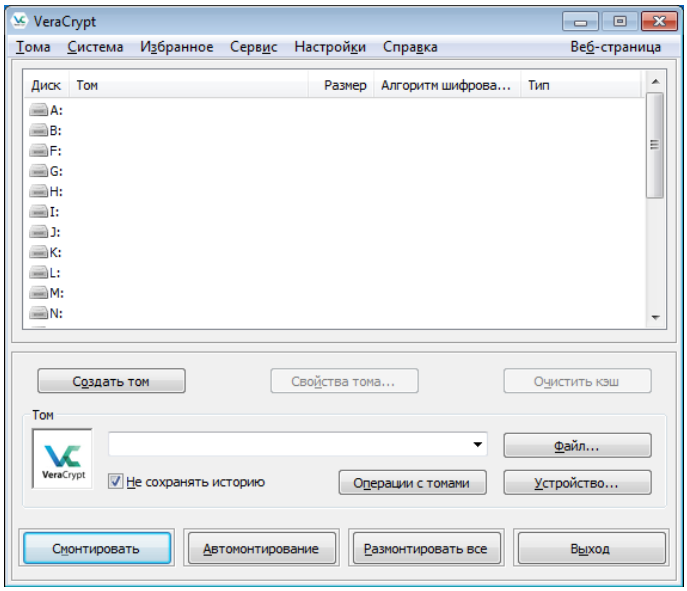


Рисунок 1 – Общий вид программы

Программа работает под операционными системами семейства Windows, Linux, MacOS X, FreeBSD 11. Выпускаются версии для установки и портативные, что не только упрощает работу с программой за счет кроссплатформенности и быстроты установки на новой системе, но и позволяет сразу избавиться от нее после завершения работы, что усложняет установку факта шифрования ею.

VeraCrypt использует следующие алгоритмы шифрования: AES, Serpent, Twofish, Camellia, Кузнечик, а также комбинации этих алгоритмов. Используемые криптографические хеш-функции: RIPEMD-160, SHA-256, SHA-512, Стрибог и Whirlpool. Ключ заголовка и вторичный ключ заголовка для режима XTS генерируются при помощи алгоритма PBKDF2 с использованием

512-битной криптографической соли, число итераций составляет от 327 661 до 655 331, в зависимости от используемой хеш-функции. Это позволяет выбрать пользователю предпочитаемый алгоритм шифрования и балансировать между производительностью и сложностью криптографических преобразований.

Программа может создавать файловые контейнеры и шифровать диски целиком, при этом имеется возможность создать дополнительно скрытые контейнеры и тома, которые будут находиться внутри других зашифрованных контейнерах и томах. Это позволяет выдать ключ для расшифрования файлов злоумышленнику, но при этом важные файлы будут все еще находиться в безопасности.

Также возможно зашифровать системный диск и создать скрытую операционную систему. В случаи вынужденной выдачи пароля, можно будет выдать пароль от операционной системы, которая не представляет ценности, в то время, как ваши файлы останутся в безопасности.

Для расшифровывания может использоваться пароль или ключевой файл.

2 Практическая часть

2.1 Создание зашифрованного файлового контейнера

Для создания зашифрованного файлового контейнера перейдите в меню программы – тома – создать новый том (рисунок 2).

В программе файловые контейнеры называются томами.

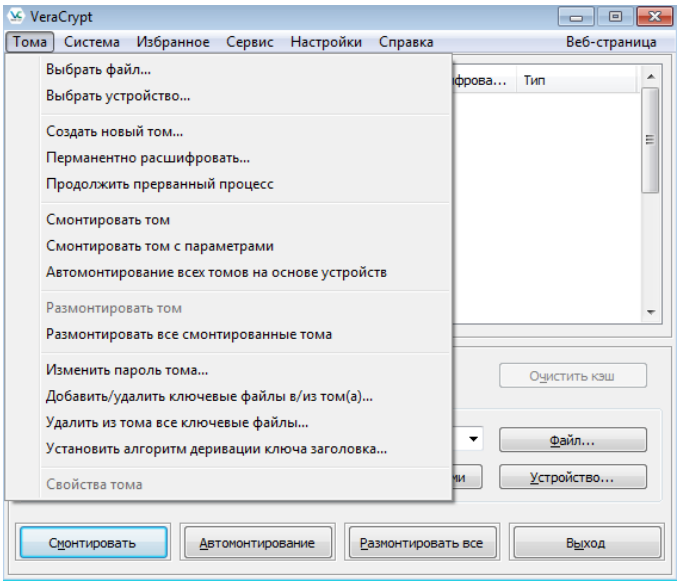


Рисунок 2 – Меню «Тома»

После этого высветится окно создания томов. Выберите пункт «Создать зашифрованный файловый контейнер» и нажмите кнопку «Далее» (рисунок 3).

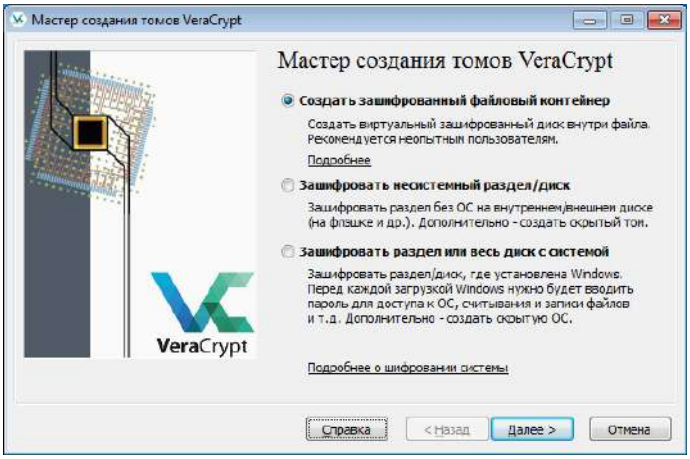


Рисунок 3 – Мастер создания томов

Далее нужно выбрать тип создаваемого тома. Если выбрать тип «Обычный том VeraCrypt», то контейнер будет просто зашифрован. Если же выбрать «Скрытый том VeraCrypt», то будут созданы два тома, один будет вложен в другой и вложенный будет скрыт. При этом не обязательно постоянно вводить оба пароля, достаточно ввести только один для тома, который хотите открыть.

Следует учитывать, что НЕ скрытый том динамически расширяется и если у вас контейнер занимает 10Гб, вы запишите в скрытый том 9Гб информации, а в не скрытый 2 Гб, то скрытый будет поврежден и сузится до 8Гб.

Выберем тип тома «Обычный том» (рисунок 4).

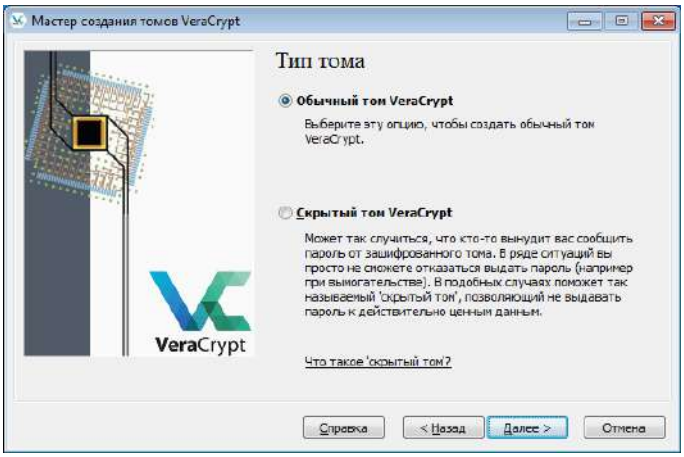


Рисунок 4 – Тип тома

Выберем путь, где будет располагаться контейнер, и название файла в соответствии с группой и инициалами (рисунок 5).

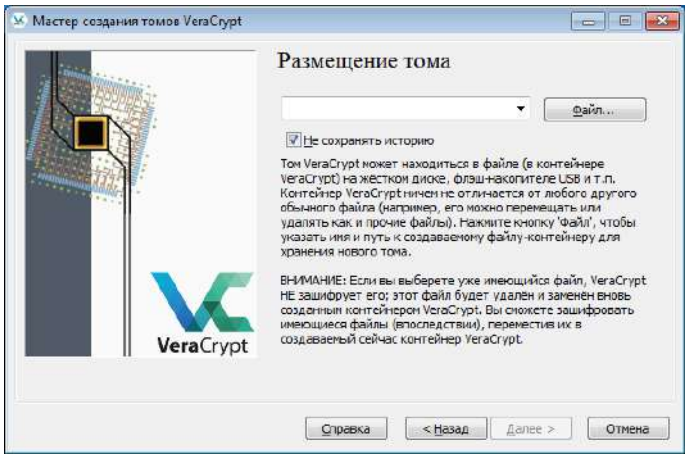


Рисунок 5 – Размещение тома

Выберите алгоритм шифрования в соответствии с вариантом (рисунок 6 и 7).

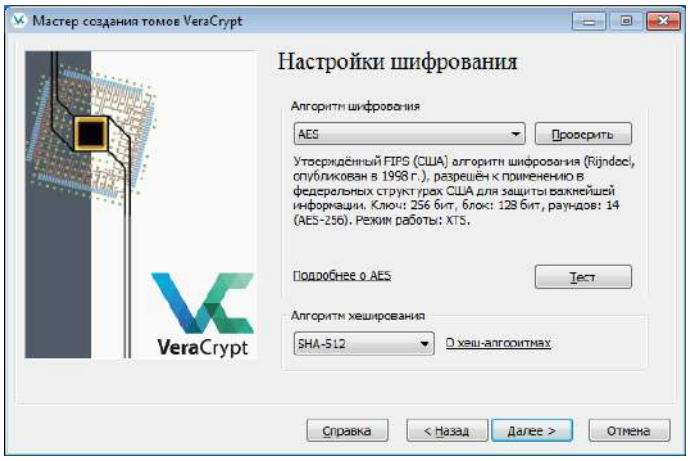


Рисунок 6 – Настройки шифрования

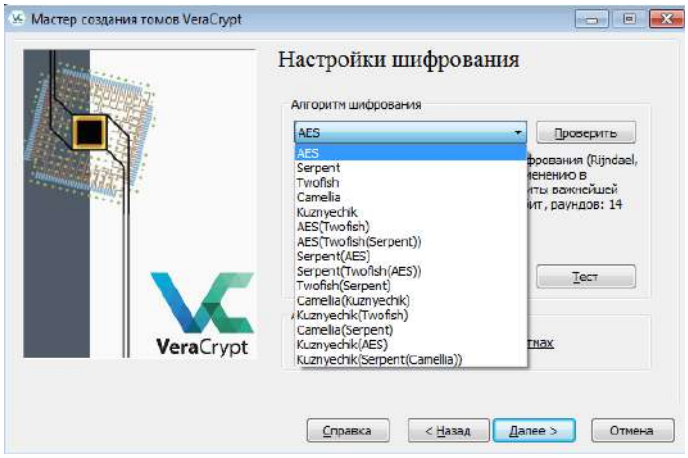


Рисунок 7 – Алгоритмы шифрования

Алгоритм хеширования оставим по умолчанию «SHA-512» (рисунок 8).

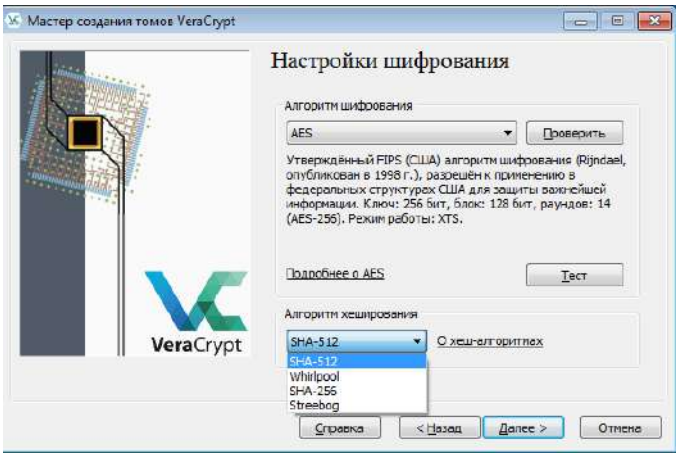


Рисунок 8 – Алгоритмы хеширования

Нажмите кнопку «Проверить» в разделе «Алгоритм шифрования». Выполните проверку выбранного алгоритма шифрования (рисунок 9).

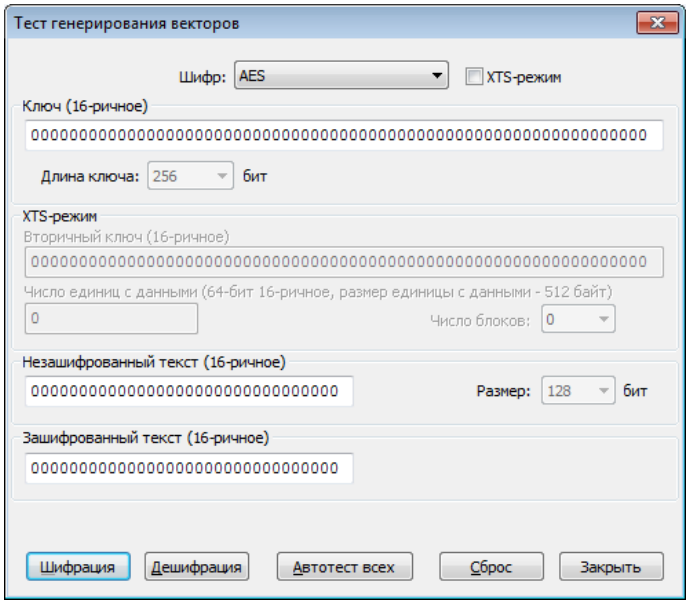


Рисунок 9 – Тестирования алгоритма шифрования

Выболните тест скорости алгоритмов шифрования нажав на кнопку «Тест» (рисунок 10). Проанализируйте полученные данные.

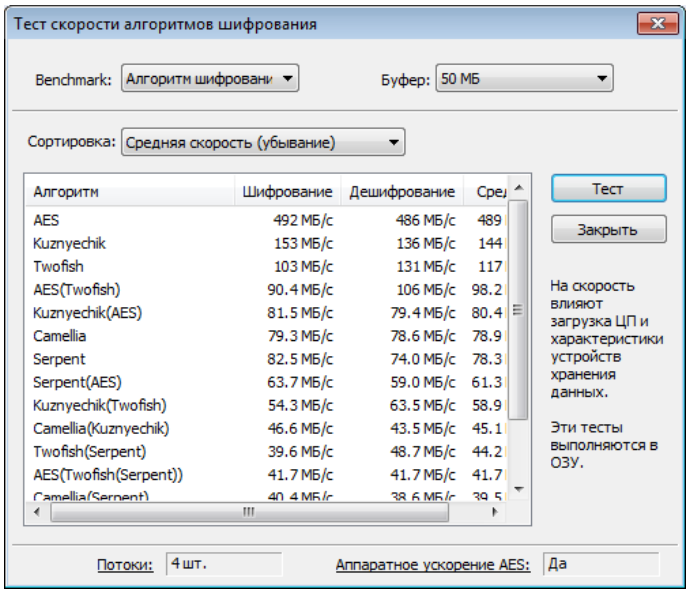


Рисунок 10 – Тест скорости алгоритмов шифрования

Выберите размер создаваемого файлового контейнера (рисунок 11).

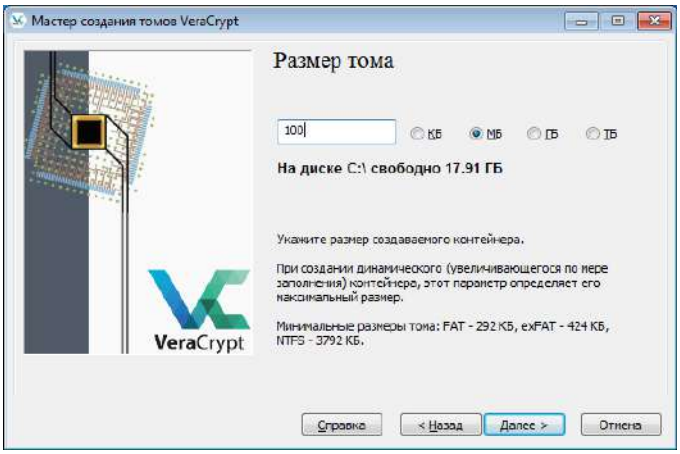


Рисунок 11 – Размер тома

Далее необходимо создать ключевые файлы для создаваемого контейнера. Для этого поставим отметку в пункте «Ключ. Файлы» и нажмем на кнопку «Ключ. Файлы» (рисунок 12).

Также возможно использовать пароль и PIM, но сейчас мы это делать не будем.

PIM – персональный умножитель итераций. Эта функция усложняет взлом перебором. При использовании PIM, при вводе пароля, потребуется постоянно его использовать.

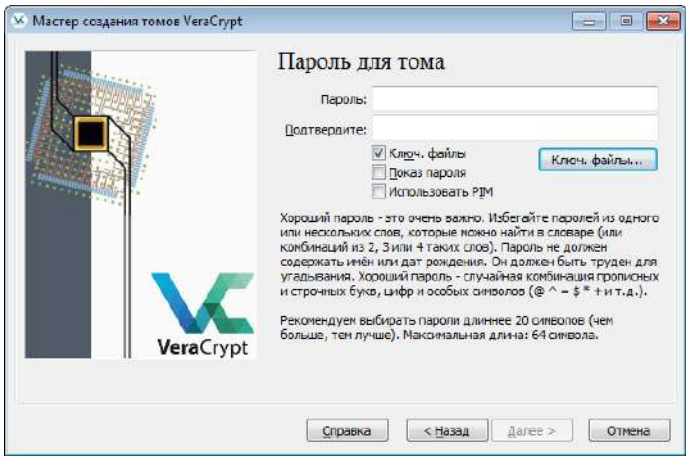


Рисунок 12 – Настройка доступ к тому

Создайте любой файл осмысленного содержимого, например, картинку, в любом месте диска виртуальной машины. Файл может иметь любое содержимое и расширение. В интерфейсе программы на кнопку «Файл» и выберите созданный файл. Нажмем кнопку «Ок» и «Далее» (рисунок 13).

Файлов может быть несколько, иметь различный формат и содержимое, располагаться в любом месте, включая флеш-диск и электронный ключ. Но учтите, что, потеряв его, вы больше никогда не сможете получить доступ к зашифрованным файлам.

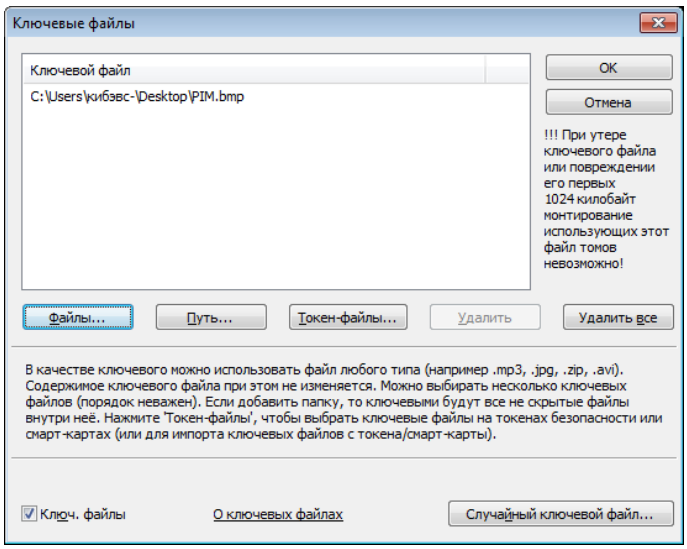


Рисунок 13 – Добавление ключевого файла

Далее выберем файловую систему FAT. Соберем энтропию, для этого будем случайно перемещать мышь по интерфейсу окна программы. В процессе будет заполняться шкала «Собрано энтропии из перемещений мыши». Чем

больше будет заполнена шкала – тем сложнее будет взломать ваш зашифрованный том.

По окончании сбора энтропии нажмите кнопку «Разметить» (рисунок 14).

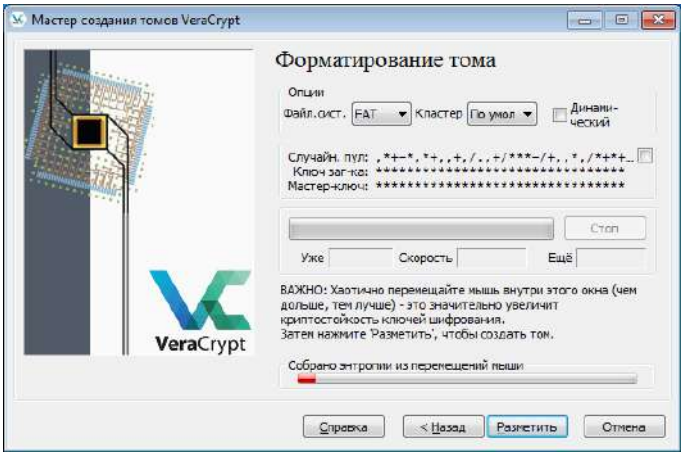


Рисунок 14 – Разметка тома

После завершения разметки будет выдано сообщение о успехе (рисунок 15).

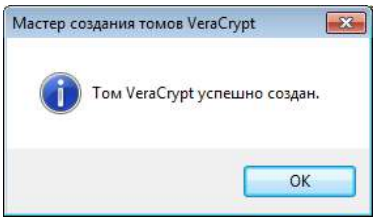


Рисунок 15 – Успешное создание тома

Перейдем в основной интерфейс программы. Для открытия созданного контейнера необходимо выбрать любую из доступных в интерфейсе программы букв диска, нажать кнопку «Файл» и выбрать контейнер. Далее необходимо нажать кнопку «Смонтировать» (рисунок 16).

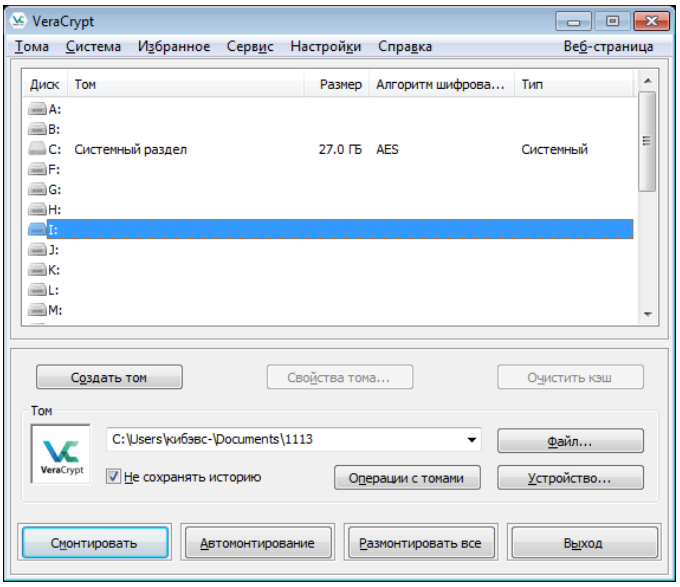


Рисунок 16 – Монтирования тома

Далее высветится окно, где необходимо выбрать ключевой файл и нажать «Ок» (рисунок 17).

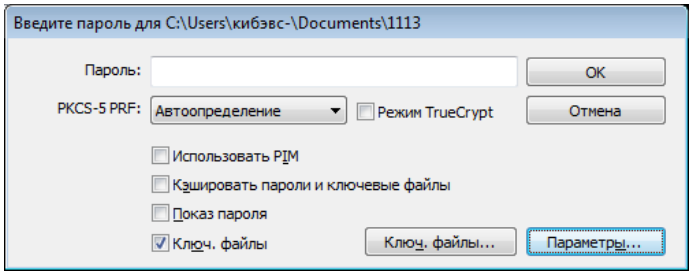


Рисунок 17 – Выбор ключевого файла

Дождитесь завершение монтирования тома. После того, как процесс завершится, диск станет доступен и его можно использовать как обычный локальный диск (рисунок 18).

Бывают ситуации, когда диск необходимо смонтировать том как сменный носитель. Для этого необходимо поставить отметку в окне параметров, нажав кнопку «Параметры» в окне ввода пароля.

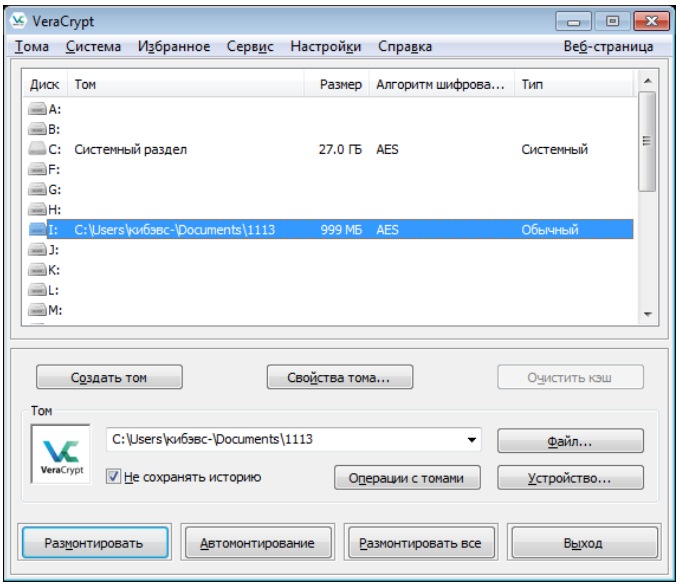


Рисунок 18 – Смонтированный раздел

После завершения работы с контейнером, его следует размонтировать в целях повышения безопасности.

Откройте ваш ключевой файл и убедитесь, что файл не был изменен.

2.2 Шифрования раздела жесткого диска

Откроем мастер томов, как и в разделе 2.1, и выберем «Зашифровать несистемный раздел/диск» (рисунок 19).

Программа может шифровать не только раздел жесткого диска или полностью жесткий диск, но и внешние накопители.

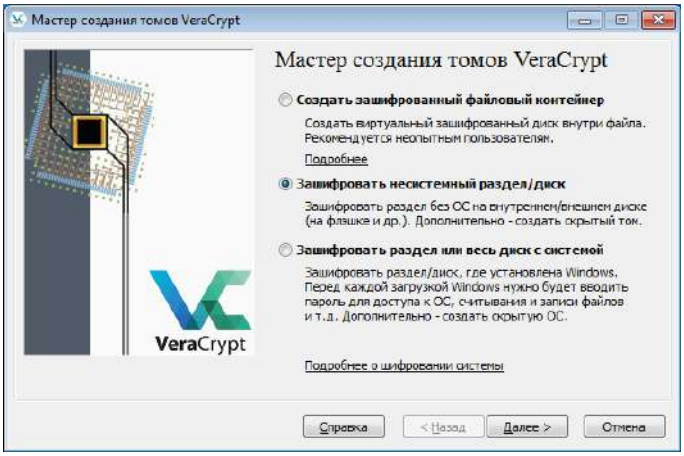


Рисунок 19 – Мастер создания томов

В этот раз выберем «Скрытый том VeraCrypt» (рисунок 20).

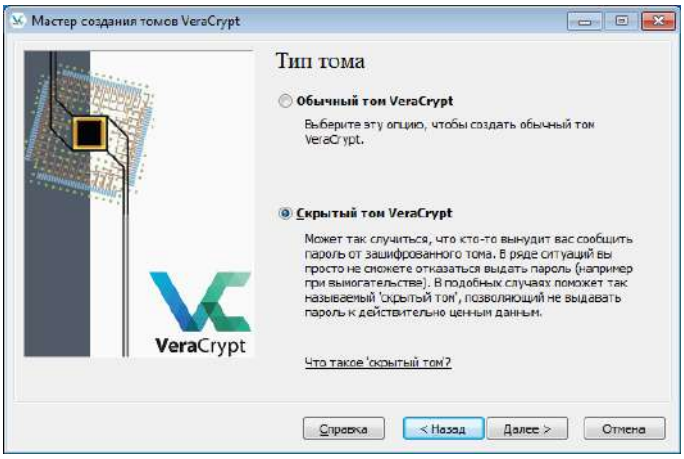


Рисунок 20 – Тип тома

Выберем обычный режим (рисунок 21).

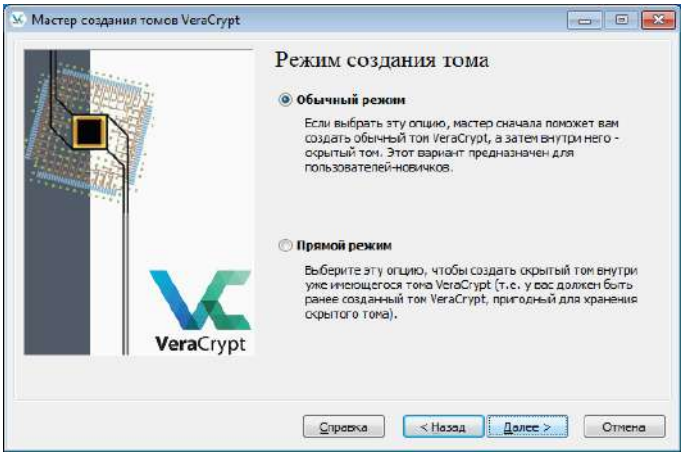


Рисунок 21 – Выбор режима

Выберем диск, который будем шифровать (рисунок 22). В нашем случаи — это диск E.

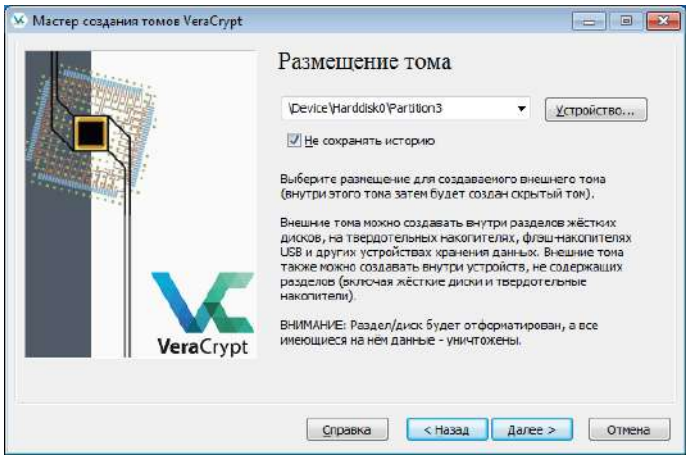


Рисунок 22 – Выбор диска

Нажмем кнопку «Далее» (рисунок 23).

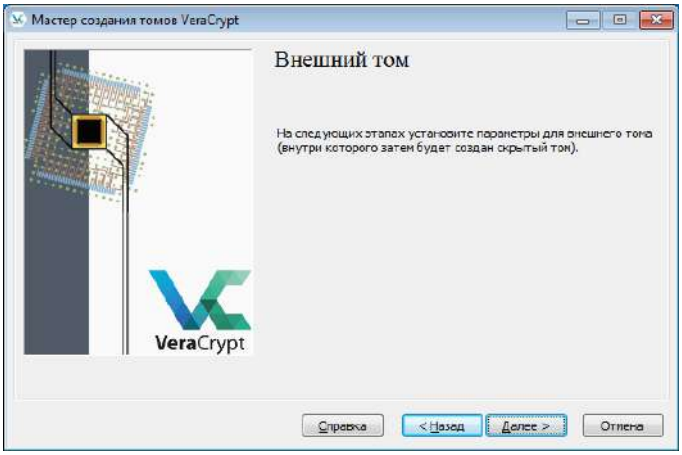


Рисунок 23 - Предупреждение

Выберем алгоритм шифрования в соответствии с вариантом и проверим алгоритм, как в пункте 2.1 (рисунок 24).

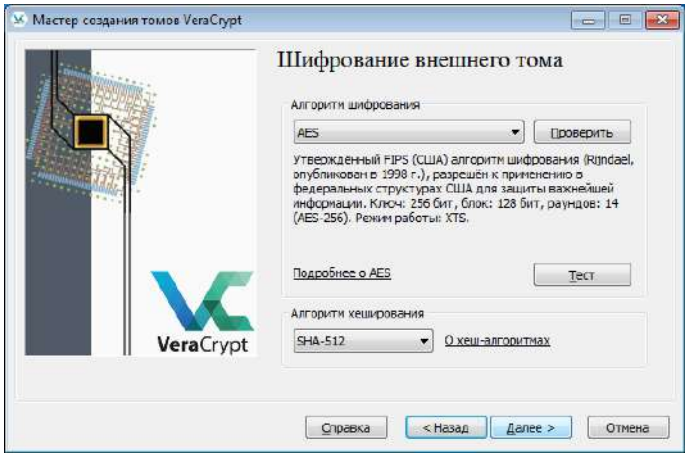


Рисунок 24 – Алгоритм шифрования

Внешний том нанимает все доступное пространство. Нажмем кнопку «Далее» (рисунок 25).

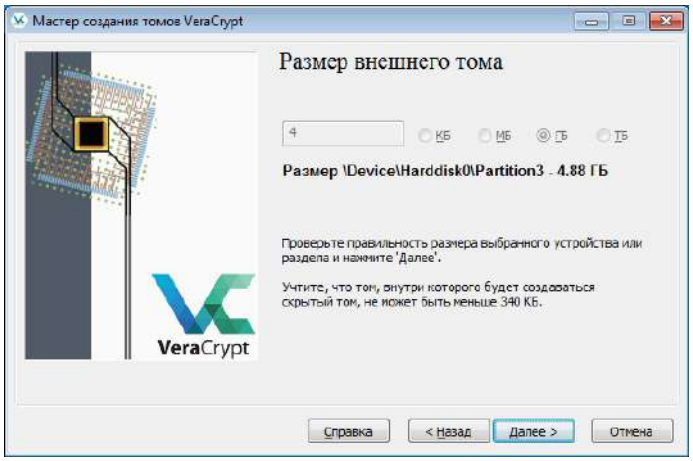


Рисунок 25 – Выбор размера тома

В этот раз введем просто пароль (рисунок 26).

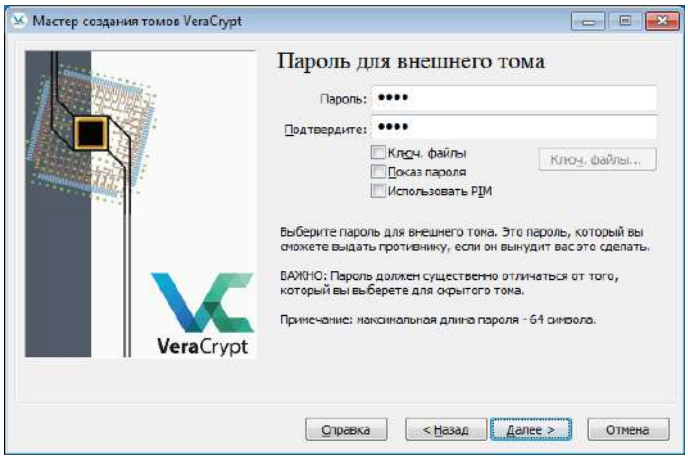


Рисунок 26 – Ввод пароля

Прочтем предупреждение и поставим отметку «Да» (рисунок 27).

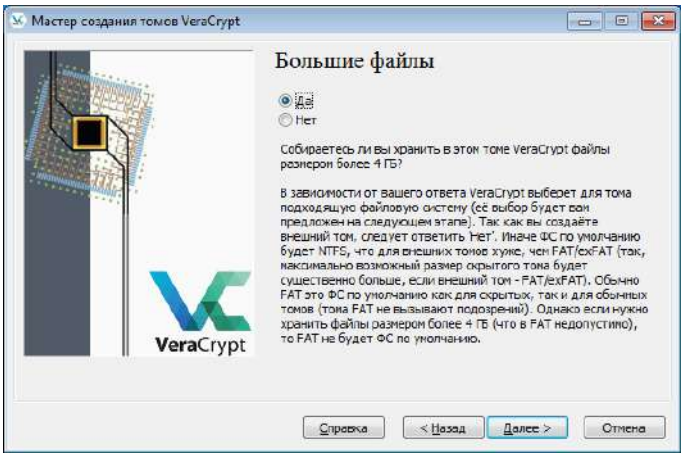


Рисунок 27 - Предупреждение

Выберите файловую систему NTFS, заполните энтропию и нажмите кнопку «Разметка» (рисунок 28).

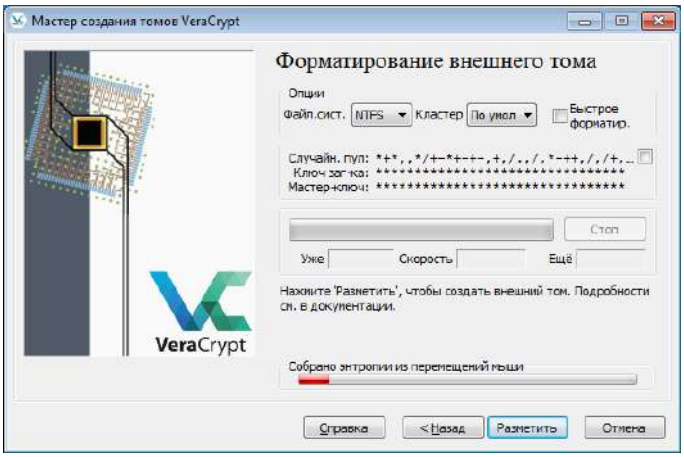


Рисунок 28 - Разметка

Прочтите предупреждение и нажмите кнопку «Да» (рисунок 29).

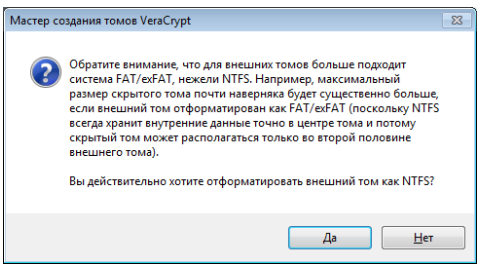


Рисунок 29 - Предупреждение

Дождитесь завершения разметки диска (рисунок 30).

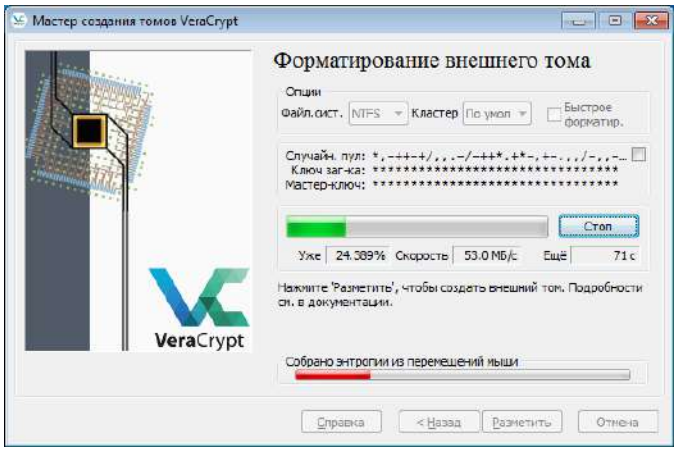


Рисунок 30 – Процесс разметки диска

После завершения разметки будет показан информационный раздел о работе с внешним томом. Нажмите кнопку «Далее» (рисунок 31).

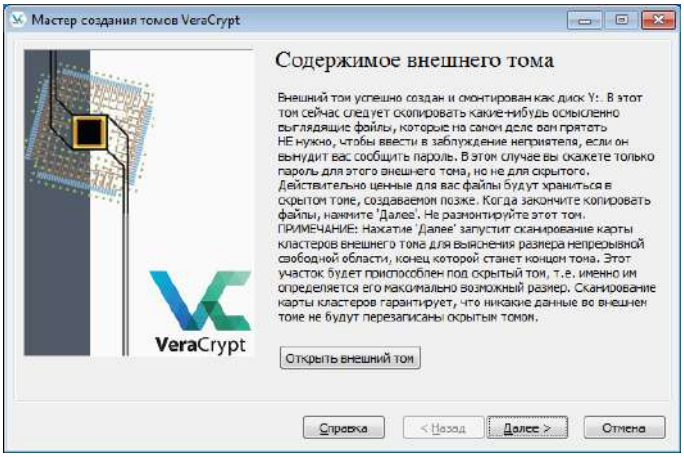


Рисунок 31 – Информационная страница

Далее мастер создания томов предложит настроить скрытый том. Нажмите кнопку «Далее» (рисунок 32).

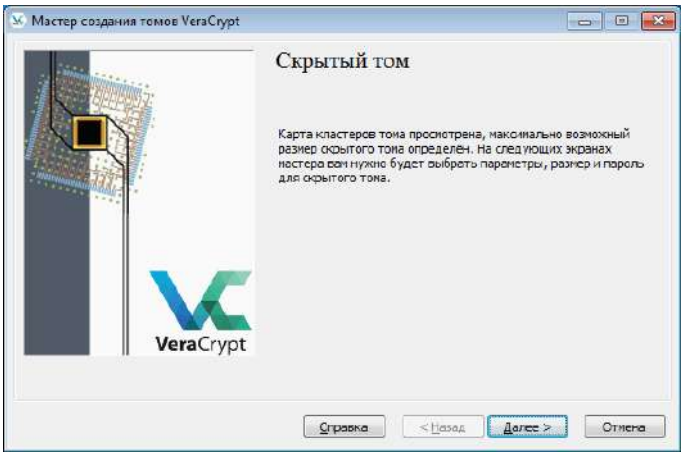


Рисунок 32 – Скрытый том

Выберите алгоритм шифрования, который выбрали для внешнего тома, и нажмите «Далее» (рисунок 33).

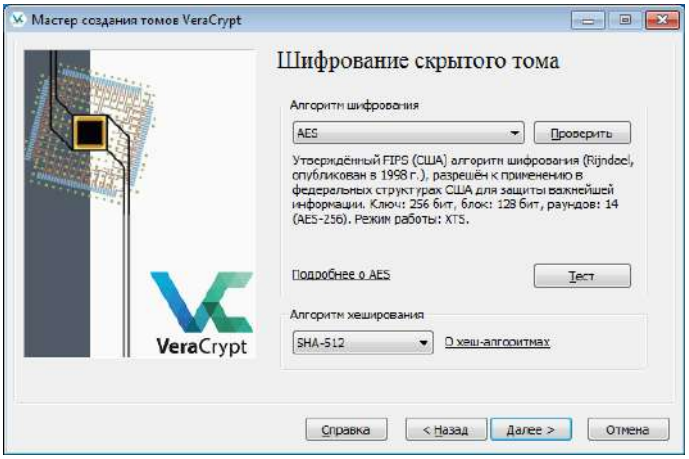


Рисунок 33 – Шифрование скрытого тома

Далее введите пароль, отличный от пароля для внешнего тома, и нажмите кнопку «Далее» (рисунок 34).

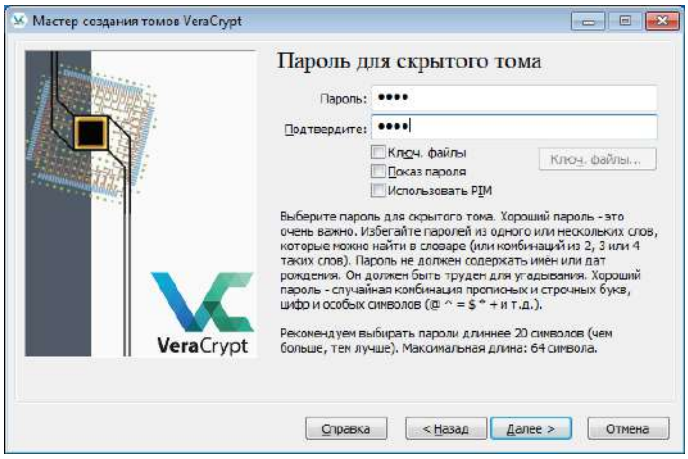


Рисунок 34 – Пароль для скрытого тома

Соберите энтропию и выполните разметку тома (рисунок 35).

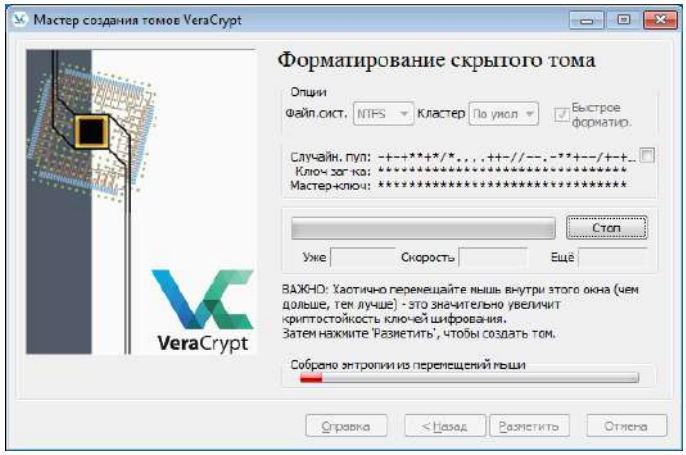


Рисунок 35 – Форматирование скрытого тома

Далее прочитайте выпадающие сообщения и согласитесь с ними. После этого будет выдано окно успешного создания скрытого тома (рисунок 36).

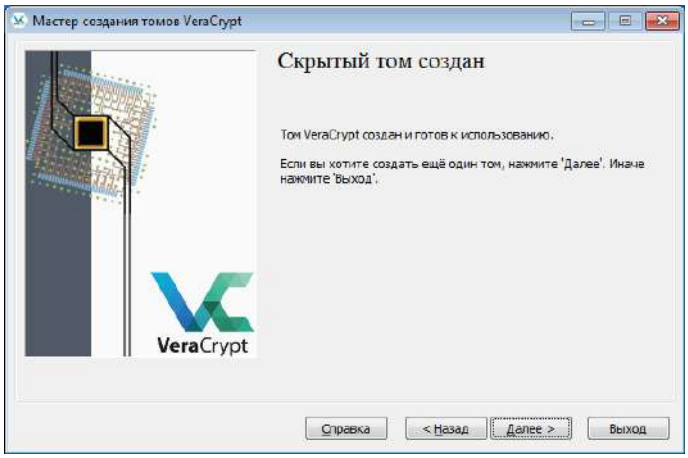


Рисунок 36 – Успешное создание скрытого тома

Работа с внешним и скрытым томом аналогична работе с файловым контейнером, но при инициализации тома необходимо ввести пароль от тома, который хотите открыть, от внешнего или скрытого.

2.3 Шифрование системного диска

В окне создания томов выберите раздел «Шифровать раздел или весь диск с системой» (рисунок 37).

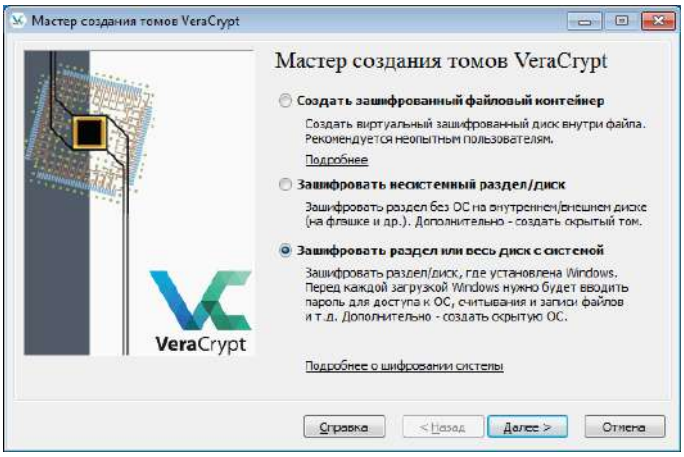


Рисунок 37 – Шифрование системного диска

Есть два типа шифрования системы – скрытый или обычный. В случаи с обычным типом системный диск будет полностью зашифрован и при загрузке компьютера будет предложено ввести пароль.

В случаи с скрытым будет создан поддельный системный раздел куда пользователь должен установить систему и загрузить неважные файлы.

Главное отличие этих двух типов в том, что если вас вынудят сообщить пароль, то вы можете сказать пароль от поддельного системного диска. В этом случаи злоумышленнику потребуется гораздо больше усилий (а может это все еще невозможно на текущий момент), чтобы понять, что существует еще одна система.

Мы выберем обычный тип шифрования (рисунок 38).

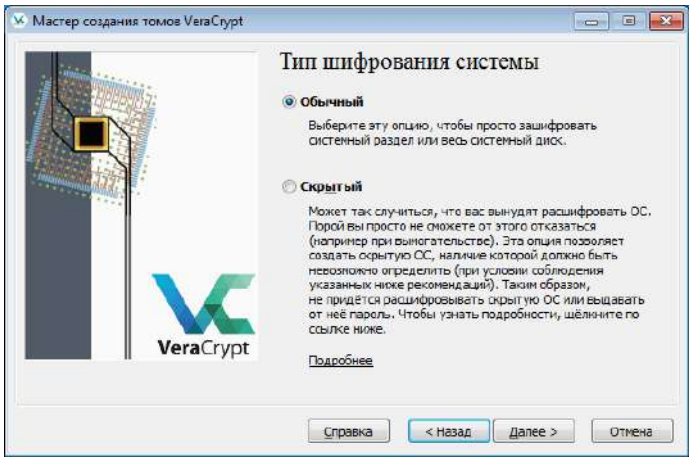


Рисунок 38 – Тип шифрования системы

Далее необходимо выбрать пункт «Зашифровать систем раздел Windows» и нажать кнопку «Далее» (рисунок 39).

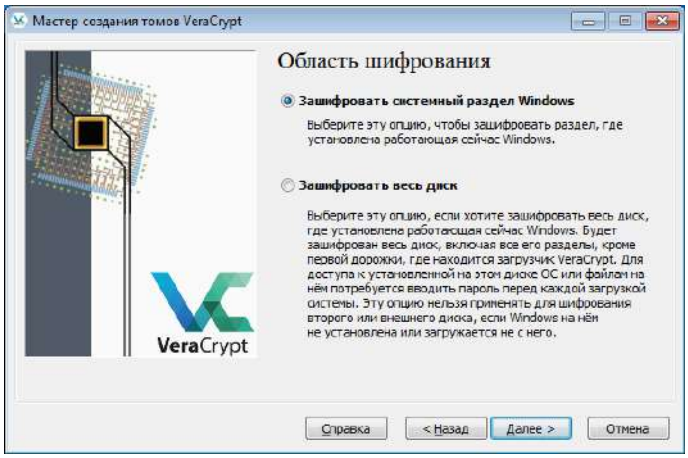


Рисунок 39 – Область шифрования

В нашем случаи установлена одна Windows, следовательно, нужно выбрать пункт «Одиночная загрузка» (рисунок 40).

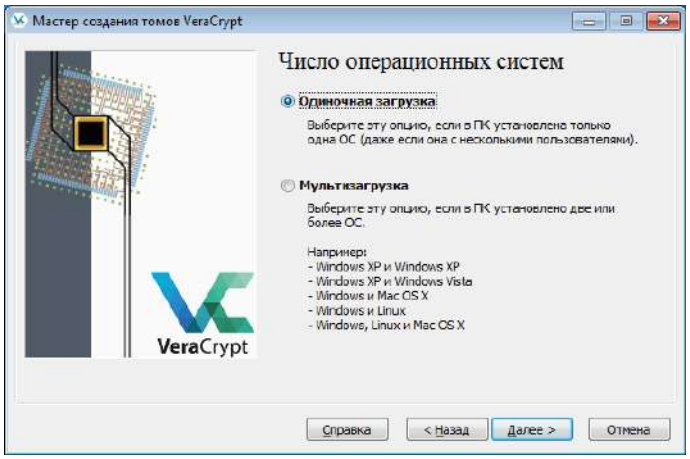


Рисунок 40 – Число операционных систем

Далее следует оставить настройки шифрования по умолчанию (рисунок 41).

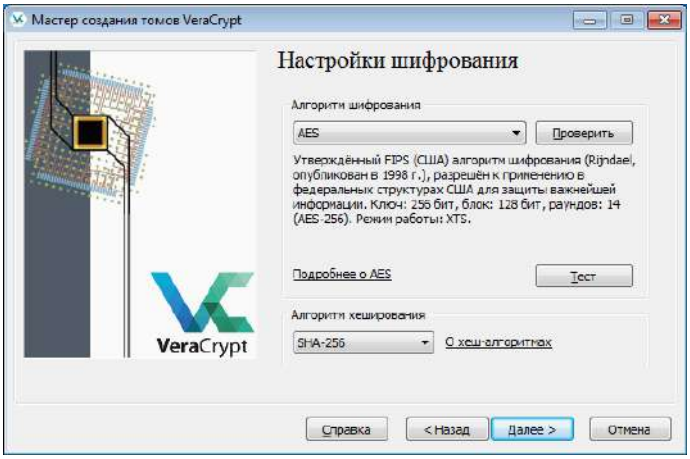


Рисунок 41 – Настройки шифрования

Поставьте галочку на пункте «Использовать PIM» и введите пароль и PIM (рисунок 42).

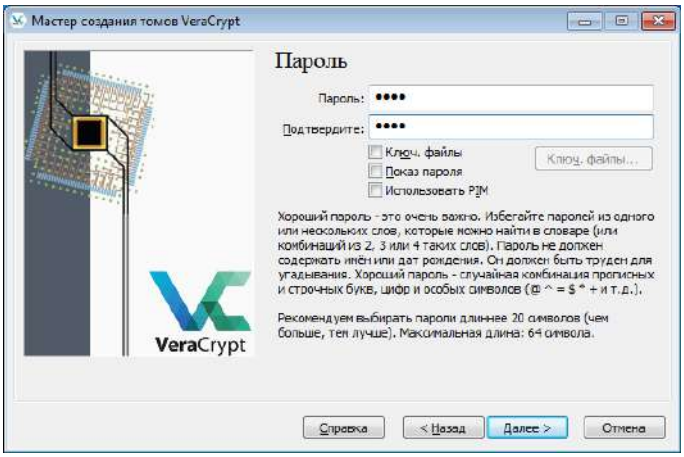


Рисунок 42 – Ввод пароля

Дайте программе собрать энтропию и нажмите кнопку «Далее» (рисунок 43).

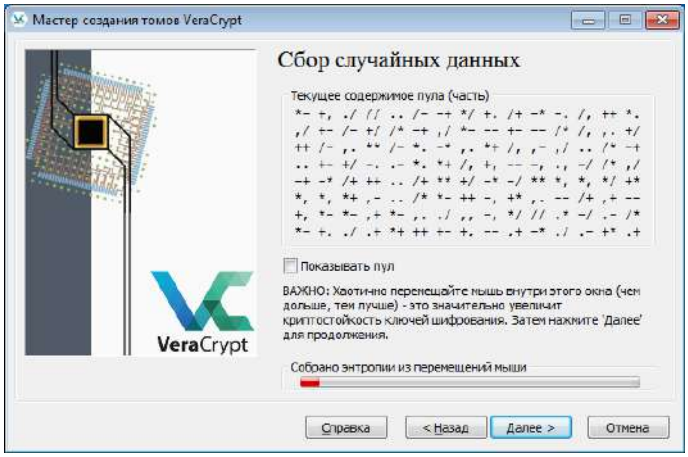


Рисунок 43 – Сбор случайных данных

В случаи успешного создания ключей, нажмите кнопку «Далее» (рисунок 44).

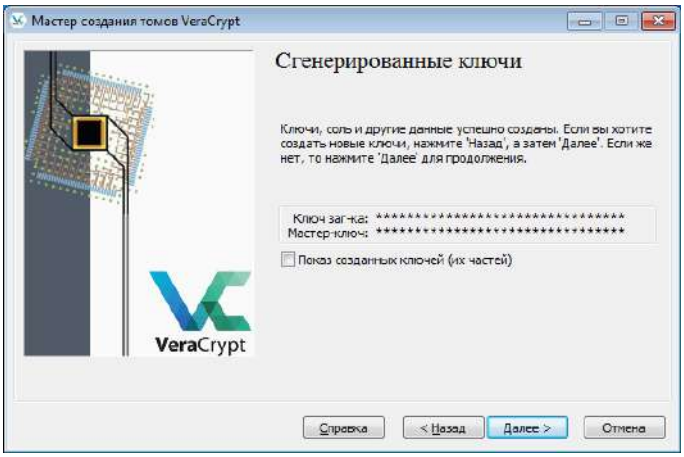


Рисунок 44 – Сгенерированные ключи

В случаи, если утрачен доступа к системе, необходимо будет предоставить диск восстановления для восстановления доступа. Рекомендуется тщательно спрятать его.

Для создания выберете путь хранения диска и нажмите «Далее» (рисунок 45).

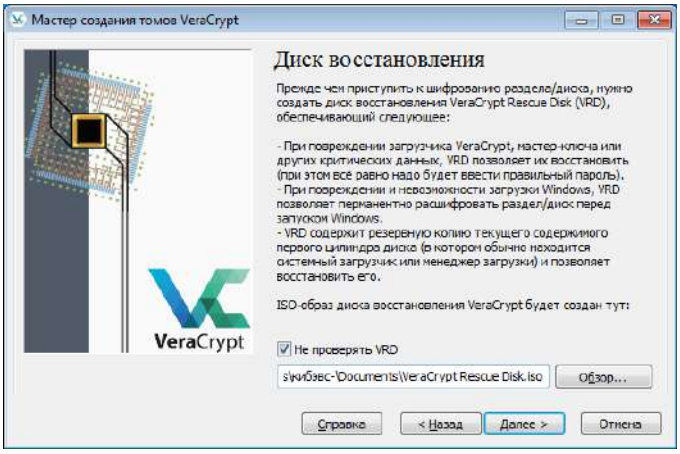


Рисунок 45 – Создания диска восстановления

После успешного создания диска восстановления будет показано соответствующее окно, где будет предложено прожечь диск восстановления на компакт-диск. Нажмите кнопку «Далее» (рисунок 46).

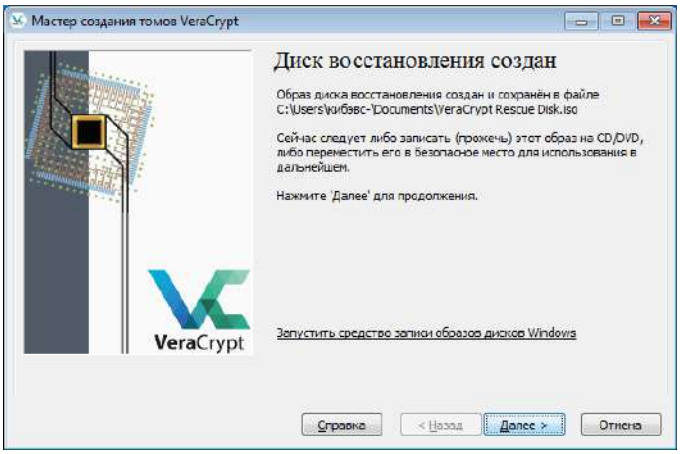


Рисунок 46 – Успешное создание образа восстановления

Внимательно ознакомьтесь с предупреждением и нажмите кнопку «Да» (рисунок 47).

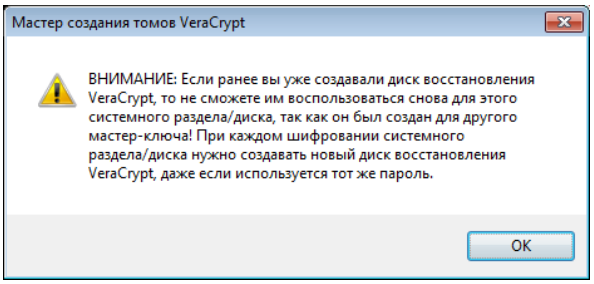


Рисунок 47 – Предупреждение

Следующим шагом будет выбор режима очистки диска. Очистка необходима в связи с особенностью хранения информации на диске. При удалении какого-либо файла с диска, фактически он не удаляется, а обнуляются только указатели на этот файл. Процедура очистки заключается в многократной перезаписи псевдослучайной информации в ячейки памяти жесткого (или какого-либо другого) диска, что затрудняет считывание остаточной незашифрованной информации с диска. Следовательно, если не провести эту процедуру, то физически на диске останутся незашифрованные данные.

В нашем случаи необходимо отказаться от очистки, выбрав из выпадающего меню пункт «Нет» (рисунок 48).

Следует учесть, что сейчас очень популярны SSD накопители. Они имеют меньше циклов записи. В связи с этим стоит подумать, нужно ли вам выполнять эту процедуру, если, например, была переустановлена ОС, но до

этого системный диск был зашифрован программой VeraCrypt и доступ не был скомпрометирован.

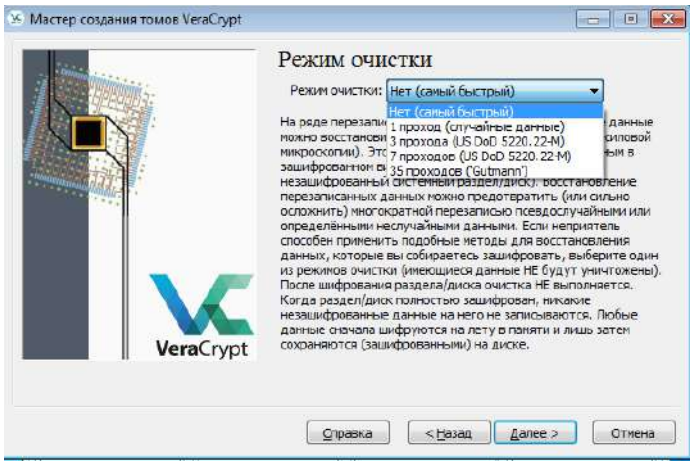


Рисунок 48 – Режим очистки

Следующим шагом необходимо провести тестирование на ошибки, которые могут возникнуть во время шифрования. Нажмите кнопку «Тест» (рисунок 49) и прочитайте предупреждение. Нажмите кнопку «Да» в окне предупреждения (рисунок 50).

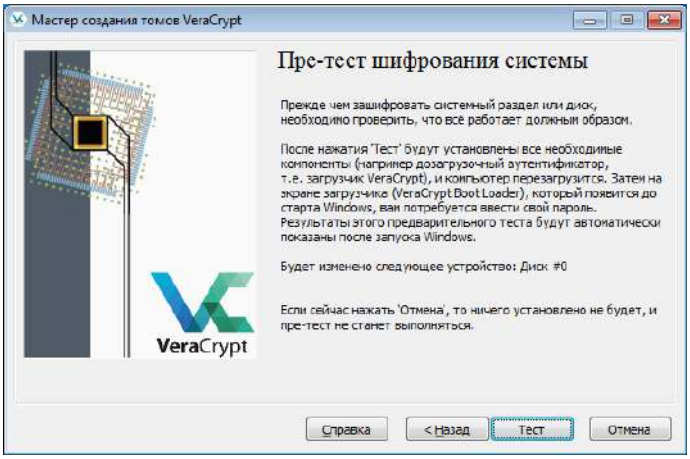


Рисунок 49 – Пре-тест

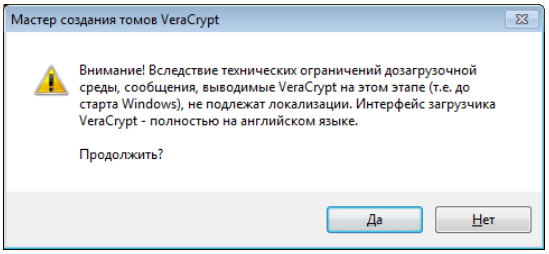


Рисунок 50 – Предупреждение

Прочитайте информационное сообщение и нажмите кнопку «ОК» (рисунок 51).

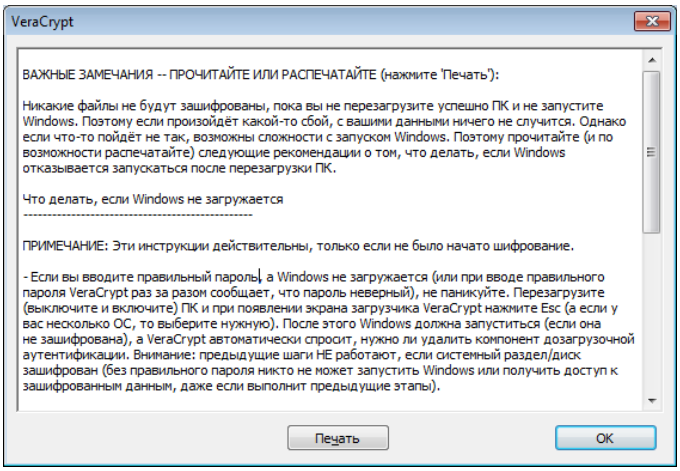


Рисунок 51 – Информационное сообщение

Выполните перезагрузку нажав кнопку «Да» (рисунок 52).

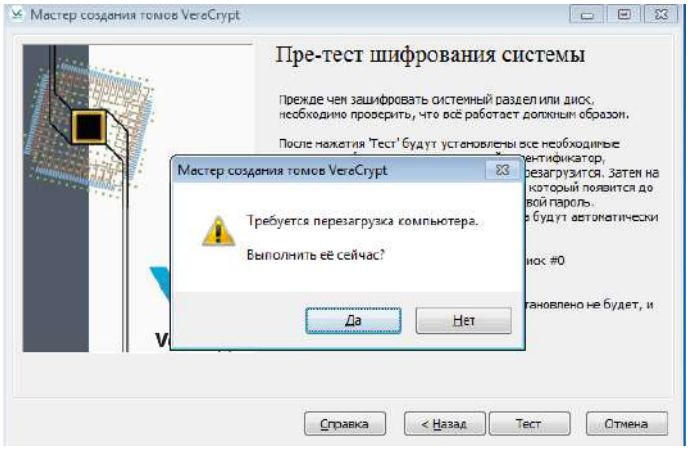


Рисунок 52 – Перезагрузка

В окне, показанном на рисунке 53, введите пароль и PIM от системы шифрования.

Рисунок 53 – Ввод паролей

Дождитесь, пока система не загрузится (рисунок 54).

Вам будет казаться, что все подвисло и ничего не работает, но это не так. Обязательно дождитесь загрузки системы или ошибки.

Рисунок 54 – Пароли введены

После того, как система будет загружена, появится сообщение о успешном прохождении пре-теста. Прочитайте информационное сообщение и нажмите на кнопку «Шифрация» (рисунок 55).

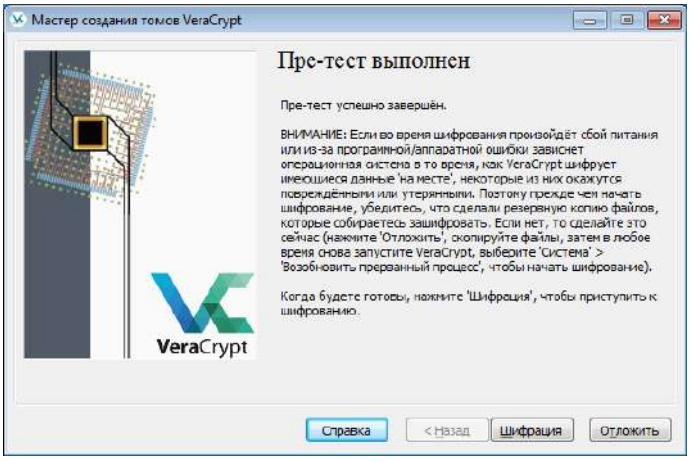


Рисунок 55 – Успешное выполнение пре-теста

Шифрование может занять некоторое время. Обязательно дождитесь окончания этого процесса (рисунок 56).

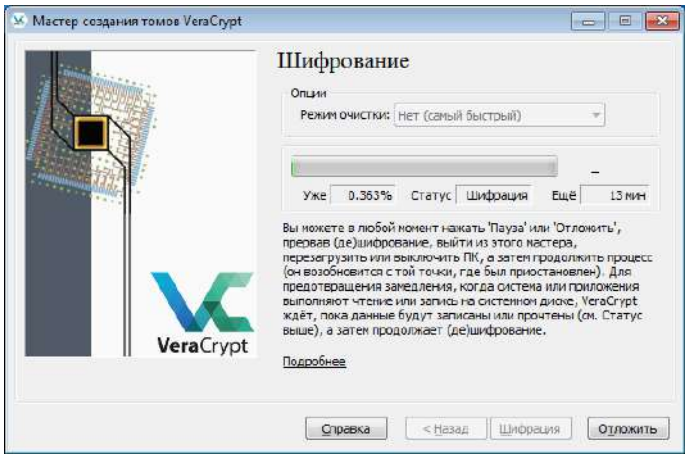


Рисунок 56 – Процесс шифрования системного диска

После успешного шифрования будет выдано соответствующее сообщение (рисунок 57).

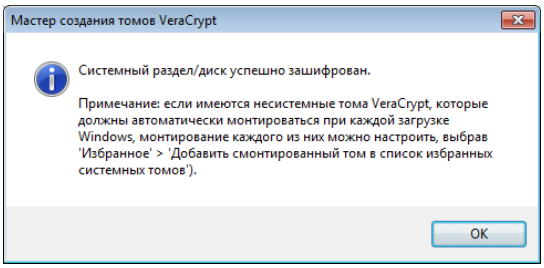


Рисунок 57 – Успешное шифрование системного диска

Перезагрузитесь, введите пароль и PIM (рисунок 58).

Рисунок 58 – Введенный пароль и PIM

Откройте программу VeraCrypt и посмотрите, как отображается в ней диск C (рисунок 59).

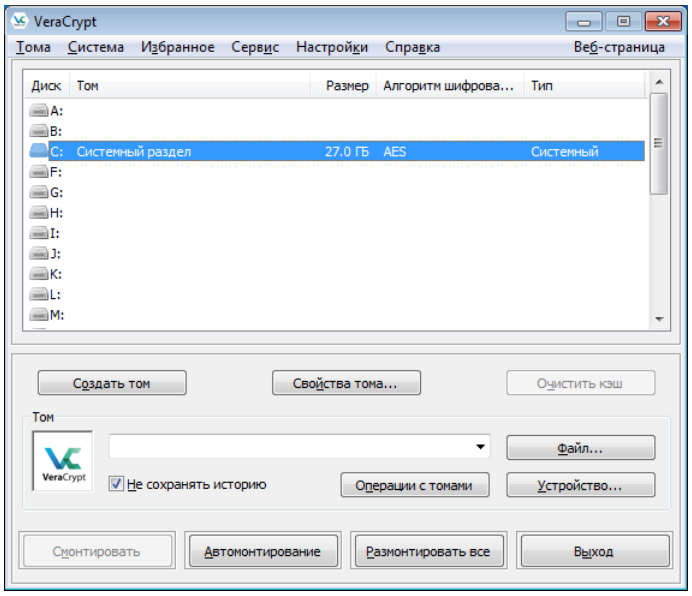


Рисунок 59 – Отображение диска C в программе

3 Варианты

Вариант	Файловый контейнер	Шифрование диска
1	AES	AES(Twofish)
2	Serpent	AES(Whofish(Serpent))
3	Twofish	Camellia
4	Camellia	Kuznyechik
5	Kuznyechik	Serpent
6	AES(Twofish)	Twofish
7	AES(Whofish(Serpent))	AES
8	Serpent(AES)	Kuznyechik(Serpent(Camellia))
9	Twofish(Serpent)	Camellia(Serpent)
10	Camellia(Kuznyechik)	Kuznyechik(AES)
11	Kuznyechik(Twofish)	Camellia(Kuznyechik)
12	Camellia(Serpent)	Kuznyechik(Twofish)
13	Kuznyechik(AES)	Serpent(AES)
14	Kuznyechik(Serpent(Camellia))	Twofish(Serpent)

Контрольные вопросы

1. Что такое файловый контейнер?
2. Чем отличается скрытый том от обычного?
3. Какой алгоритм шифрования, на ваш взгляд, предпочтительнее?
4. Для чего необходима очистка диска при шифровании системного диска?
5. Как подключить зашифрованный диск (системный, локальный том, файловый контейнер)?
6. Что такое PIM?
7. Какие плюсы и минусы использования ключевых файлов?
8. Что такое скрытая ОС?
9. Что будет, если в обычный записать сильно много информации и в скрытый? Как это на них отразится?

Лабораторная работа № 15
Анализ защищенности сетевых протоколов

Цель работы

В результате работы необходимо научиться использовать анализатор трафика Wireshark как средство перехвата информации и средство анализа защищенности сетевых протоколов.

Теоретические сведения

Sniffer (от англ. to sniff – нюхать) – это сетевой анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов.

Снифферы применяются как в благих, так и в деструктивных целях. Анализ прошедшего через сниффер трафика, позволяет:

- Отслеживать сетевую активность приложений.
- Отлаживать протоколы сетевых приложений.
- Локализовать неисправность или ошибку конфигурации.
- Обнаружить паразитный, вирусный и закольцованный трафик, наличие которого увеличивает нагрузку сетевого оборудования и каналов связи.
- Выявить в сети вредоносное и несанкционированное ПО, например, сетевые сканеры, флудеры, троянские программы, клиенты пиринговых сетей и другие.
- Перехватить любой незашифрованный (а порой и зашифрованный) пользовательский трафик с целью узнавания паролей и другой информации.

Wireshark – это программа для перехвата и анализа сетевого трафика. Используется она для сбора информации о сетевых взаимодействиях и для обнаружения и устранения неполадок в сети. Анализаторы трафика применяются при разработке новых протоколов и программного обеспечения.

Wireshark позволяет обнаружить и изучить любой протокольный блок данных (Protocol Data Unit, PDU), который был отправлен и получен с помощью установленных на компьютере сетевых адаптеров (Network Interface Card, NIC). По мере движения потоков данных по сети анализатор перехватывает каждый протокольный блок данных, после чего расшифровывает или анализирует его содержание согласно соответствующему документу RFC или другим спецификациям.

Анализатор трафика (сниффер) может анализировать только то, что проходит через его сетевую карту. Внутри одного сегмента сети Ethernet все пакеты рассылаются на все компьютеры сегмента. Использование коммутаторов (switch, switch-hub) и их грамотная конфигурация уже является защитой от прослушивания. Между сегментами информация передаётся через коммутаторы. Коммутация пакетов – форма передачи, при которой данные, разбитые на отдельные пакеты, могут пересылаться из исходного пункта в пункт назначения разными маршрутами. Если в другом сегменте внутри него передаются какие-либо пакеты, то в другой сегмент коммутатор эти данные не отправит.

Перехват трафика может осуществляться различными способами, а именно:

- обычным «прослушиванием» сетевого интерфейса (метод эффективен при использовании в сегменте концентраторов (хабов) вместо коммутаторов (свитчей), в противном случае метод малоэффективен, поскольку на сниффер попадают лишь отдельные фреймы);
- подключением сниффера в разрыв канала;
- ответвлением (программным или аппаратным) трафика и направлением его копии на сниффер;

- через анализ побочных электромагнитных излучений и восстановление таким образом прослушиваемого трафика;
- через атаку на канальном или сетевом уровне, приводящую к перенаправлению трафика жертвы или всего трафика сегмента на сниффер с последующим возвращением трафика в надлежащий адрес.

Ход работы

Для работы с программой Wireshark необходимо, само собой, ее установить. Это можно совершить, скачав установочный файл с официального сайта www.wireshark.org.

После установки запускаем программу. Встречает она пользователя следующим окном.

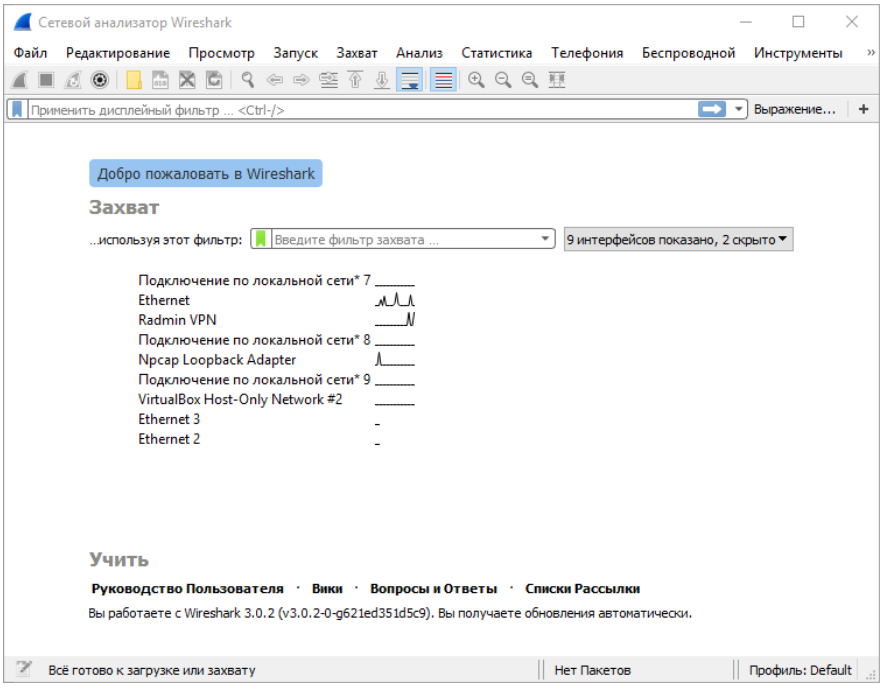


Рисунок 1 – Главное окно Wireshark

В самом центре мы можем увидеть список интерфейсов. Выберем наш основной сетевой интерфейс, по которому у нас идет Интернет-трафик (на рисунке он назван Ethernet, но на вашем устройстве его имя может быть другим).

После выбора интерфейса, Wireshark начнет перехватывать на нем пакеты.

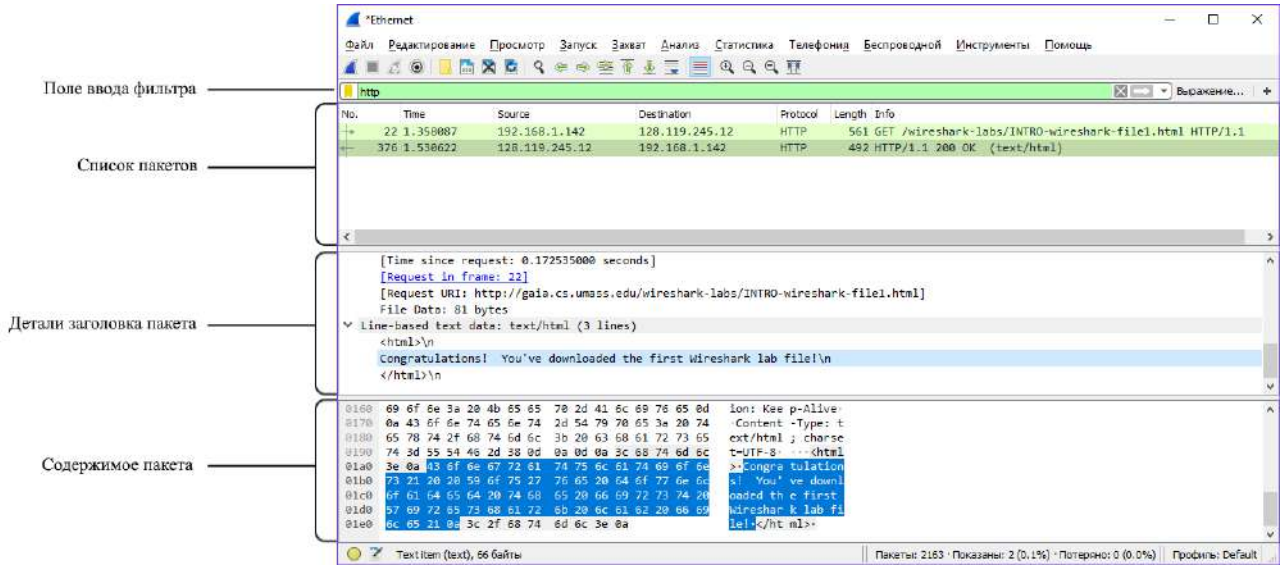


Рисунок 2 – Окно захвата и анализа пакетов

Окно захвата и анализа пакетов делится на 4 части:

- В поле ввода фильтра можно и нужно использовать различные фильтры для поиска необходимых пакетов с данными
- В списке пакетов указаны все захваченные пакеты, а также основная информация, такая как: время захвата, адрес отправителя, адрес получателя, тип протокола, длина пакета и служебная информация. Именно список пакетов можно отфильтровывать при помощи поля ввода фильтров.
- В окне деталей заголовка пакета указана подробная информация о выбранном пакете.
- В окне содержимого пакета содержится весь блок данных, который находится в пакете.

Давайте попробуем перехватить данные. Для этого запустим Захват (вкладка Захват – Старт) и откроем в браузере следующую страницу http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html.

После успешной загрузки страницы, останавливаем захват (вкладка Захват – Стоп) и путем фильтрации по протоколу http, найдем нужные нам пакеты.

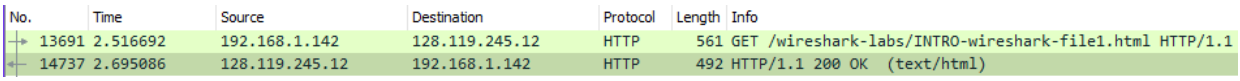


Рисунок 3 – Перехваченные пакеты

В панели захвата можно увидеть наш http-запрос. В Wireshark можно посмотреть его представление для протоколов различных уровней. Для этого кликнем на пакет и рассмотрим данные, указанные в панели заголовков пакета.

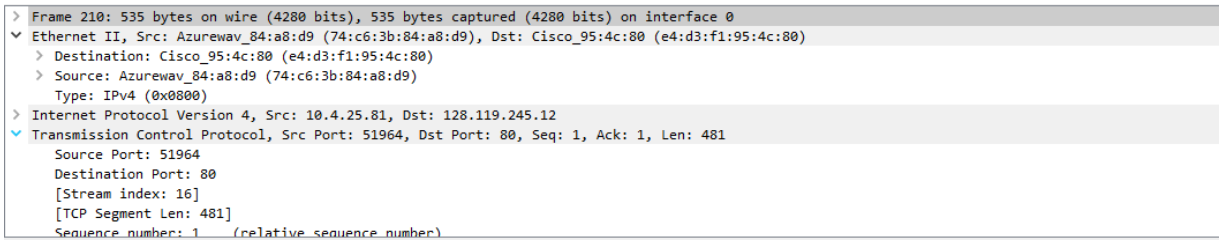


Рисунок 4 – Окно заголовка пакета

В первую очередь посмотрим на кадр Ethernet.

Таблица 1 – Заголовки кадра Ethernet

Преамбула	Адрес назначения	Адрес источника	Тип кадра	Данные	FCS
8 байт	6 байт	6 байт	2 байта	От 46 до 1500 байт	4 байта

В преамбуле пакета содержатся синхронизированные биты, обработанные сетевой платой. Они не показываются в захвате данных.

Адрес назначения - Cisco_95:4c:80 (e4:d3:f1:95:4c:80).

Адрес отправителя - Azurewav_84:a8:d9 (74:c6:3b:84:a8:d9).

Длина каждого адреса составляет 48 бит или 6 октетов, выраженных 12 цифрами в шестнадцатеричной системе. Общий формат — 12:34:56:78:9A:BC. Первые шесть шестнадцатеричных чисел обозначают производителя сетевой платы, а последние — ее серийный номер. Адрес назначения может быть

широковещательным (состоящим только из единиц) или индивидуальным (unicast). Адрес источника всегда должен быть индивидуальным адресом.

Тип кадра - IPv4 (0x0800).

В кадрах Ethernet II это поле содержит шестнадцатеричное значение, которое используется для указания типа протокола верхнего уровня в поле данных. Ethernet II поддерживает множество протоколов верхнего уровня.

Данные – IPv4.

Поле Данные содержит инкапсулированный протокол верхнего уровня. Поле данных в диапазоне от 46 до 1500 байт. В нашем случае, в нем находятся данные пакета протокола IP.

Теперь попробуем разобрать протокол IP.

Таблица 2 – Строение пакета IP

<table>
<tr><td>Номер версии
4 бита</td><td>Длина заголовка
4 бита</td><td>DSCP
6 бит</td><td>ECN
2 бита</td><td colspan="4">Общая длина
16 бит</td></tr>
<tr><td colspan="4" rowspan="2">Идентификатор пакета
16 бит</td><td colspan="3">Флаги
3 бита</td><td rowspan="2">Смещение фрагмента
13 бит</td></tr>
<tr><td></td><td>D</td><td>M</td></tr>
<tr><td>Время жизни
8 бит</td><td>Протокол верхнего уровня
8 бит</td><td colspan="6">Контрольная сумма
16 бит</td></tr>
<tr><td colspan="8">IP-адрес отправителя
32 бита</td></tr>
<tr><td colspan="8">IP-адрес получателя
32 бита</td></tr>
<tr><td colspan="8">Параметры и выравнивание</td></tr>
<tr><td colspan="8">Данные</td></tr>
</table>

Номер версии - Version: 4

Это первое поле, в котором указана версия протокола

Длина заголовка - Header Length: 20 bytes (5)

Длина заголовка, в данном случае она равна 20 байт.

DSCP - Differentiated Services Codepoint: Default (0)

DSCP используются для обозначения специального байта данных стандартного заголовка IP-пакета. Этот байт несет информацию о приоритете трафика. В нашем случае приоритет стандартный.

ECN - Explicit Congestion Notification: Not ECN-Capable Transport (0)

ECN позволяет обеим сторонам в сети узнавать о возникновении затора на маршруте к заданному хосту или сети без отбрасывания пакетов. Это дополнительная функция, которая используется только в том случае, когда обе конечные точки обмена информацией сообщают, что они хотят её использовать. В нашем случае указатель перегрузки не используется.

Общая длина - Total Length: 521.

Общая длина показывает размер IP-пакета в байтах.

Идентификатор пакета - Identification: 0x07a2 (1954).

Идентификатор пакета назначается отправителем пакета для корректной последовательности фрагментов при сборке пакета. Имеет смысл обращать внимание на идентификатор при фрагментации пакета, чего в нашем случае не было.

Флаги - Flags: 0x4000, Don't fragment

0... .... = Reserved bit: Not set

.1.. .... = Don't fragment: Set

..0. .... = More fragments: Not set

Флаги состоят из 3 битов. Первый бит должен быть равен нулю, второй сообщает о возможности фрагментации, а последний говорит о том, является ли наш пакет последним в цепочке.

Время жизни пакета - Time to live: 44.

TTL - число маршрутизаторов, которые может пройти этот пакет. При прохождении маршрутизатора это число уменьшается на единицу.

Протокол - Protocol: TCP (6).

Поле протокол показывает, данные какого протокола содержит пакет.

Контрольная сумма - Header checksum: 0xe0ff [validation disabled]

После того, как пакет был сформирован, для его заголовка была посчитана контрольная сумма.

IP-адрес отправителя - Source: 128.119.245.12.

IP-адрес получателя - Destination: 10.4.25.81.

Поля «Параметры» нет, потому что никакие опции и параметры не использовались.

В поле «Данные» содержатся данные.

Разберем структуру пакета протокола TCP.

Таблица 3 – Структура заголовка TCP

<table>
<tr><td colspan="3">Порт отправителя
32 бита</td><td>Порт получателя
32 бита</td></tr>
<tr><td colspan="4">Порядковый номер
32 бита</td></tr>
<tr><td colspan="4">Номер подтверждения
32 бита</td></tr>
<tr><td>Длина заголовка
4 бита</td><td>Зарезервировано
6 бит</td><td>Флаги
6 бит</td><td>Размер окна
16 бит</td></tr>
<tr><td colspan="2">Контрольная сумма
16 бит</td><td colspan="2">Указатель срочности
16 бит</td></tr>
<tr><td colspan="4">Параметры (необязательное поле)
32 бита</td></tr>
<tr><td colspan="4">Данные
32 бита</td></tr>
</table>

Порт отправителя - Source Port: 80

Содержит номер порта, который идентифицирует приложение клиента, с которого отправлены пакеты.

Порт назначения - Destination Port: 51964

Идентифицирует порт, на который отправлен пакет.

Порядковый номер - Sequence number: 1

Это поле показывает порядковый номер пакета при передаче. Именно поэтому принимающая система собирает пакеты именно так, как надо.

Номер подтверждения - Acknowledgment number: 482

Это поле показывает, на какой именно пакет отвечает удаленная система. В нашем случае – на пакет с Sequence Number = 482.

Длина заголовка - Header Length: 20 bytes.

Поле «Зарезервировано», собственно, представляет собою зарезервированные 6 бит для будущего использования.

Флаги - Flags: 0x018 (PSH, ACK).

Поле «Флаги» содержит 6 управляющих битов:

URG — поле «Указатель важности» задействовано

ACK — поле «Номер подтверждения» задействовано

PSH — инструктирует получателя протолкнуть данные, накопившиеся в приёмном буфере, в приложение пользователя

RST — оборвать соединения, сбросить буфер (очистка буфера)

SYN — синхронизация номеров последовательности

FIN — флаг, будучи установлен, указывает на завершение соединения.

Размер окна - Window size value: 237

Размер окна определяет количество байт данных, после передачи которых отправитель ожидает подтверждения от получателя, что данные получены.

Контрольная сумма - Checksum: 0xf781

Контрольная сумма – это 16-битное дополнение к сумме всех 16-битных слов заголовка и данных.

Указатель важности - Urgent pointer: 0

16-битовое значение положительного смещения от порядкового номера в данном сегменте. Это поле указывает порядковый номер октета, которым заканчиваются важные данные.

В ответ на компьютер приходит уже второй пакет. Это и есть тот ответ на запрос GET. В окне деталей заголовка и окне содержимого пакета можно увидеть текст из страницы в браузере.

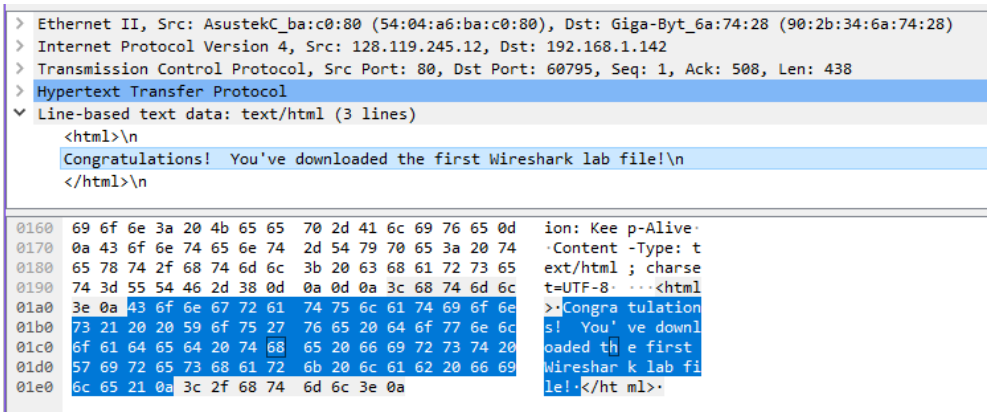


Рисунок 4 – Содержимое пакета

Попробуем отправить запрос PING и перехватить пакеты.

Поле фильтра в Wireshark также поддерживает логические выражения и операторы синтаксиса языка Си.

Список поддерживаемых операторов и выражений:

eq	==	равенство
ne	!=	не равно
gt	>	больше чем
Lt	<	меньше чем
ge	>=	больше равно
and	&&	логическое И
or	||	логическое ИЛИ
not	!	логическое НЕ

Также фильтры можно создавать через окно Выражений. Для этого нужно нажать на кнопку «Выражение...»

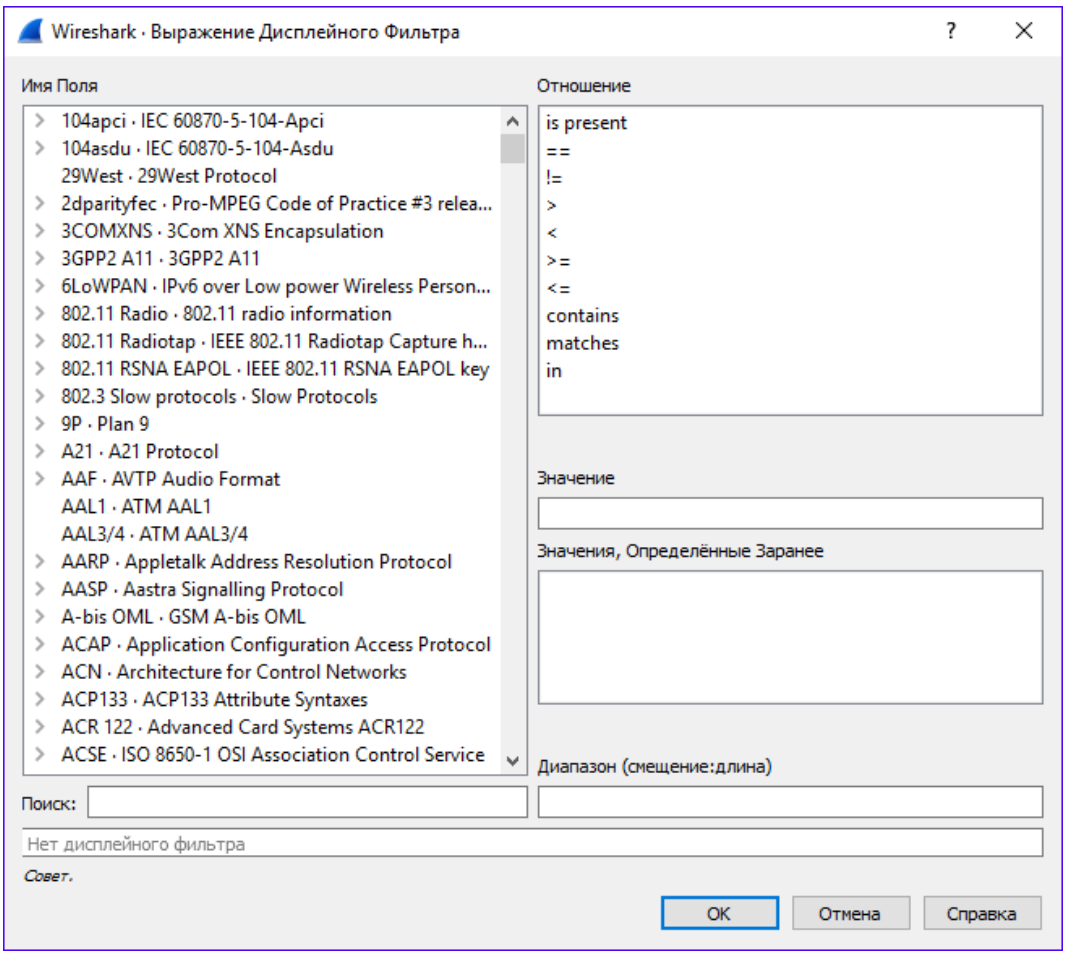


Рисунок 5 – Выражения

Попробуем в фильтр прописать следующее выражение: tcp.port == 80. После нажатия кнопки Enter будет выведен список пакетов, проходящих через 80 порт TCP. Этот порт предназначен для передачи данных по протоколу HTTP, поэтому они-то нам и будут выведены.

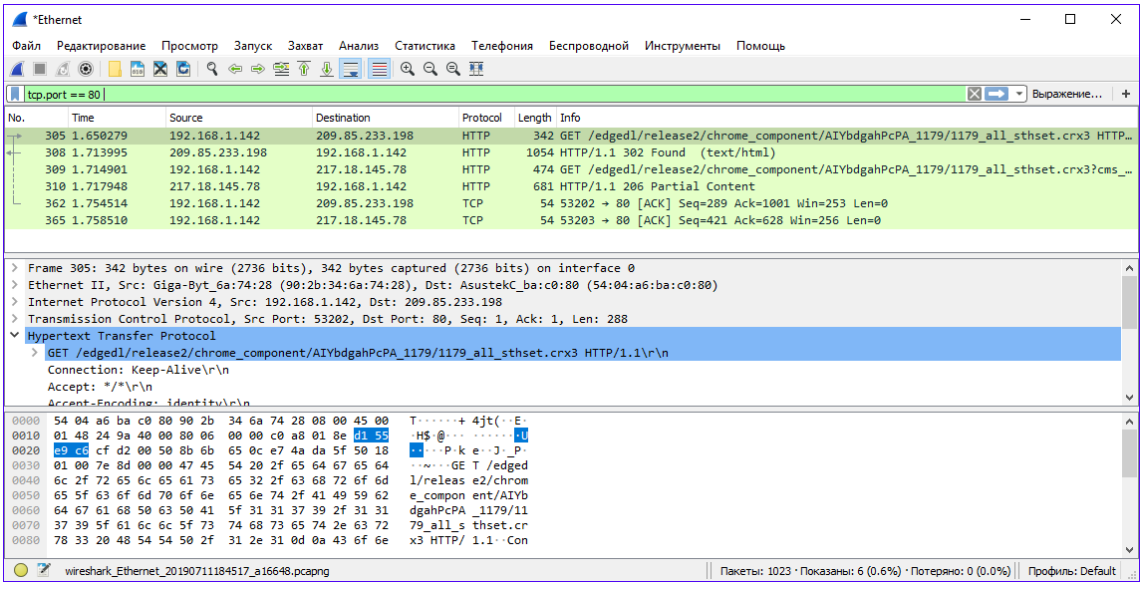


Рисунок 6 – Использование фильтра

Все захваченные пакеты можно сохранить в отдельный файл. Для этого достаточно выбрать Файл – Сохранить.

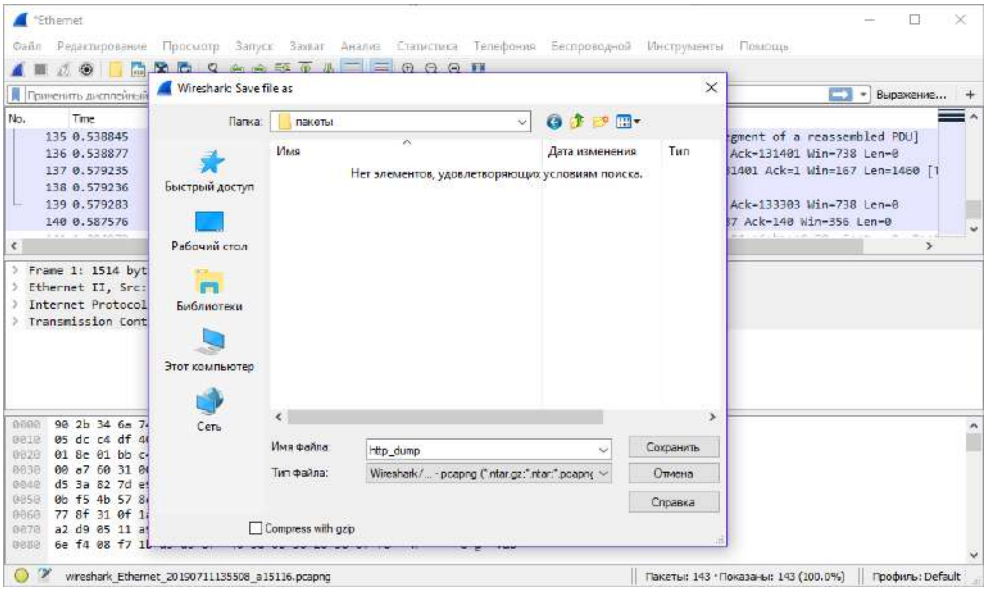


Рисунок 7 – Сохранение дампа

Попробуем перехватить логин и пароль, отправляемые через протокол HTTP. Для этого перейдем http://testing-ground.scraping.pro/login, запустим захват и введем логин и пароль в поля. После этого остановим захват пакетов.

Теперь отфильтруем пакеты по протоколу HTTP. Кликаем правой кнопкой мыши по первому пакету и выбираем Следовать – Поток HTTP.

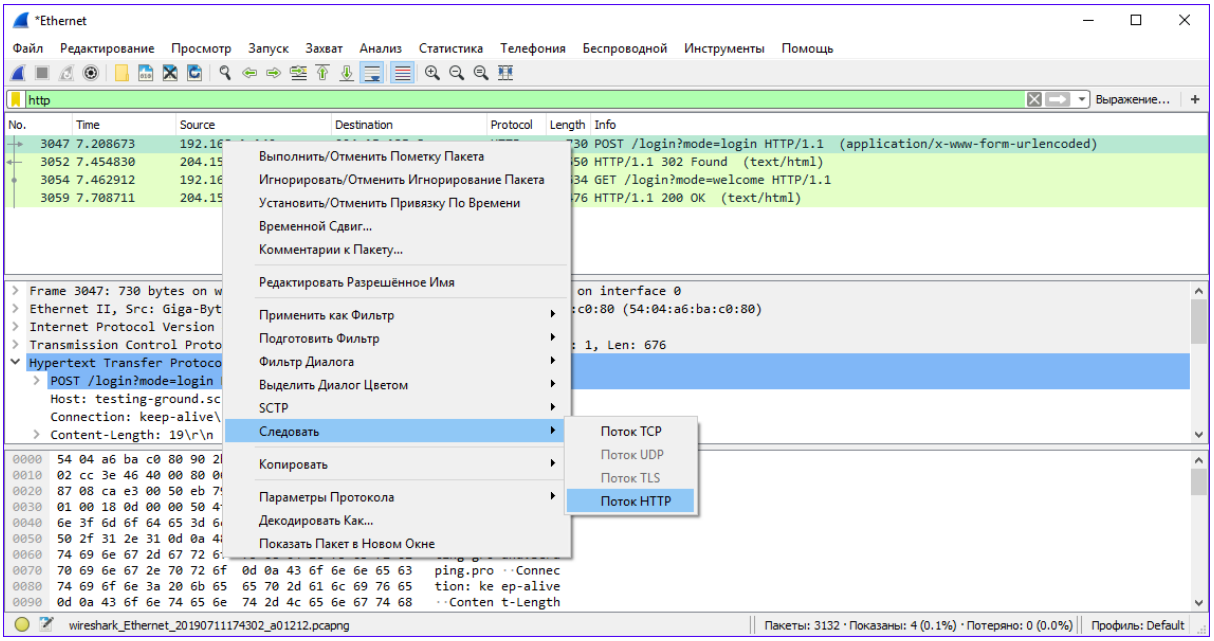


Рисунок 8 – Контекстное меню

Нам откроется окно со всеми HTTP-запросами и ответами на них, которые были переданы за эту сессию.

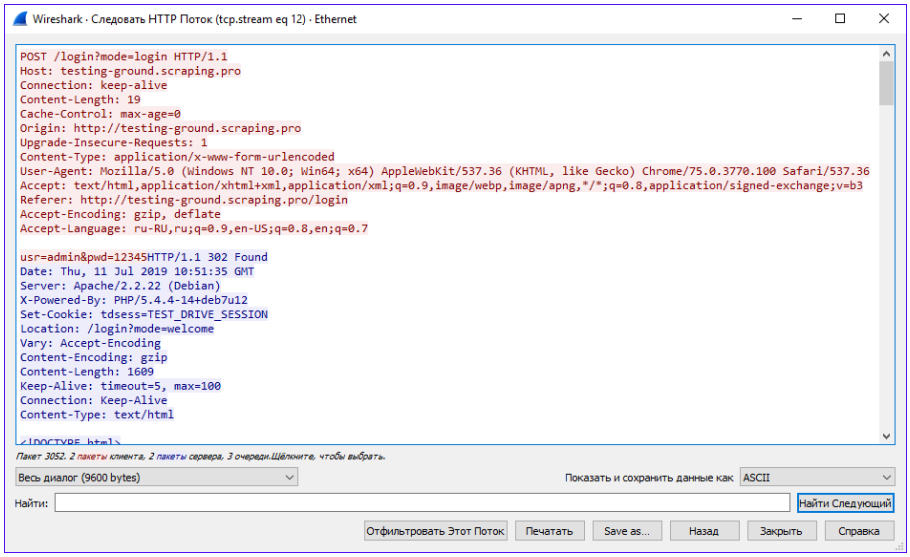


Рисунок 9 – HTTP Поток

Здесь нас интересует строка usr=admin&pwd=12345. Как можно заметить, логин и пароль на этой странице передаются путем запроса POST. Такие POST-запросы, как и GET-запросы, достаточно легко перехватить.

Попробуем вытянуть из перехваченных пакетов целый файл. Для этого воспользуемся FTP-сервером ftp://test.rebex.net/pub/example/ (при возможности можно воспользоваться другим). Запускаем захват, заходим на сервер под логином «demo» и паролем «password», после чего качаем любой из доступных нам файлов. После загрузки останавливаем захват пакетов.

Теперь отфильтруем наши пакеты по протоколу FTP. Кликаем правой кнопкой мыши по первому пакету и выбираем Следовать – Поток TCP.

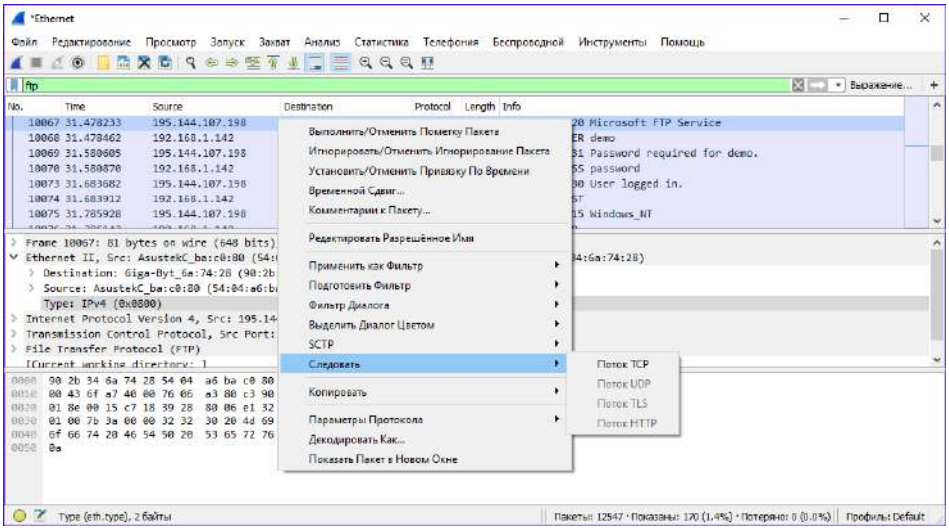


Рисунок 10 – Контекстное меню

Нам откроется окно со всеми FTP-командами и ответами на них, которые были переданы за эту сессию.

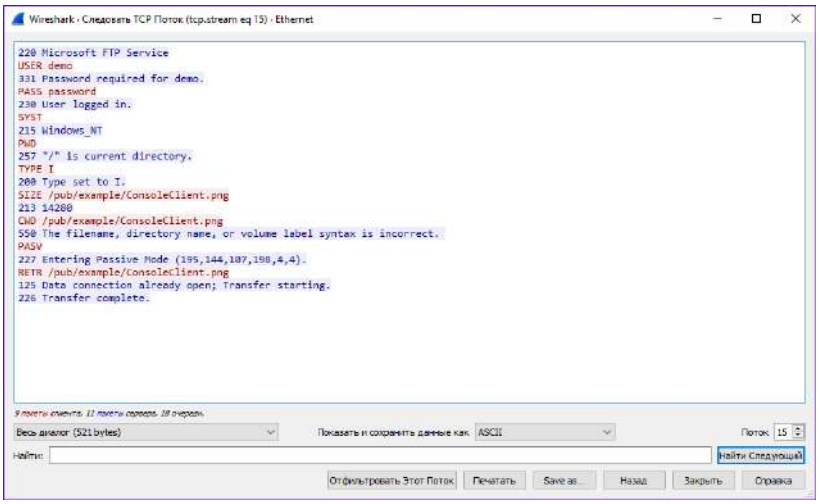


Рисунок 11 – TCP Поток

Из интересного мы можем здесь найти:

- USER demo – наш логин, который мы ввели.
- PASS password – пароль для этого логина
- SIZE /pub/example/ConsoleClient.png – запрос размера файла, который мы планируем скачать
- RETR /pub/example/ConsoleClient.png – запрос на загрузку данного файла.

Как можно было заметить, пользователем demo был скачан файл ConsoleClient формата png. Чтобы его получить, отфильтруем список пакетов по параметру ftp-data, найдем момент передачи файла (команда RETR) и откроем TCP Поток.

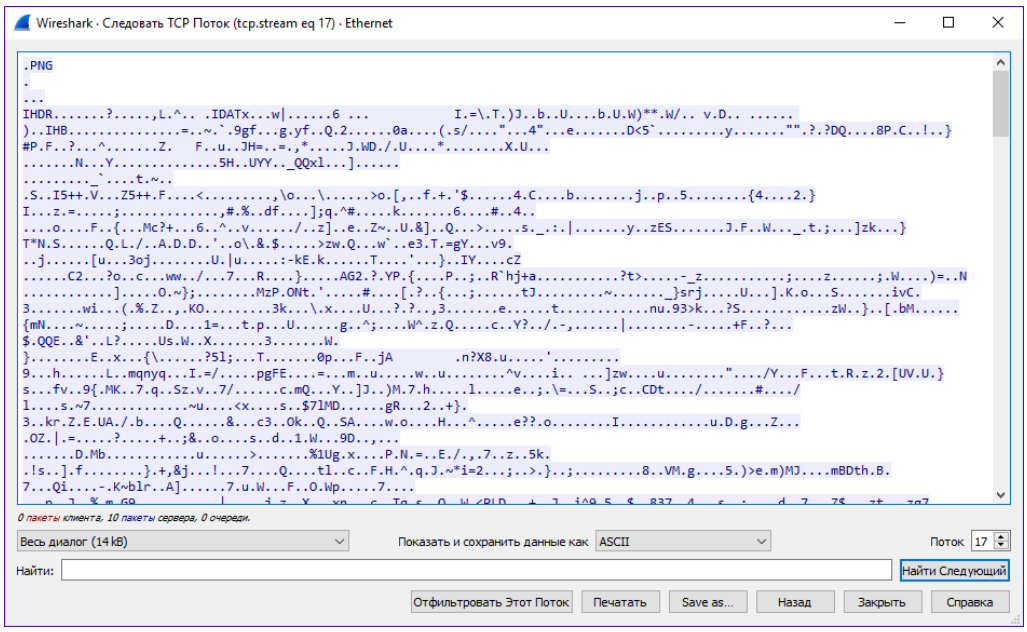


Рисунок 12 – TCP Поток

Нашему взору будет представлена каша из символов. Чтобы представить ее в виде картинки достаточно выбрать формат «Необработанный», нажать на кнопку «Save as…» и сохранить в любом удобном месте, указав расширение файла «.png».

В результате мы получил наше изображение.

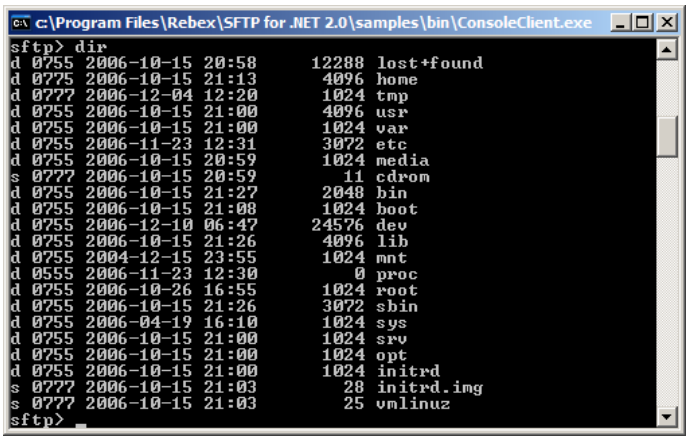


Рисунок 13 – Скачанное изображение

Попробуем перехватить почтовый трафик по протоколу POP3. Для этого используем любой почтовый клиент (в нашем случае JBMail). Включаем перехват и подключаемся к нашему серверу, используя логин и пароль. После чего подгрузиться список писем.

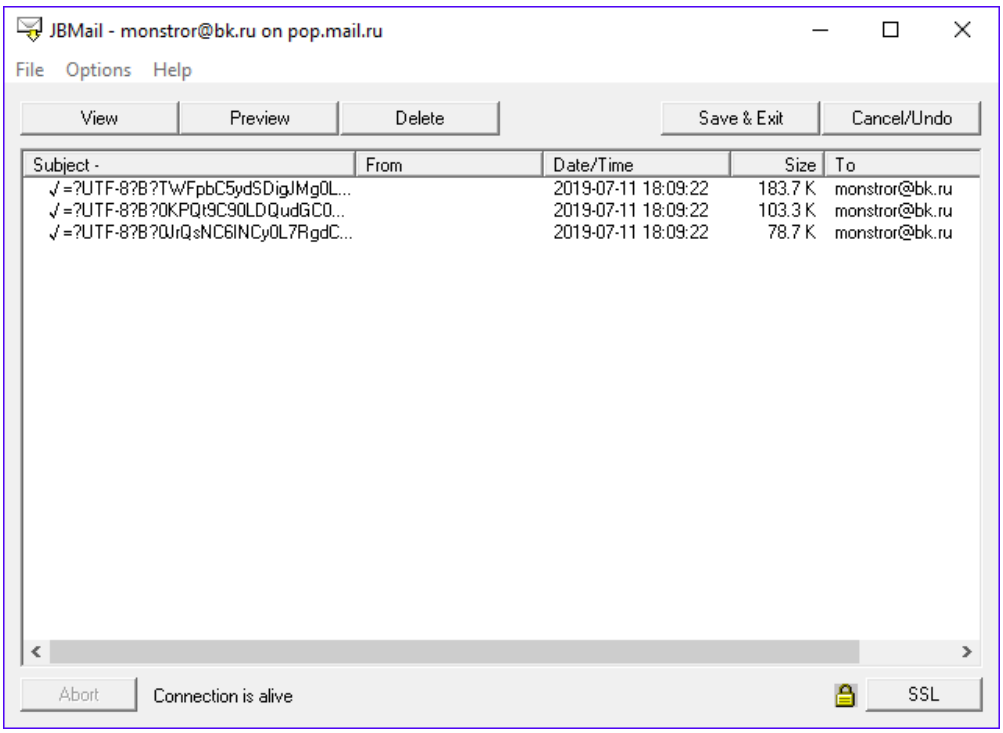


Рисунок 14 – Список писем в JBMail

Теперь открываем любое из них и останавливаем захват пакетов. Попробуем прочитать письма через перехваченные пакеты.

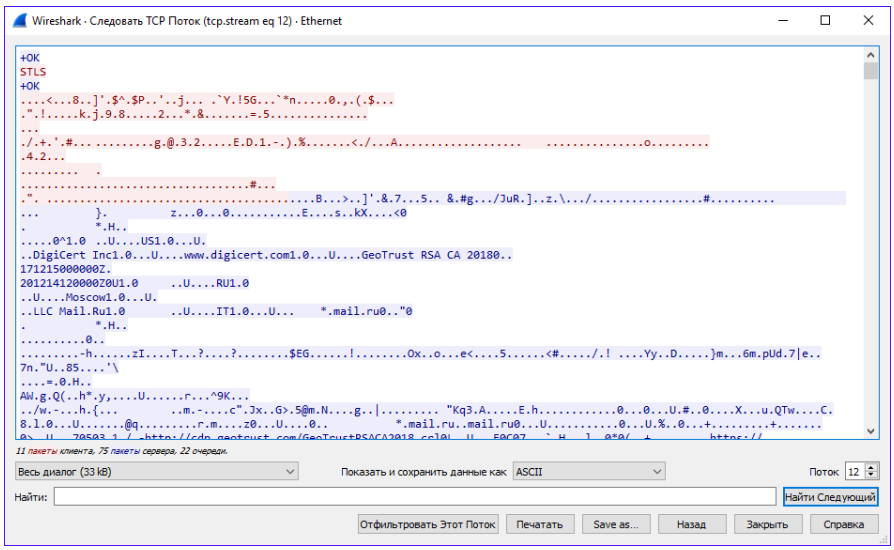


Рисунок 15 – Перехваченный поток

Здесь нас ждет подвох. Из всего потока можно разобрать лишь три первые команды. Вторая команда STLS запускает шифрование связи. Примерно то же самое ждет нас и в случае с IMAP-протоколом, так как практически все почтовые сервисы на сегодняшний день требуют обязательное шифрование для работы по этим протоколам.

Запустим командную строку и выполним команду ping 8.8.8.8, предварительно запустив захват пакетов.

Найдем наши пакеты по фильтру «ip.dst == 8.8.8.8 || ip.addr == 8.8.8.8».

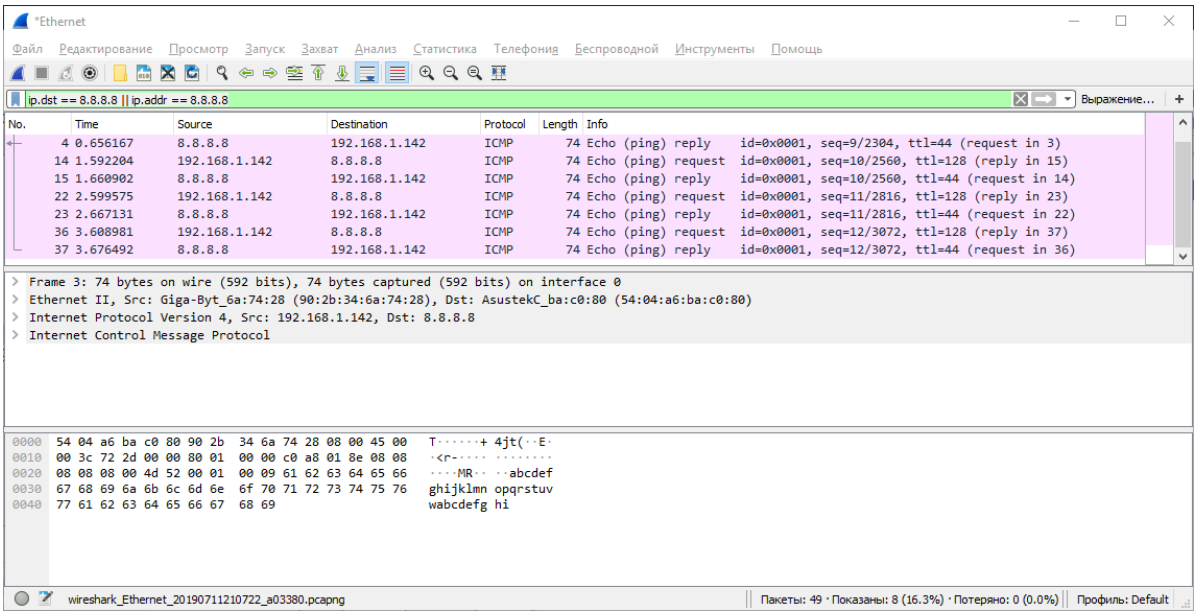


Рисунок 16 – Найденные пакеты

Попробуем перехватить данные протокола синхронизации времени NTP. NTP — сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью.

Для работы скачаем простой NTP-клиент, который можно найти по адресу https://www.qsl.net/dl4yhf/rsNTP/rsNTP.zip. Запустим программу от имени администратора и перехватим трафик. После попробуем найти нужные нам пакеты по фильтру «ntp».

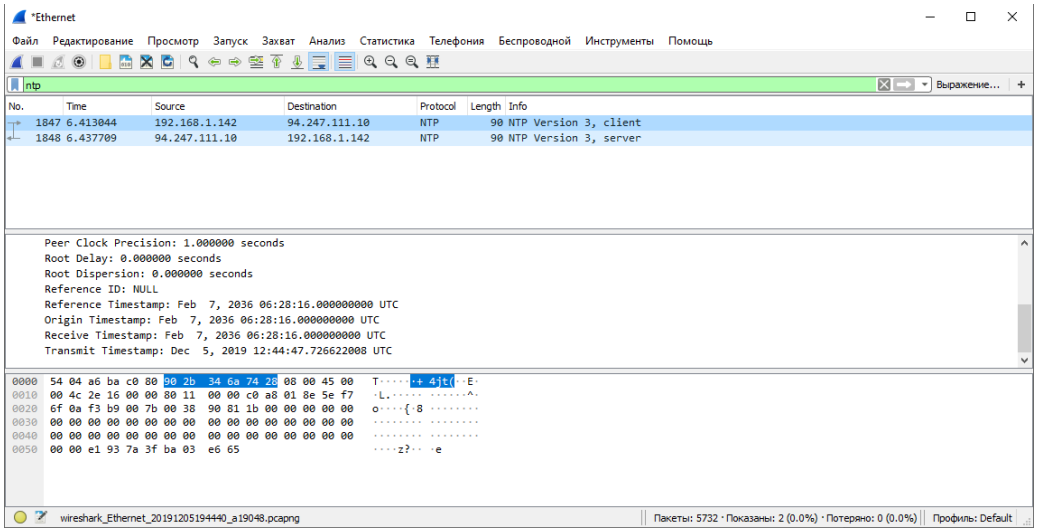


Рисунок 17 – Перехваченные пакеты протокола NTP

Самое интересное здесь – последние 4 пункта.

Время обновления - время, когда система последний раз устанавливала или корректировала время.

Начальное время - время клиента, когда запрос отправляется серверу.

Время приёма - время сервера, когда запрос приходит от клиента.

Время отправки - время сервера, когда запрос отправляется клиенту.

Пакеты, перехваченные при помощи Wireshark, можно сохранять, чтобы после редактировать и вручную отправлять. Выберем исходящий пакет и сохраним его, выбрав Файл – Экспортировать Указанные Пакеты... В параметрах сохранения нужно выбрать Selected Packet.

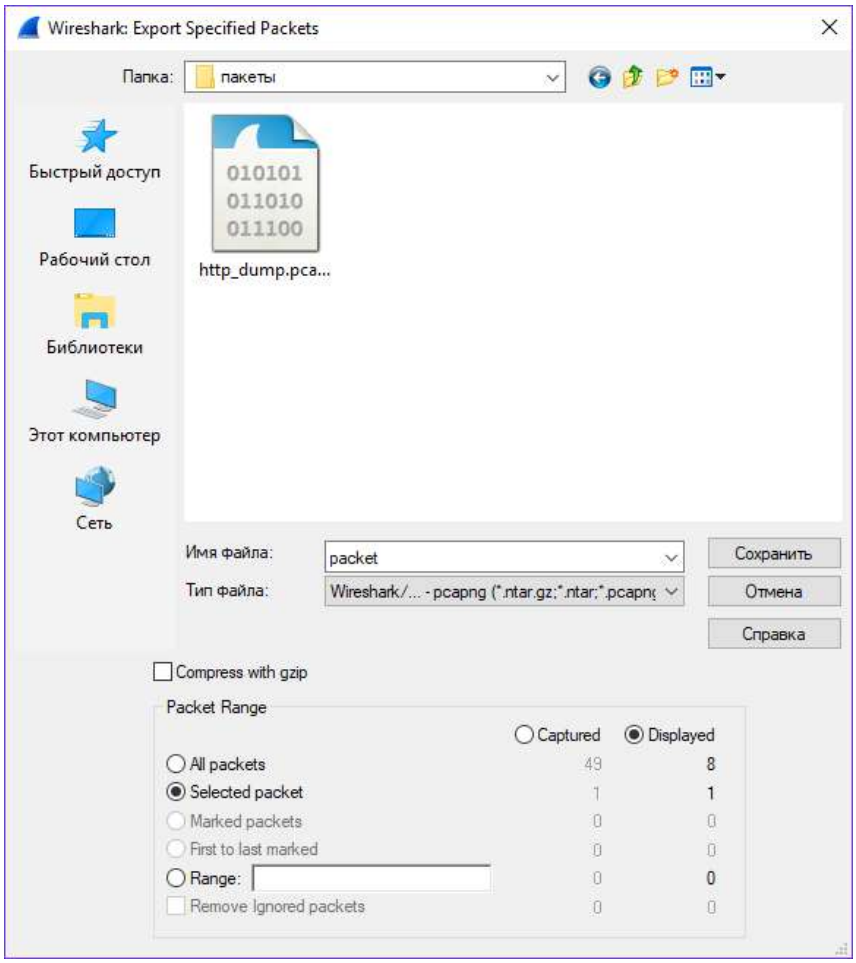


Рисунок 18 – Сохранение пакета

В самом Wireshark нет возможности генерировать или редактировать пакеты, поэтому воспользуемся Colasoft Packet Builder.

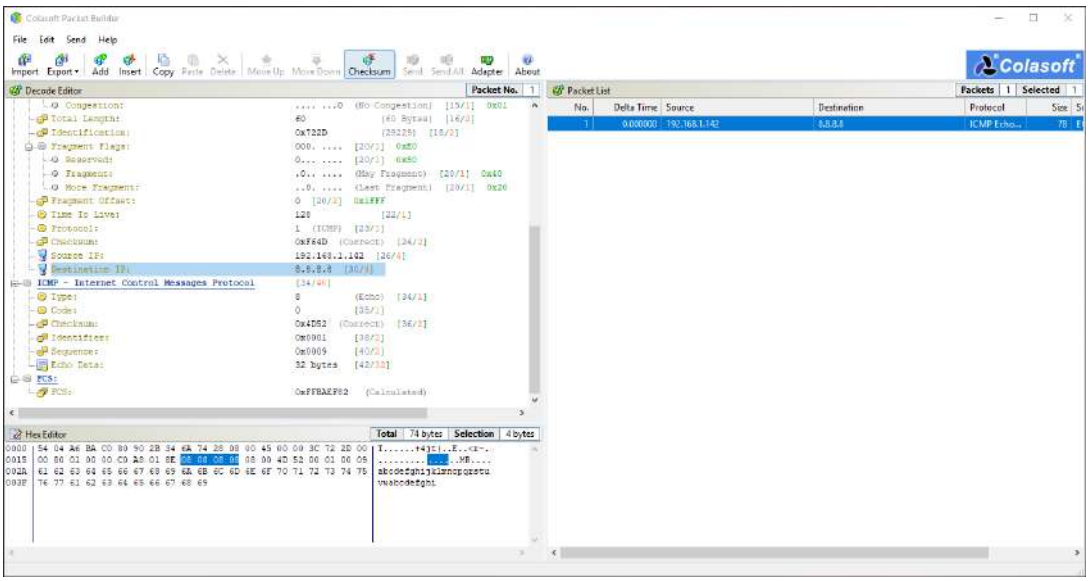


Рисунок 19 – Окно Packet Builder

В левой части программы указаны параметры пакета, которые можно свободно редактировать. Заменим Destination IP на 1.1.1.1.

Выберем пакет в правой части программы и, запустив захват в Wireshark, отправим его, нажав на Send. Здесь необходимо выбрать адаптер и нажать Start.

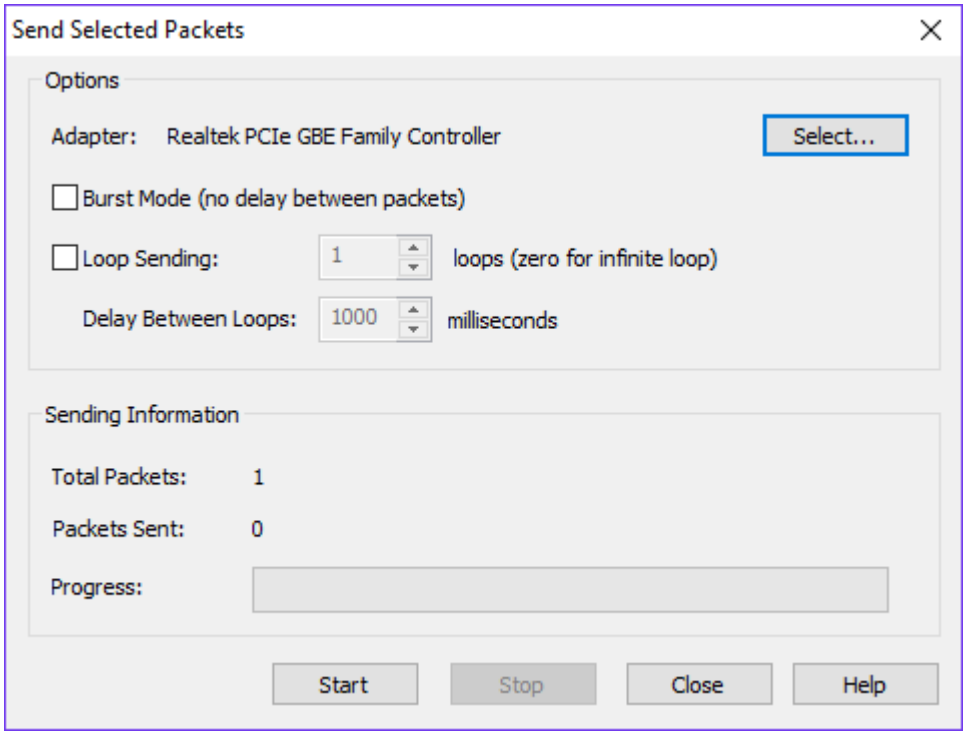


Рисунок 19 – Отправка пакета

Проверим наши захваченные пакеты.

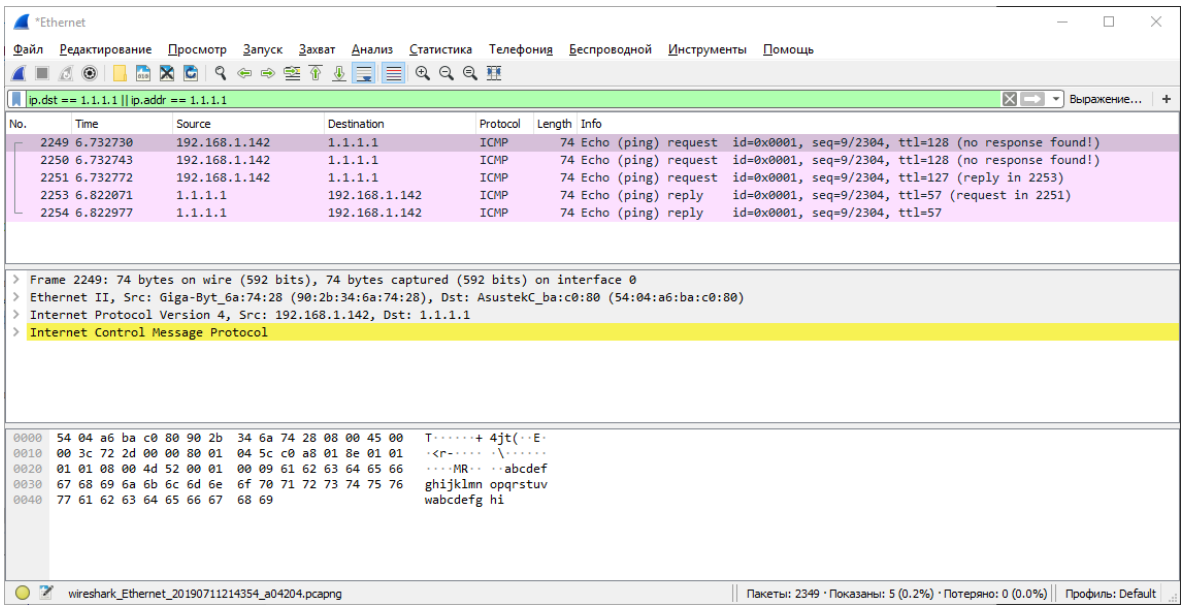


Рисунок 20 – Захваченный сгенерированный пакет

Задание

1. Установить и настроить анализатор трафика
2. При необходимости установить программу-клиент заданного прикладного протокола
3. Выполнить базовые процедуры для заданного протокола
4. Расписать структуру одного из перехваченных пакетов для трех видов протоколов (Ethernet, IP, TCP/UDP)
5. Перехватить пакеты и провести их анализ (найти адрес отправителя и адрес принимающего, протоколы передачи, передаваемые данные)
6. Сгенерировать пакет, отправить его и принять на другом устройстве (виртуальная машина, другой компьютер и т.п.)

Лабораторная работа № 16
Виртуальные защищенные сети

Цель работы

Изучить технологии виртуальных частных сетей для организации защищенных каналов связи через сети общего пользования (Интернет), получить практические навыки настройки виртуальных частных сетей на примере программного продукта OpenVPN.

Теоретические сведения

OpenVPN — свободная реализация технологии виртуальных частных сетей (Virtual Private Network, VPN) с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами. Она позволяет устанавливать соединения между компьютерами, находящимися за NAT-firewall без необходимости изменения его настроек. OpenVPN была создана Джеймсом Йонаном (James Yonan) и распространяется под лицензией GNU GPL.

Для обеспечения безопасности управляющего канала и потока данных, OpenVPN использует библиотеку OpenSSL. Благодаря этому задействуется весь набор шифров, доступных в данной библиотеке. Также может использоваться пакетная авторизация HMAC, для обеспечения большей безопасности, и аппаратное ускорение для улучшения производительности шифрования. Эта библиотека использует OpenSSL, а точнее протоколы SSLv3/TLSv1. OpenVPN используется на Solaris, OpenBSD, FreeBSD, NetBSD, GNU/Linux, Apple Mac OS X и Microsoft Windows.

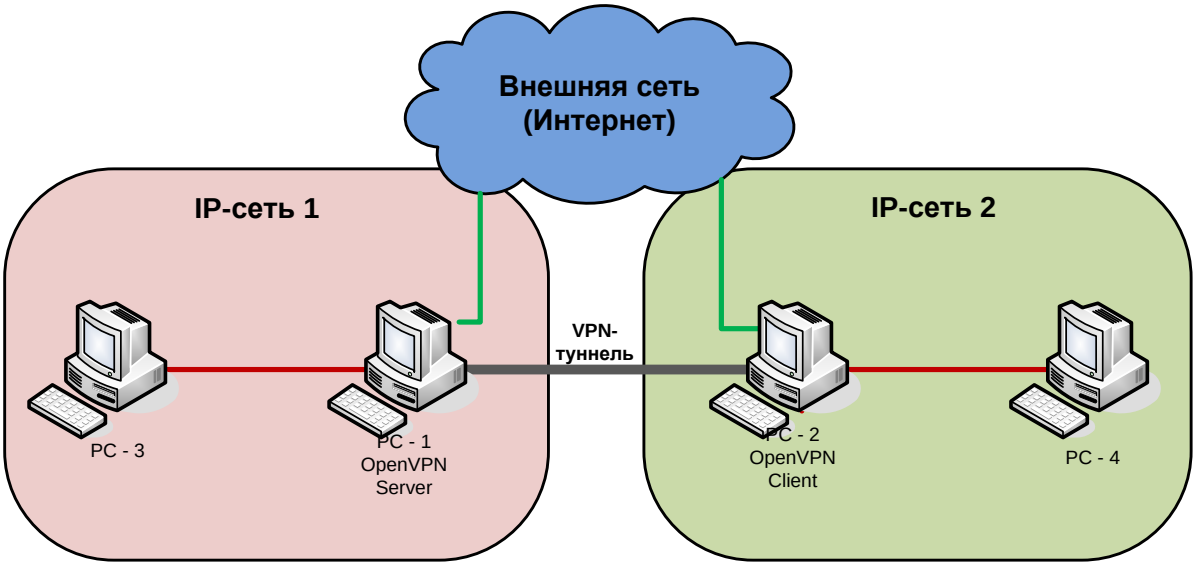
OpenVPN предлагает пользователю несколько видов аутентификации. Предустановленный ключ, — самый простой метод. Сертификатная аутентификация, — наиболее гибкий в настройках метод. С помощью логина и пароля, — может использоваться без создания клиентского сертификата (серверный сертификат все равно нужен).

OpenVPN проводит все сетевые операции через TCP, либо UDP порт. Также возможна работа через большую часть прокси-серверов, включая HTTP, через NAT и сетевые фильтры. Сервер может быть настроен на назначение сетевых настроек клиенту. Например, IP адрес, настройки маршрутизации и параметры соединения. OpenVPN предлагает два различных варианта сетевых интерфейсов, используя драйвер TUN/TAP. Возможно создание Layer 3 based IP туннель, называемый TUN, и Layer 2 based Ethernet — TAP, способный передавать Ethernet трафик. Также возможно использование библиотеки компрессии LZO, для сжатия потока данных. Используемый порт 1194 выделен Internet Assigned Numbers Authority для работы данной программы. Версия 2.0 позволяет контролировать несколько одновременных туннелей, в отличие от версии 1.0, позволявшей создавать только 1 туннель на 1 процесс.

Использование OpenVPN стандартных протоколов TCP и UDP позволяет ему стать альтернативой IPsec в ситуациях, когда Интернет-провайдер блокирует некоторые VPN протоколы.

Задание

Настроить безопасное взаимодействие двух IP-сетей между собой через сеть общего пользования (Интернет), средствами программного продукта OpenVPN. Создать ключи и сертификаты безопасности. Настроить конфигурационный файл VPN-сервера и VPN-клиента.



1. **Подготовка виртуальных машин**

В данной лабораторной работе, в качестве примера, используется Windows 10, но вы можете выбрать любую другую ОС с поддержкой OpenVPN.

Лабораторная работа выполнена во внутренней сети VirtualBox (Рисунок 1.1), но вы можете объединится в пары и из домашних сетей создать одну общую, но для этого вам необходимо выполнить проброс портов.

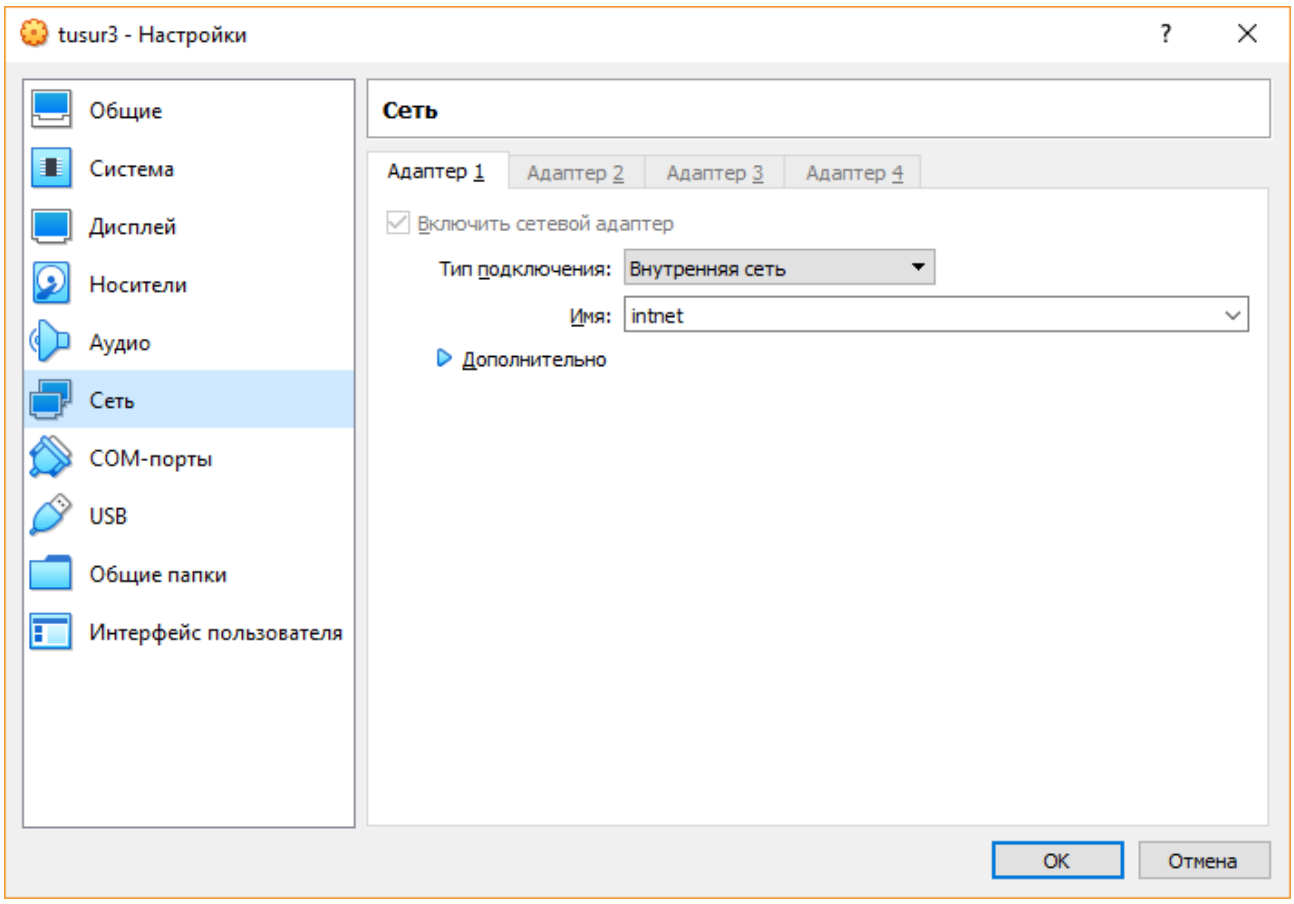


Рисунок 1.1 – Внутренняя сеть VirtualBox

Рекомендуется установить расширение гостевой ОС VirtualBox (Рисунок 1.2) для корректной работы и возможности использовании общих папок (Рисунок 1.3).

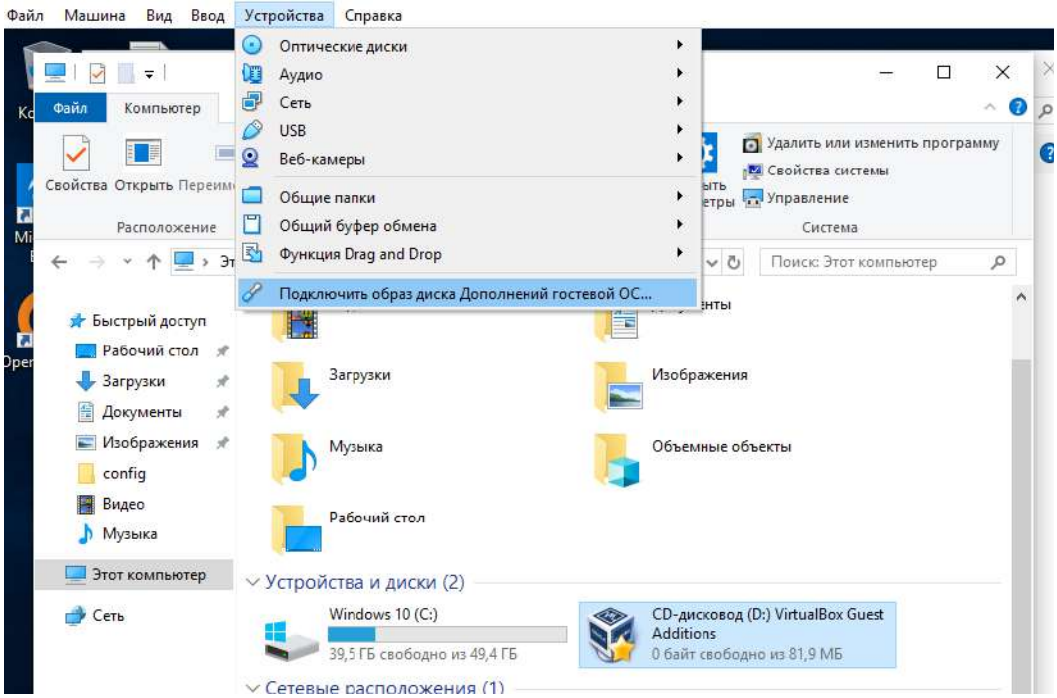


Рисунок 1.2 – расширения гостевой ОС

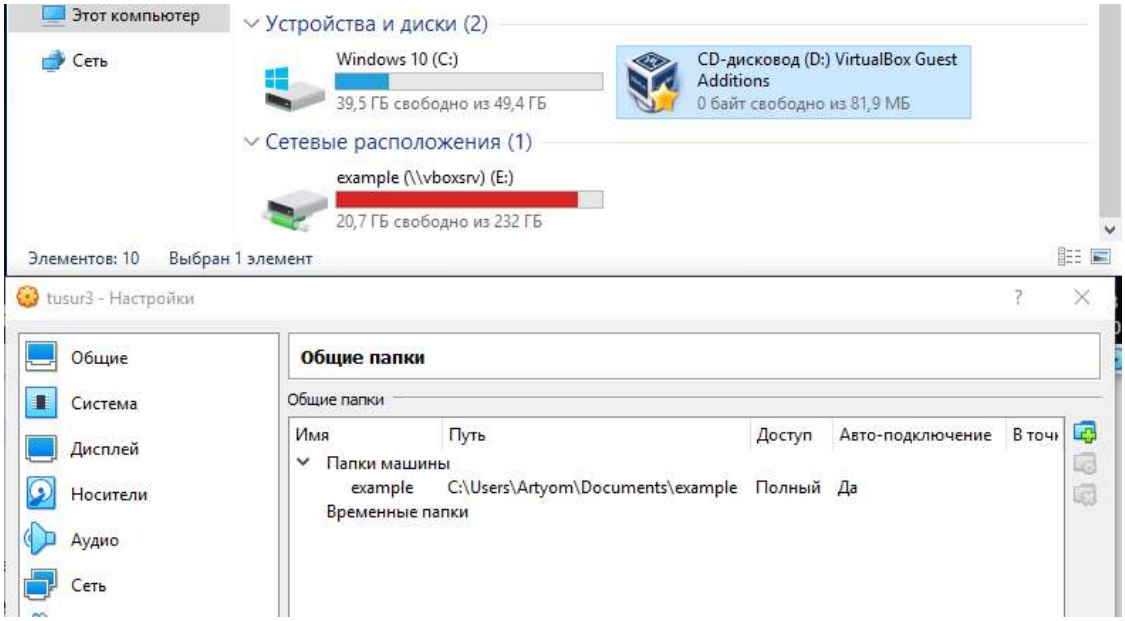


Рисунок 1.3 – Настройка общих папок

Также, для удобства рекомендуется включить видимость расширений файла (Рисунок 1.4).

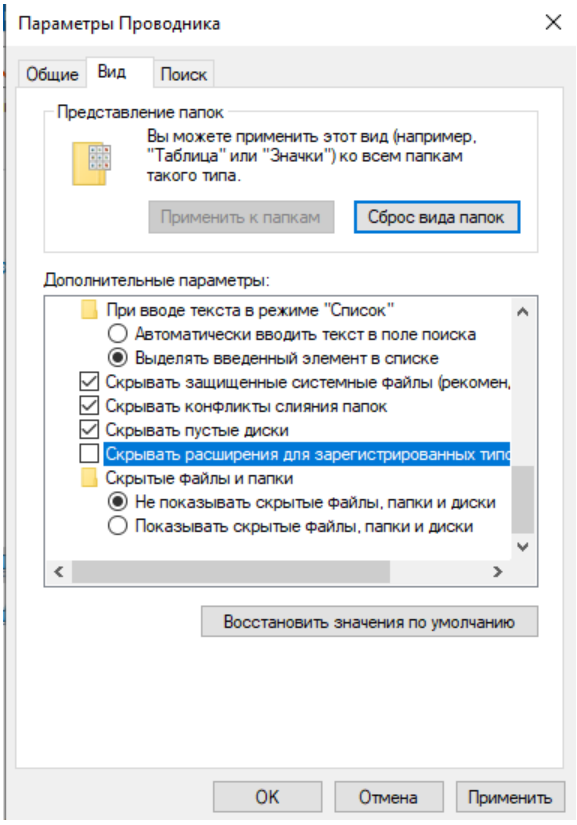


Рисунок 1.4 – настройка параметров проводника

Для начала, необходимо скачать и установить OpenVPN с официального сайта openvpn.net/community-downloads/ на обе сетевые машины. Во время установки на сервере поставить галочку на против EasyRSA (Рисунок 1.5), с помощью данной программы мы, в дальнейшем, будем генерировать сертификаты и ключи.

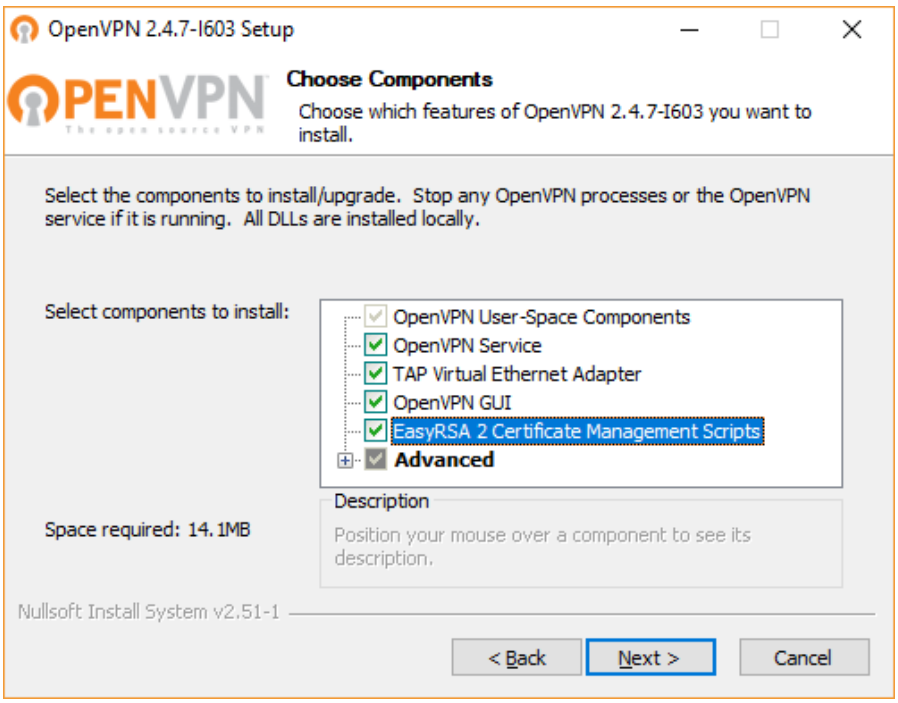


Рисунок 1.5 – EasyRSA

В процессе установки в систему инсталлируется виртуальный сетевой адаптер TAP-Windows Adapter V9 и соответственно драйвер к нему (Рисунок 1.6).

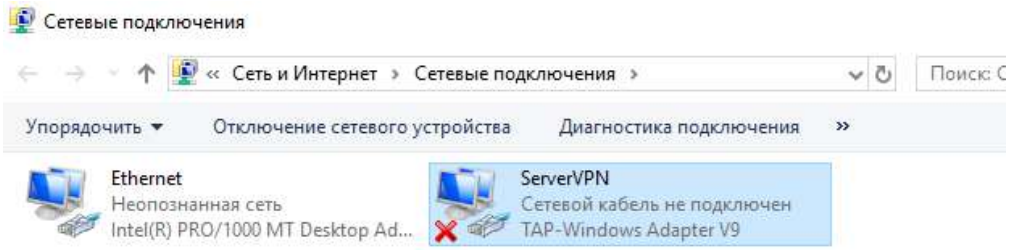


Рисунок 1.6 – Сетевой адаптер

Этому интерфейсу программа OpenVPN будет назначать ip-адрес и маску виртуальной сети.

Проверьте, чтобы ваши машины видели друг друга. Для определения ip можно воспользоваться командой ipconfig и командой ping для проверки соединения (Рисунок 1.7).

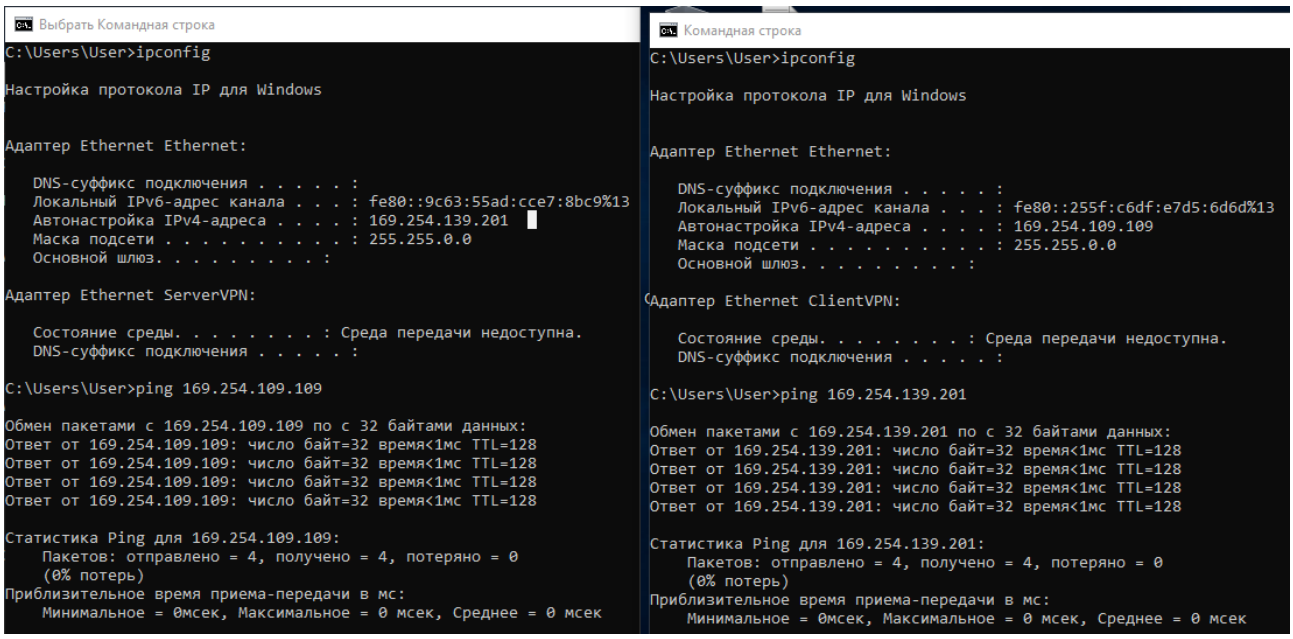


Рисунок 1.7 – Проверка соединения

Это подойдет, если машины находятся в одной локальной сети. Если машины скрыты друг от друга с помощью NAT, необходимо выполнить проброс портов и свой ip адрес можно узнать с помощью различных сервисов, например, 2ip.ru.

2. **Создание сертификатов и ключей для OpenVPN сервера и клиента**.

Все действия по созданию ключей и сертификатов проводятся на OpenVPN сервере.

Последовательность действий:

1. Открыть командную строку от имени администратора и с помощью команды cd переходим в папку с EasyRSA и выполняем команду init-config.bat (Рисунок 2.1). В результате в папке OpenVPN\easy-rsa\ появится файл vars.bat. Данный пакетный файл будет задавать переменные для сеанса генерации сертификатов.

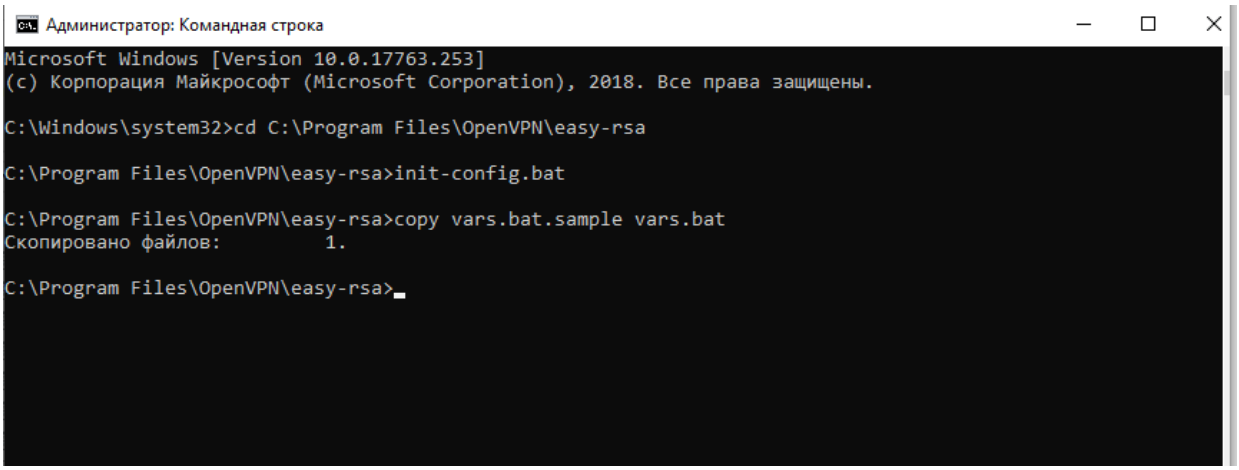


Рисунок 2.1 – config.bat

2. Откроем vars.bat с помощью блокнота и изменим часть данных, которые касаются организации и расположения (Рисунок 2.2). Эти данные можно не заполнять, они не влияют на работу OpenVPN и в дальнейшем их можно изменить.

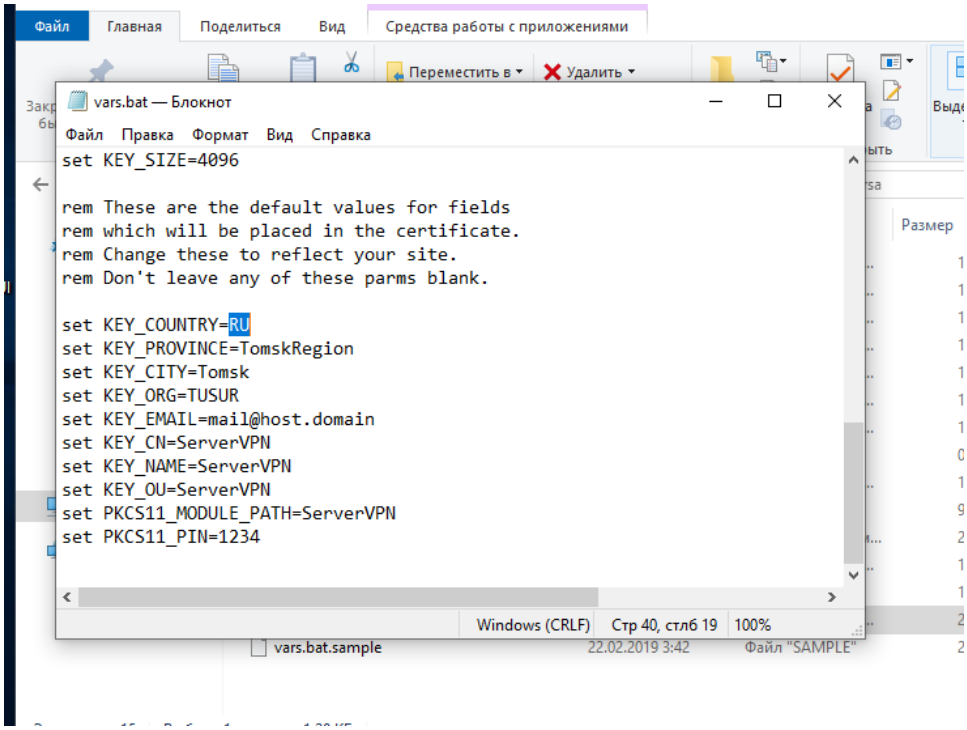


Рисунок 2.2 – vars.bat

3. Вернемся в командную строку и выполним две команды vars и clean-all, в ответ должны получить два раза скопировано 1 (Рисунок 2.3).

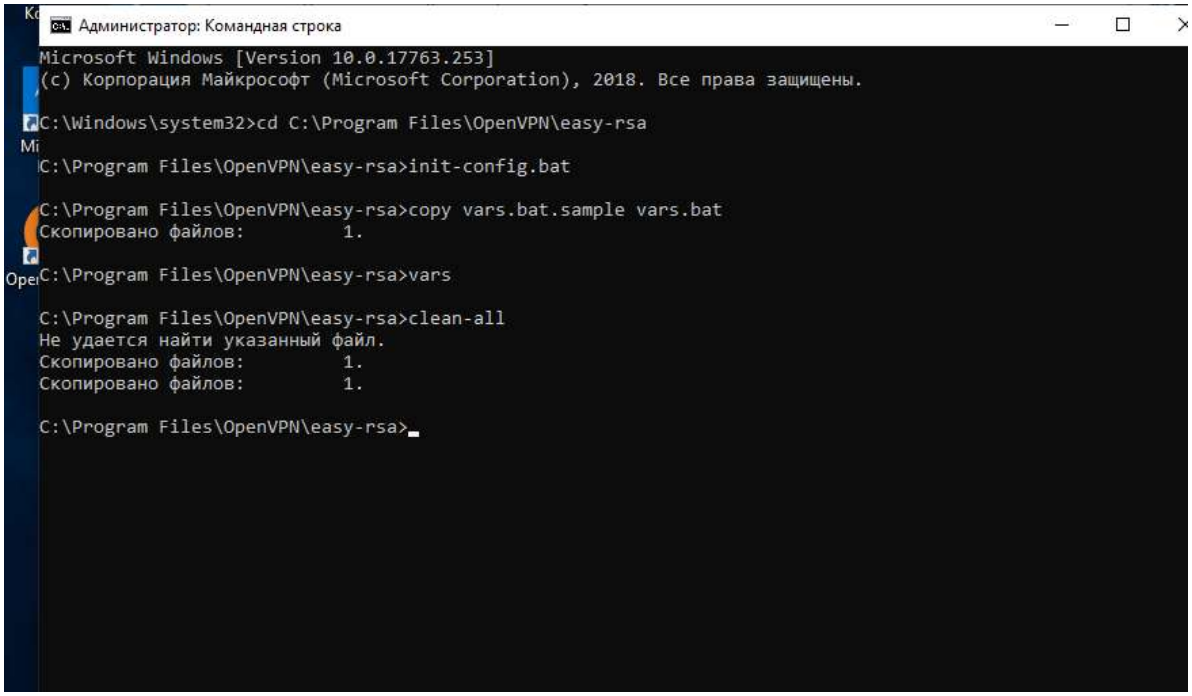


Рисунок 2.3 – результат двух команд

4. Создадим параметры Diffie Hellman, используя команду build-dh, если вы увидите ошибку: «openssl» не является внутренней или внешней исполняемой командой (Рисунок 2.4),

необходимо в «переменные среды» добавить в Path путь OpenVPN\bin (Мой Компьютер – Свойства – Дополнительные параметры системы – Вкладка «Дополнительно» – Переменные среды – Path – Изменить – Обзор) (Рисунок 2.5)

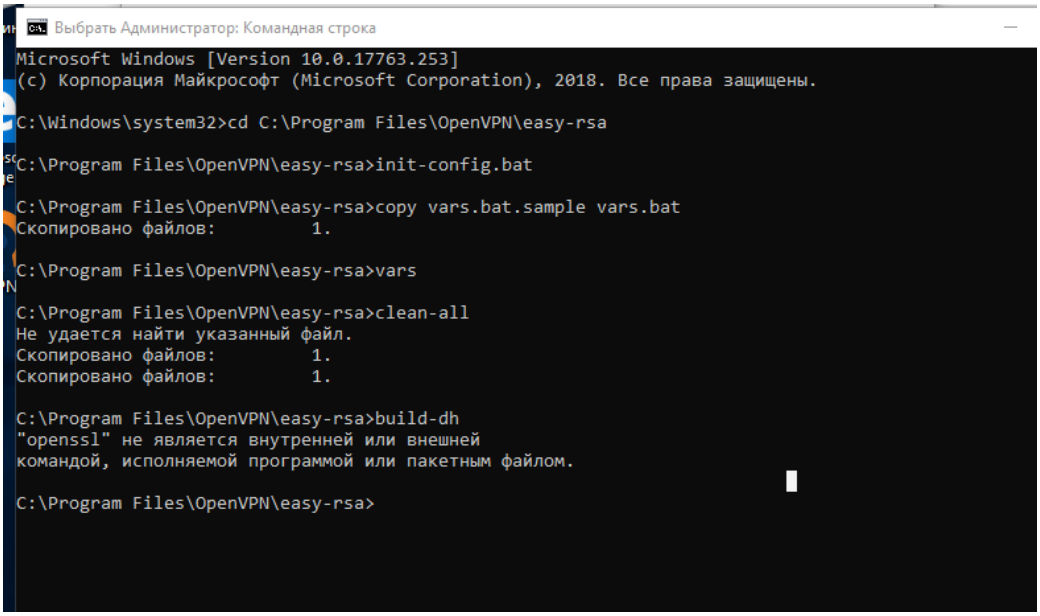


Рисунок 2.4 – Ошибка

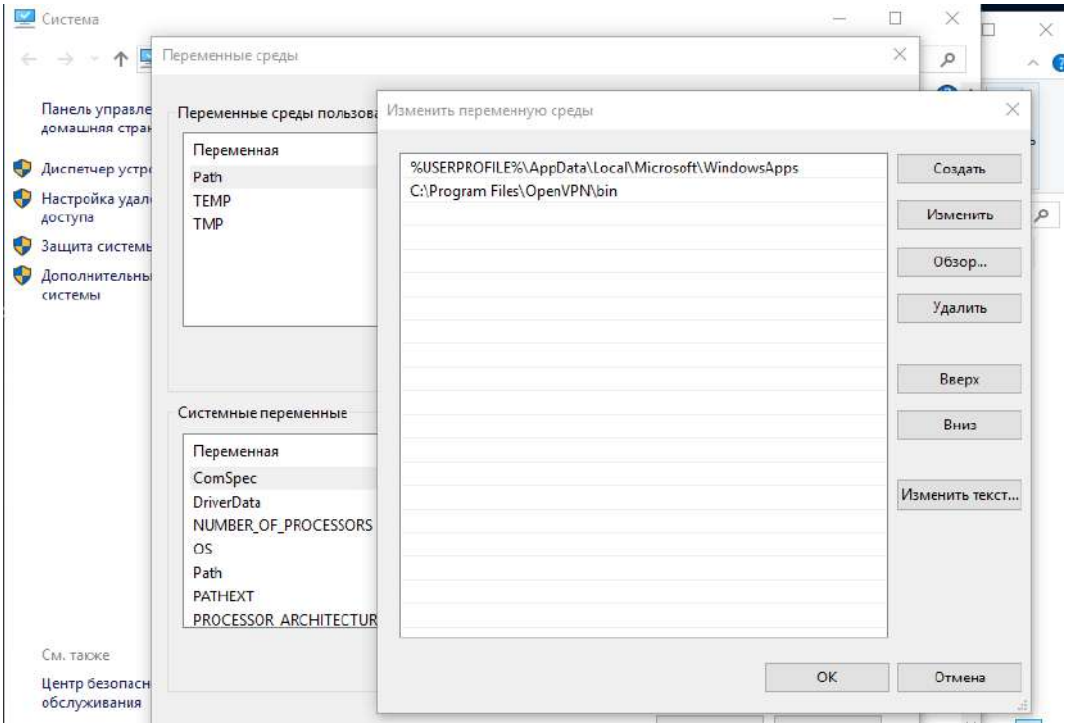


Рисунок 2.5 – Добавление в переменную среду

После заново откройте командную строку и выполните выше указанные действия еще раз (Рисунок 2.6).

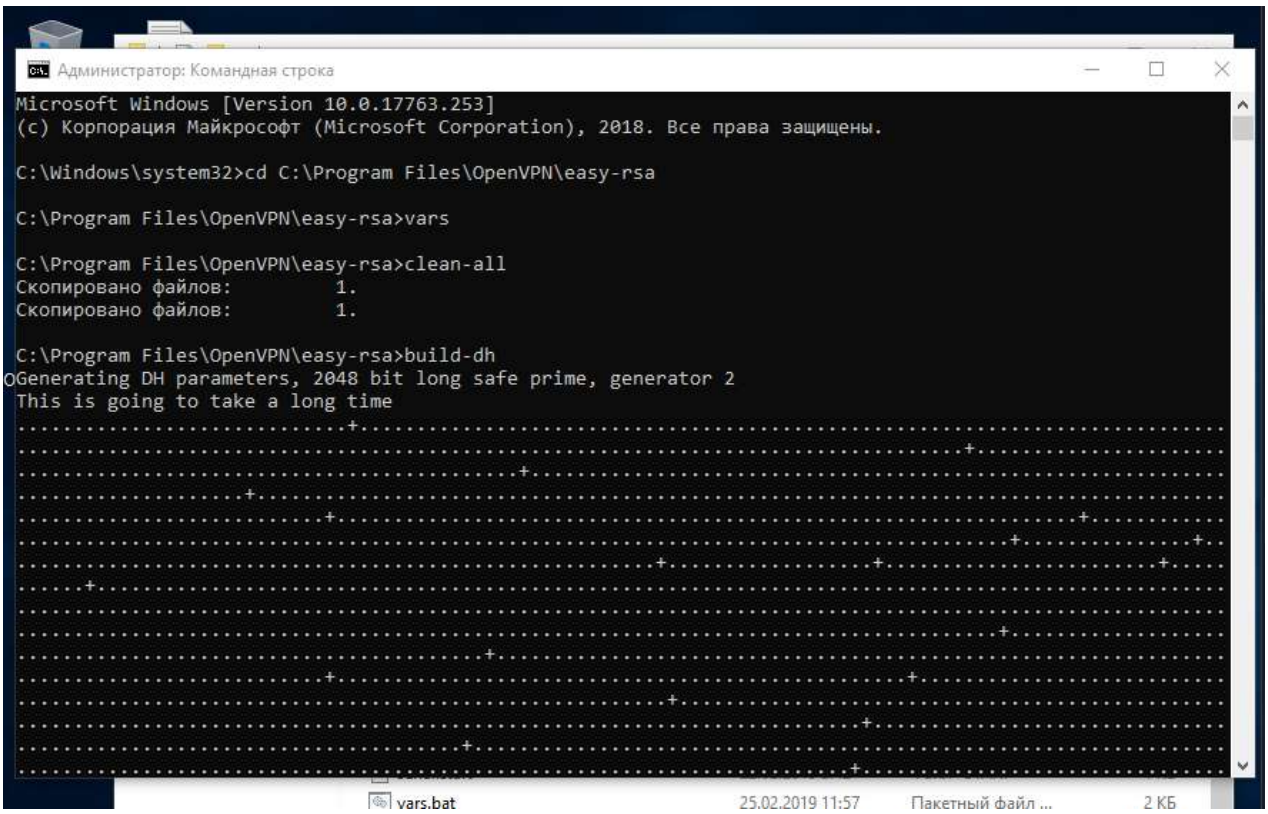


Рисунок 2.6 – Генерация DH

В результате в папке easy-rsa\keys появится файл dh2048.pem

5. Создадим основной Certificate Authority (CA) сертификат и ключ, для этого продолжим вводить в командную строку build-ca. Здесь можно изменить ранее заданные параметры в vars.bat, меняем, если нужно изменить, если нет, то enter (Рисунок 2.7).

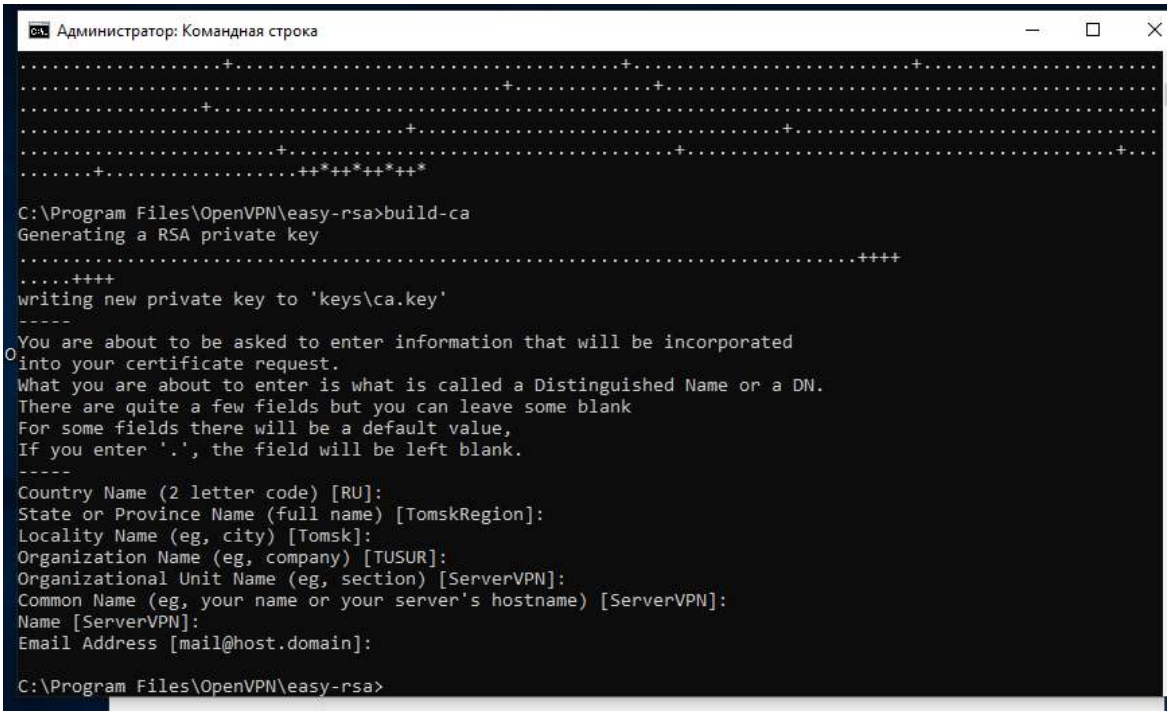


Рисунок 2.7 – Генерация CA

В результате в папке easy-rsa\keys появятся два файла ca.crt и ca.key

6. Создадим сертификат и ключ сервера, для этого продолжаем вводить build-key-server [CommonName] (В примере ServerVPN), в конце на два вопроса отвечаем положительно (Рисунок 2.8).

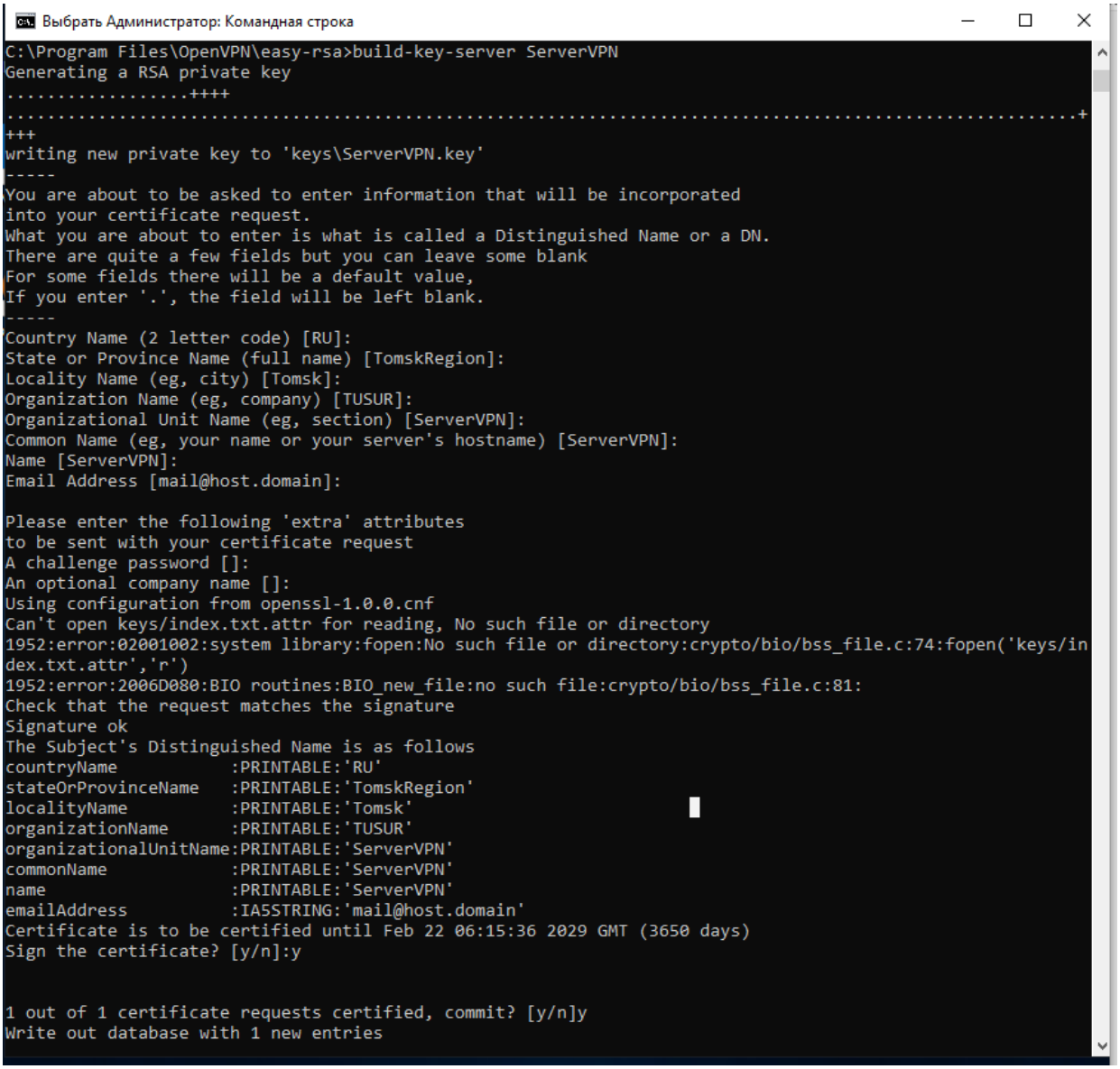


Рисунок 2.8 – Генерация сертификата и ключа сервера

В результате в папке easy-rsa\keys появятся три файла [CommonName].crt, [CommonName].csr и [CommonName].key.

7. Создадим сертификат и ключи для клиента, для этого продолжим вводить в командную строку build-key [CommonNameClient] (Рисунок 2.9). У каждого клиента должны быть свои сертификат и ключи со своим именем. Генерируем столько раз, сколько хотим добавить клиентов.

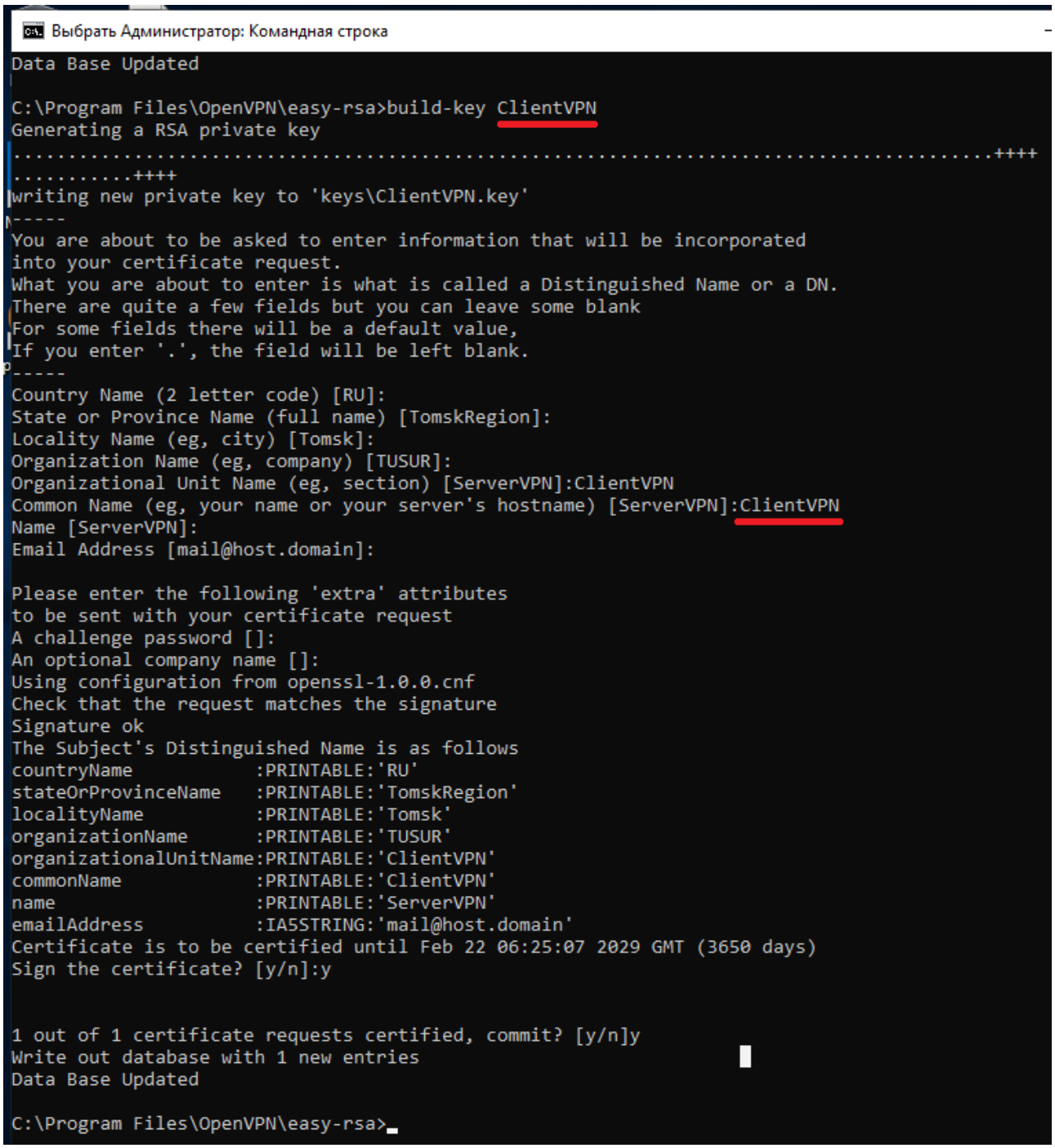


Рисунок 2.9 – Генерация сертификата и ключа клиента

В результате в папке easy-rsa\keys появятся три файла [CommonNameClient].crt, [CommonNameClient].csr и [CommonNameClient].key.

8. Создадим ключ для аутентификации пакетов, для этого выполним команду «openvpn --genkey --secret keys/ta.key» (Рисунок 2.10).

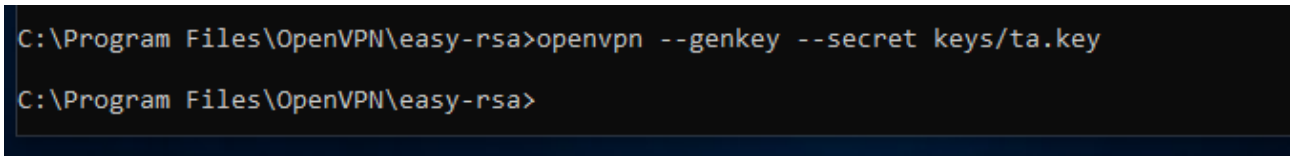


Рисунок 2.10 – Генерация ключа аутентификации пакетов

В результате в папке easy-rsa\keys появится файл ta.key

После выполнения шагов 1-8 подкаталоге keys создаются ключи и сертификаты.

Имя файла	Где нужен	Назначение	Секретный
ca.crt	сервер + все клиенты	Root CA certificate	НЕТ
ta.key	сервер + все клиенты	Аутентификация пакетов	ДА
ca.key	ключ подписывающей машины	Root CA key	ДА
dh{n}.pem	только на сервере	Diffie Hellman параметры	НЕТ
server.crt	только на сервере	Server сертификат	НЕТ
server.key	только на сервере	Server ключ	ДА
client1.crt	только на client1	Client1 сертификат	НЕТ
client1.key	только на client1	Client1 ключ	ДА

Окончательный шаг процесса создания ключей - копирование ключей и сертификатов на требуемые машины. Необходимые ключи и сертификаты нужно скопировать в подкаталог «Config» установочного каталога OpenVPN (Рисунок 2.11).

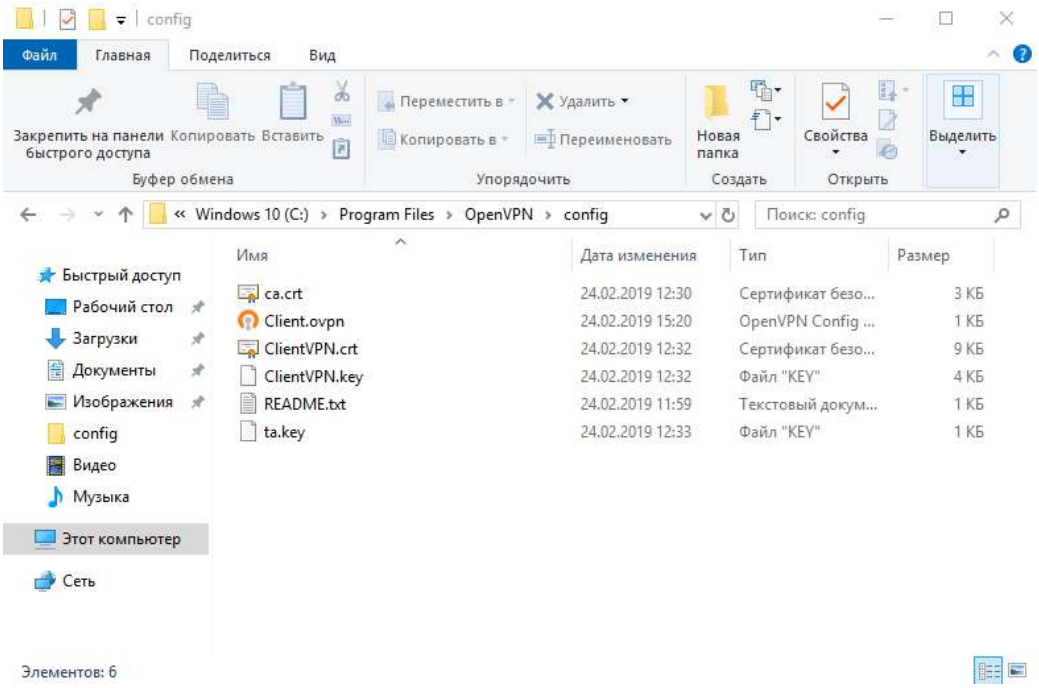


Рисунок 2.11 – Сертификаты и ключи клиента

3.

Создание файлов конфигурации OpenVPN сервера и клиентов.

3.1. Пример конфигурационных файлов

Свою конфигурацию рекомендуется базировать на исходных конфигурационных файлах OpenVPN. Их можно найти в меню (Пуск -> Программы -> OpenVPN -> OpenVPN Sample Configuration Files) или на диске (%ProgramFiles%/OpenVPN/sample-config)

В Linux, BSD, или UNIX-подобных ОС файлы конфигураций называются server.conf и client.conf, а в Windows называются server.ovpn и client.ovpn.

3.2. Редактирование файла конфигурации сервера

При конфигурации сервера рекомендуется основываться на примере этого файла из OpenVPN. VPN создается с использованием виртуального сетевого интерфейса, с ожиданием подключения клиентов на UDP порт 1194 (официальный номер порта OpenVPN), и распределением виртуальных адресов подключаемых клиентов из заданной подсети (Для примера – 10.1.0.0/24.)

Перед использованием примера файла конфигурации необходимо установить ca, cert, key, и dh параметры на файлы, полученные при создании PKI.

Уже на этом шаге файл конфигурации готов к использованию. Или можно поменять следующие настройки:

- dev [tun | tap] (сервер, клиент) - указание типа интерфейса и режима работы: tun = L3-туннель, tap = L2-туннель.

L3 и L2 - 3-ий и 2-ой уровни в обеих распространённых моделях сетевых протоколов - и ISO OSI Reference Model (Эталонная модель взаимодействия открытых систем) и Internet Protocol Suite. Точное название термина - Layer 3, однако иногда говорят и Level 3.

- L3 (Layer 3) - 3-ий уровень - Network Layer, сетевой уровень, уровень Internet. Если идёт речь об IP-маршрутизации, то это как раз L3, соответственно, на уровне 3 находится IP-протокол (не путать с TCP, UDP и т.п. - они выше). Хосты, соединённые через маршрутизаторы, могут напрямую (без технологий инкапсуляции) обмениваться только данными 3 уровня (более высокие уровни вложены в него), то есть IP-пакетами (и соответственно не могут обмениваться L2-кадрами). Важно также запомнить, что термин пакет относится именно к данному уровню и подразумевает именно IP-пакет.
- L2 (Layer 2) - 2-ой уровень - Data Link Layer, канальный уровень. Если идёт речь о коммутации, то это как раз L2. Хосты, соединённые через коммутаторы или мосты, могут напрямую обмениваться данными 2 уровня (более высокие уровни вложены в него), то есть Eth-кадрами (L2-кадрами). Важно также запомнить, что термин кадр (frame, фрейм) относится именно к данному уровню и подразумевает именно Eth-кадр.

- Если используете Ethernet bridging, необходимо указать server-bridge и dev tap вместо server и dev tun.

- Если ваш OpenVPN сервер прослушивает TCP порт вместо UDP порта, используйте proto tcp вместо proto udp (если необходимо прослушивать и TCP, и UDP порты, необходимо запустить две независимые копии OpenVPN).
- При необходимости использования другого виртуального IP адресного пространства (вместо 10.1.0.0/24), нужно модифицировать директиву server. Помните, что это адресное пространство не должно использоваться вашей сетью.
- Раскомментируйте директиву client-to-client, если хотите, чтобы клиенты могли устанавливать между собой соединения при помощи VPN. По умолчанию клиенты могут подключаться только к серверу.

3.3. Редактирование конфигурационных файлов клиентов

В примере конфигурационного файла клиента (client.conf в Linux/BSD/Unix или client.ovpn в Windows) директивы по умолчанию отражают значения из примера конфигурационного файла сервера.

Как и в серверном файле конфигурации, вначале отредактируйте значения параметров ca, cert и key, указав файлы, сгенерированные в PKI. Помните, что каждый клиент должен иметь свою пару сертификат/ключ (cert/key). Только ca файл один и тот же на сервере и всех клиентах.

Затем отредактируйте remote директиву для указания хоста/IP адреса и номера порта OpenVPN сервера (если ваш OpenVPN сервер запущен за межсетевым экраном или NAT'ом, укажите реальный IP адрес шлюза, а также номер порта, который проброшен со шлюза к вашему OpenVPN серверу).

В завершении проверьте, совпадают ли директивы в конфигурационном файле клиента и сервера. Проверьте совпадение директив dev (tun или tap) и proto (udp или tcp). Также проверьте, чтобы comp-lzo и fragment, если используются, присутствовали в конфигурационных файлах сервера и клиента.

4. Настройка и запуск

1. Для того, чтобы на сервере работала маршрутизация, необходимо запустить regedit.exe, перейти в:

Компьютер\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

и изменить IPEnableRouter на 1 (Рисунок 4.1), необходима перезагрузка.

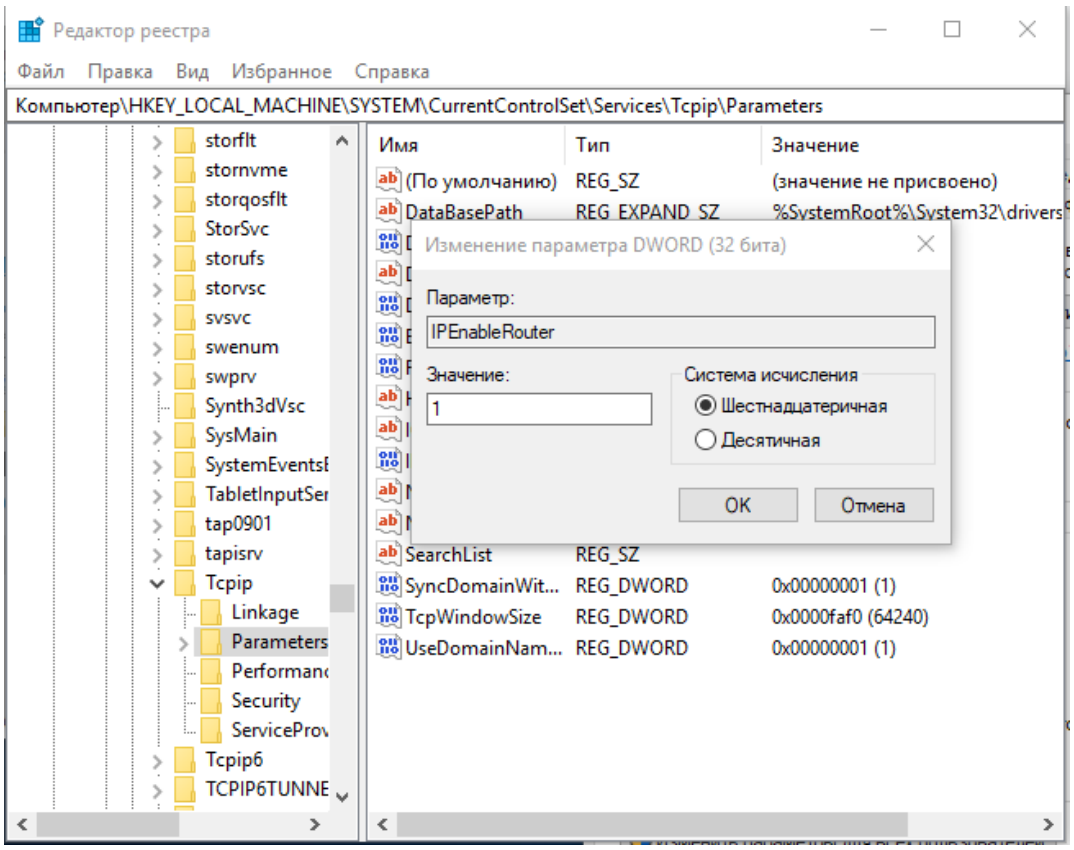


Рисунок 4.1 – Редактор реестра

2. На всех машина для openvpn.exe установите запуск от администратора (Рисунок 4.2). Это необходимо для разрешений созданий маршрутов.

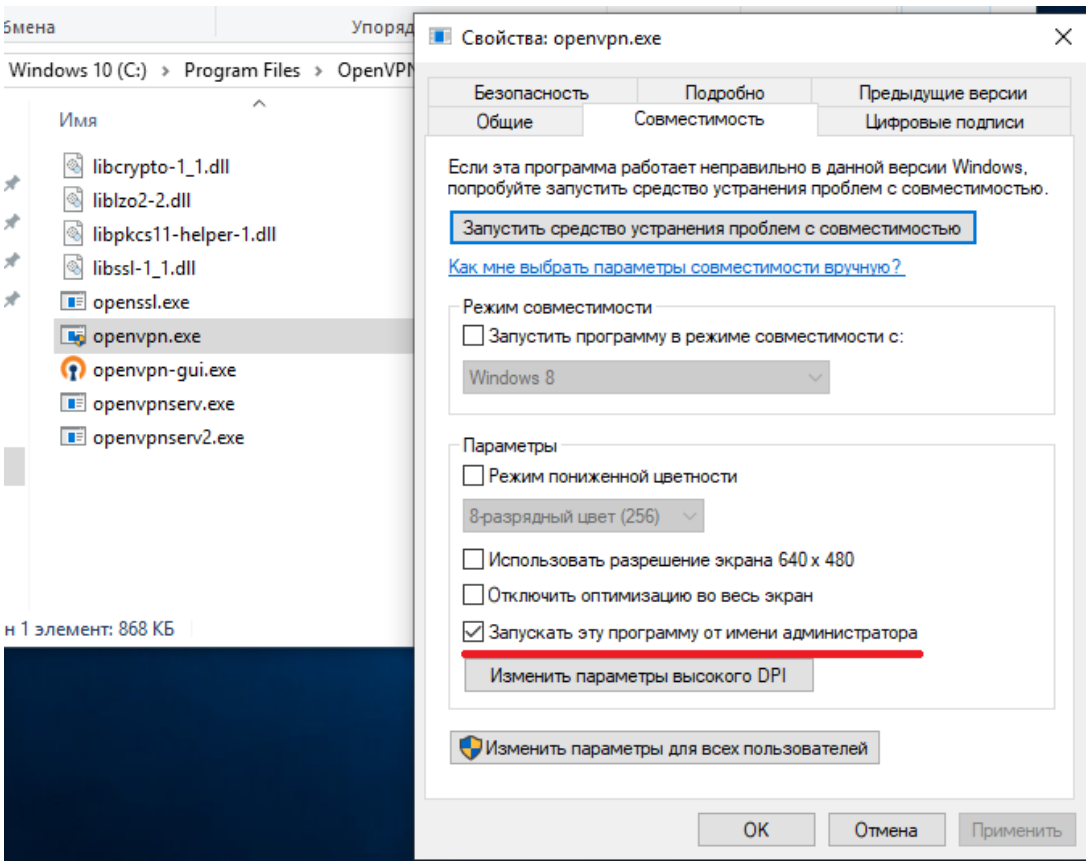


Рисунок 4.2 – Запуск от администратора

3. Запускаем сервер (Рисунок 4.3-4.4).

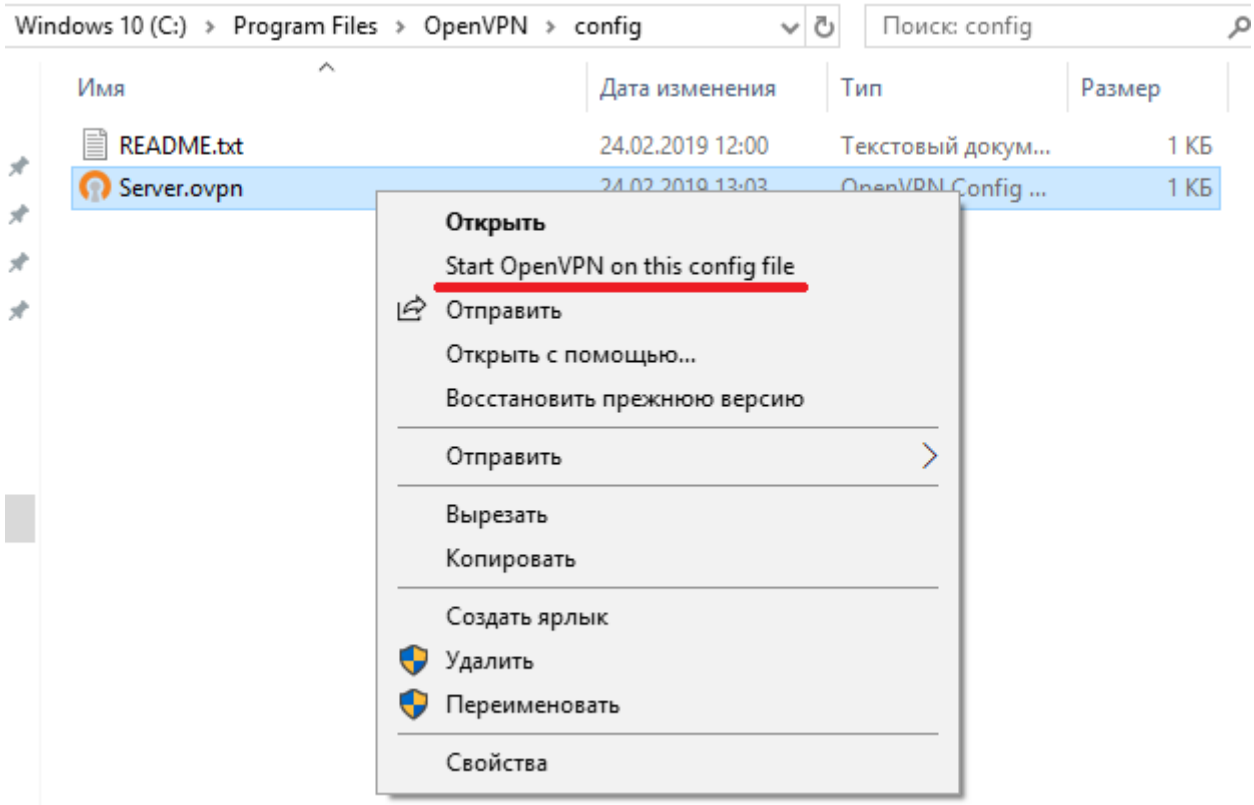


Рисунок 4.3 – Запуск сервера

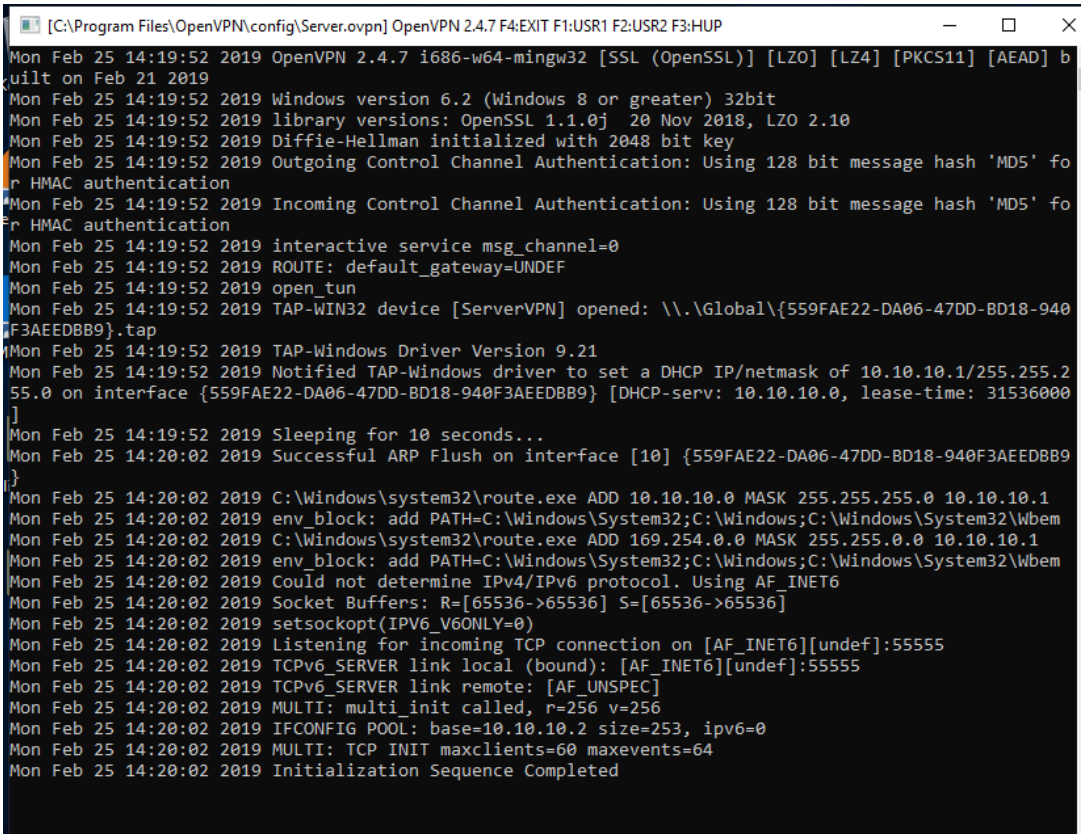


Рисунок 4.4 – Консоль

4. Запускаем клиент (Рисунок 4.5) и видим изменения на сервере (Рисунок 4.6).

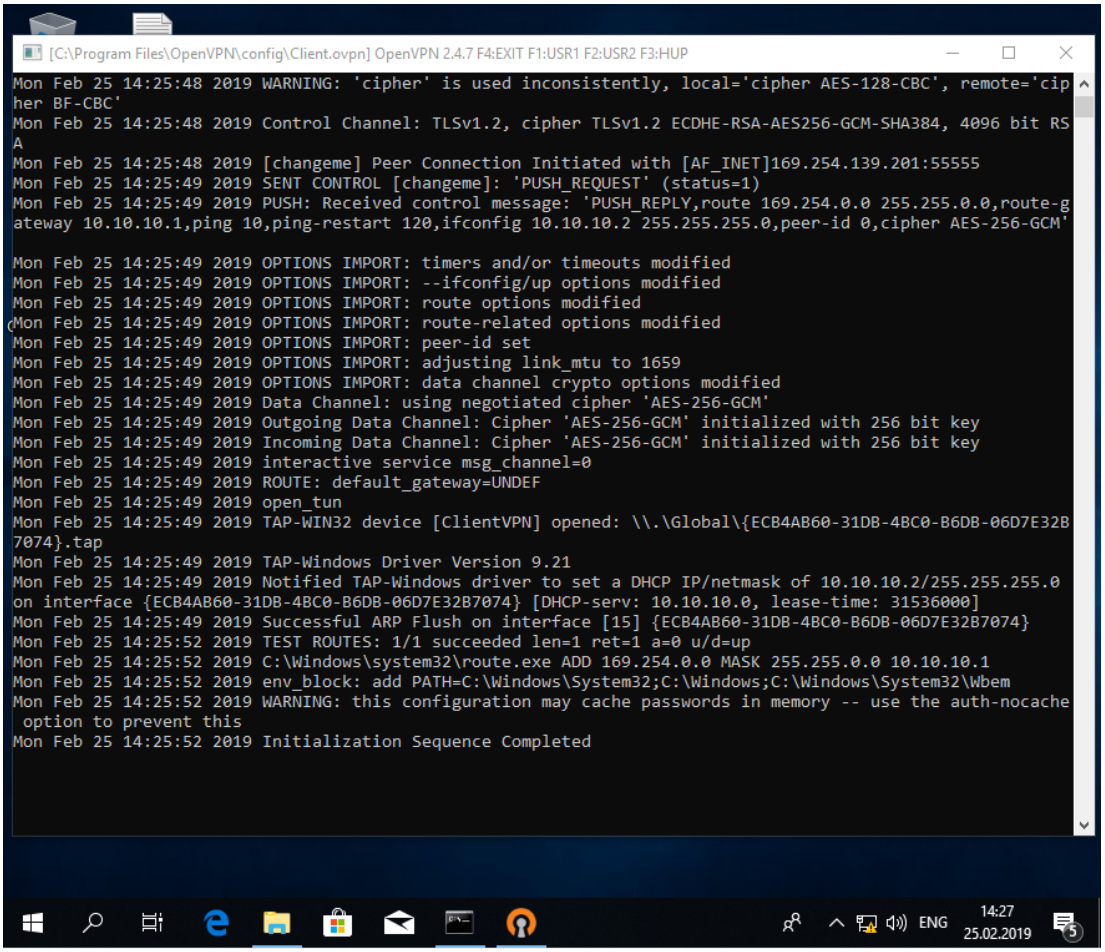


Рисунок 4.5 – Клиент

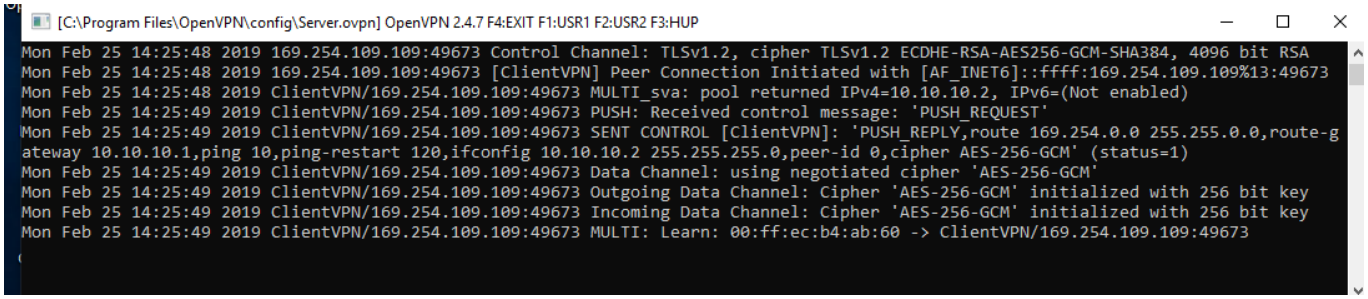


Рисунок 4.6 – Сервер

5. Проверим подключение, создадим на сервере и клиенте папку с общим доступом (Рисунок 4.7), проверим ip-адреса (Рисунок 4.8), отключим парольную защиту, если пользователи не имеют пароли (Рисунок 4.9) и проверим доступ (Рисунок 4.10).

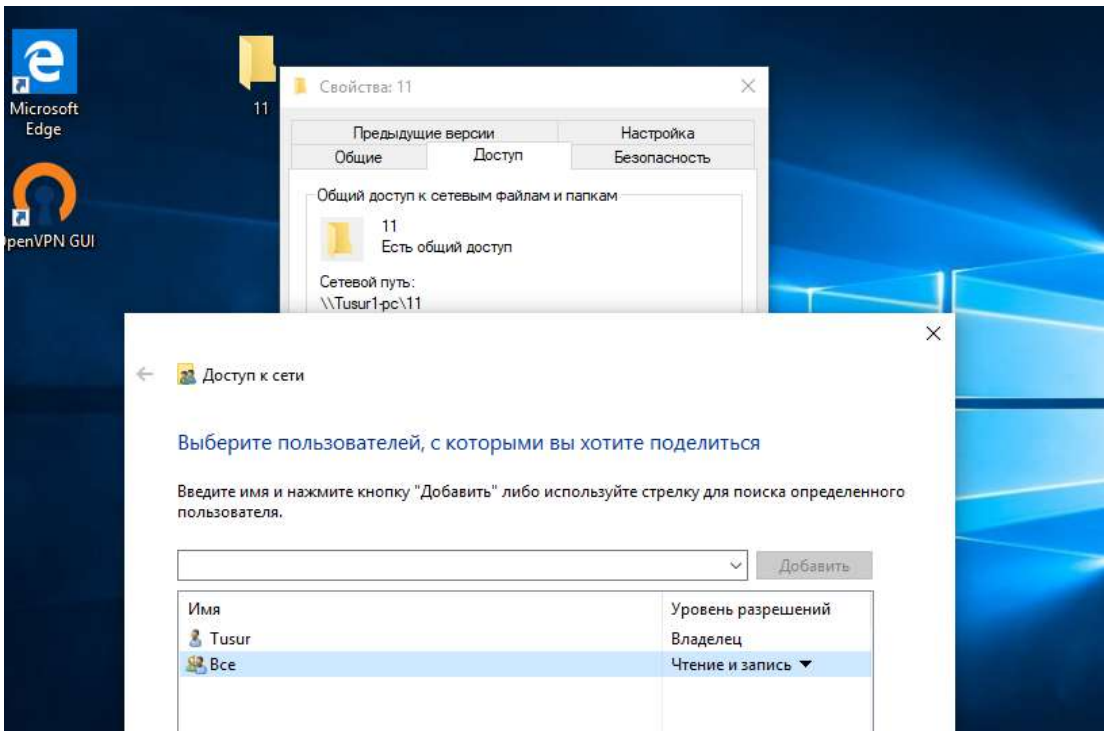


Рисунок 4.7 – Папка с общим доступом

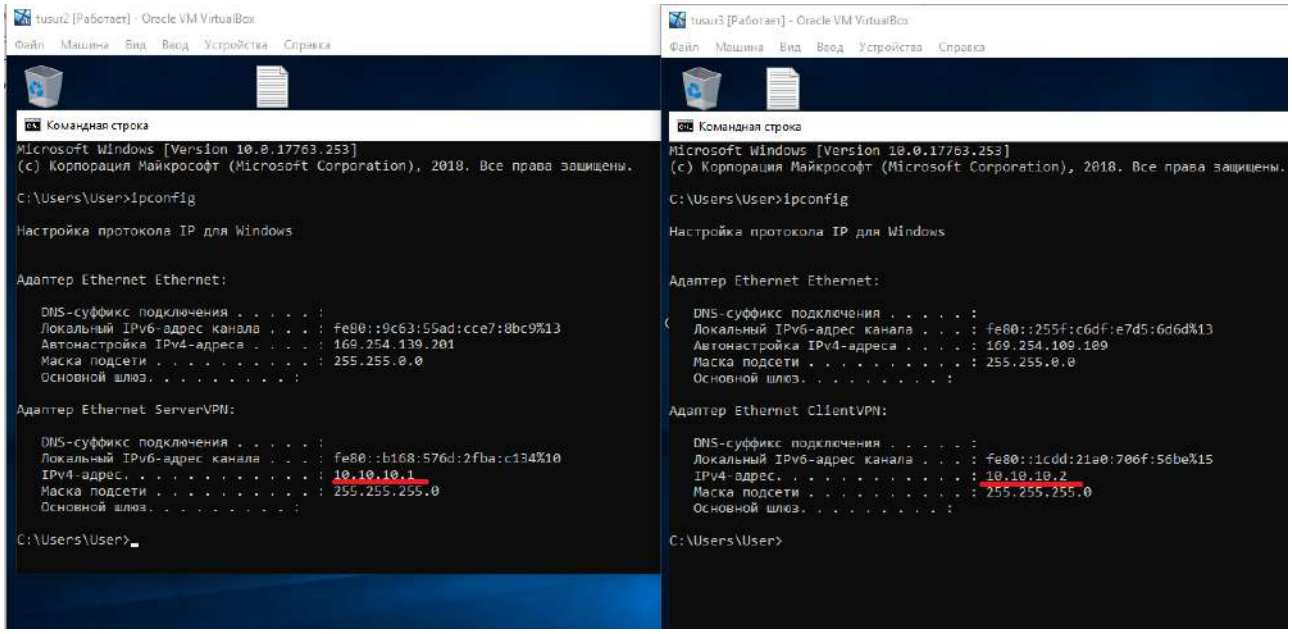


Рисунок 4.8 – Проверка ip

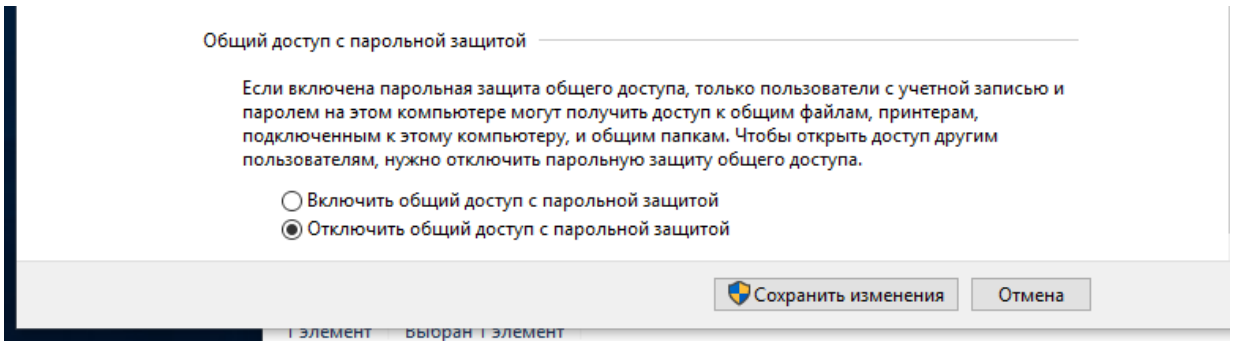


Рисунок 4.9 – Отключение парольной защиты

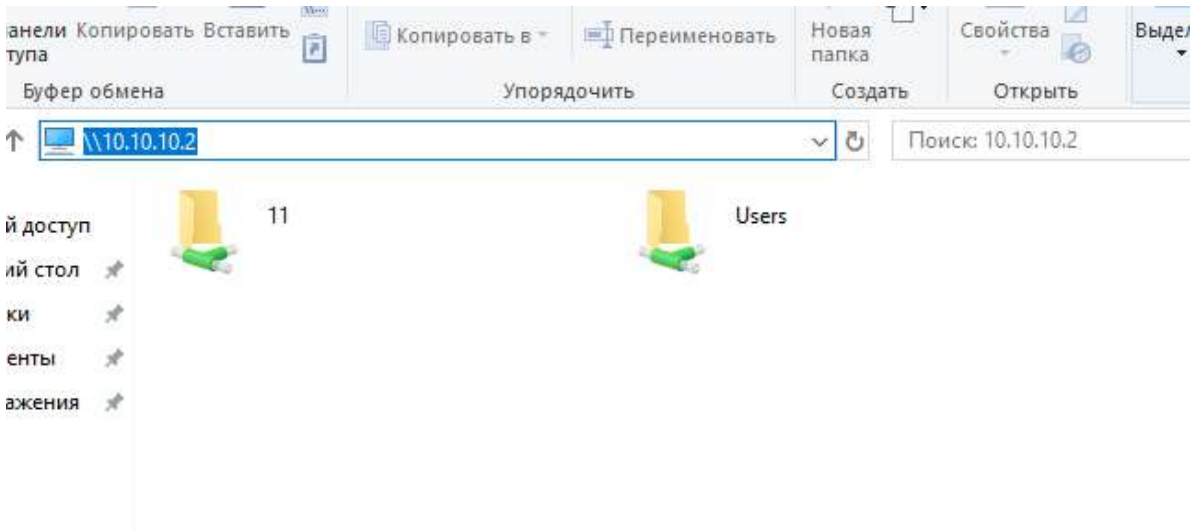


Рисунок 4.10 – Отключение парольной защиты

Контрольные вопросы

1) Что такое VPN?

2) Какие существуют уровни протоколов защищенного канала?

3) По какому параметру обычно классифицируют VPN?

4) Чем отличаются виртуальные машины для сервера и клиента?

5) Какие типы ключей есть в OpenVPN?

Лабораторная работа № 17

Применение средств защиты информации для контроля целостности операционных систем

Целью данной работы является изучение и приобретение навыков настройки и управления основными защитными механизмами СЗИ от НСД «Secret Net». Рассмотрены принципы обеспечения замкнутой программной среды и настройки контроля целостности.

Краткие теоритические сведения

Механизм контроля целостности (КЦ) предназначен для слежения за неизменностью содержимого ресурсов компьютера. Действие этого механизма основано на сравнении текущих значений контролируемых параметров проверяемых ресурсов и значений, принятых за эталон. Эталонные значения контролируемых параметров определяются или рассчитываются при настройке механизма. В процессе контроля при обнаружении несоответствия текущих и эталонных значений система оповещает администратора о нарушении целостности ресурсов и выполняет заданное при настройке действие, например, блокирует компьютер, на котором нарушение обнаружено.

Механизм замкнутой программной среды (ЗПС) предназначен для ограничения использования ПО на компьютере. Доступ разрешается только к тем программам, которые необходимы пользователям для работы. Для каждого пользователя определяется перечень ресурсов, в который входят разрешенные для запуска программы, библиотеки и сценарии. Попытки запуска других ресурсов блокируются, и в журнале безопасности регистрируются события несанкционированного доступа (НСД).

На этапе настройки механизма ЗПС составляется список ресурсов, разрешенных для запуска и выполнения. Список может быть сформирован автоматически на основании сведений об установленных на компьютере программах или по записям журналов, содержащих сведения о запусках программ, библиотек и сценариев. Также предусмотрена возможность ручного формирования списка. Для файлов, входящих в список, можно включить режим контроля целостности. По этой причине механизм замкнутой программной среды и механизм контроля целостности используют единую модель данных.

При включенном «мягком» режиме работы подсистемы замкнутой программной среды контролируются попытки запуска программ, библиотек и сценариев, но разрешается использование любого ПО. Этот режим обычно используется на этапе настройки механизма ЗПС. Помимо параметра «Мягкий» режим в свойствах субъекта управления есть еще три параметра:

– Проверять целостность модулей перед запуском. Этот параметр отвечает за проверку целостности программ перед их запуском.

– Проверять заголовки модулей перед запуском. При установке этого параметра в процессе контроля включается дополнительный механизм, повышающий надежность разделения ресурсов на исполняемые и неисполняемые файлы, т. е. подлежащие и не подлежащие проверке.

– Контролировать исполняемые скрипты. Этот параметр отвечает за блокировку выполнение сценариев (скриптов), не входящих в перечень разрешенных для запуска и не зарегистрированных в базе данных системы Secret Net.

Для управления режимами замкнутой программной среды и контроля целостности, а также моделью данных используется программа «Контроль программ и данных». Окно программы (рис. 2) содержит следующие элементы:

(1) – Меню. Содержит команды управления программой.

(2) – Панель инструментов. Содержит кнопки быстрого вызова команд управления.

(3) – Информационный заголовок. Содержит название выбранной для отображения категории объектов.

(4) – Панель категорий. Содержит ярлыки для выполнения одноименных команд меню «вид».
(5) – Область списка объектов.
(6) – Окно структуры.
(7) – Окно зависимостей. Содержит список объектов, связанных с объектом, который выбран в области списка объектов. В верхней части окна расположены кнопки, управляющие фильтрацией объектов списка.
(8) – Строка состояния. Содержит служебные сообщения программы.

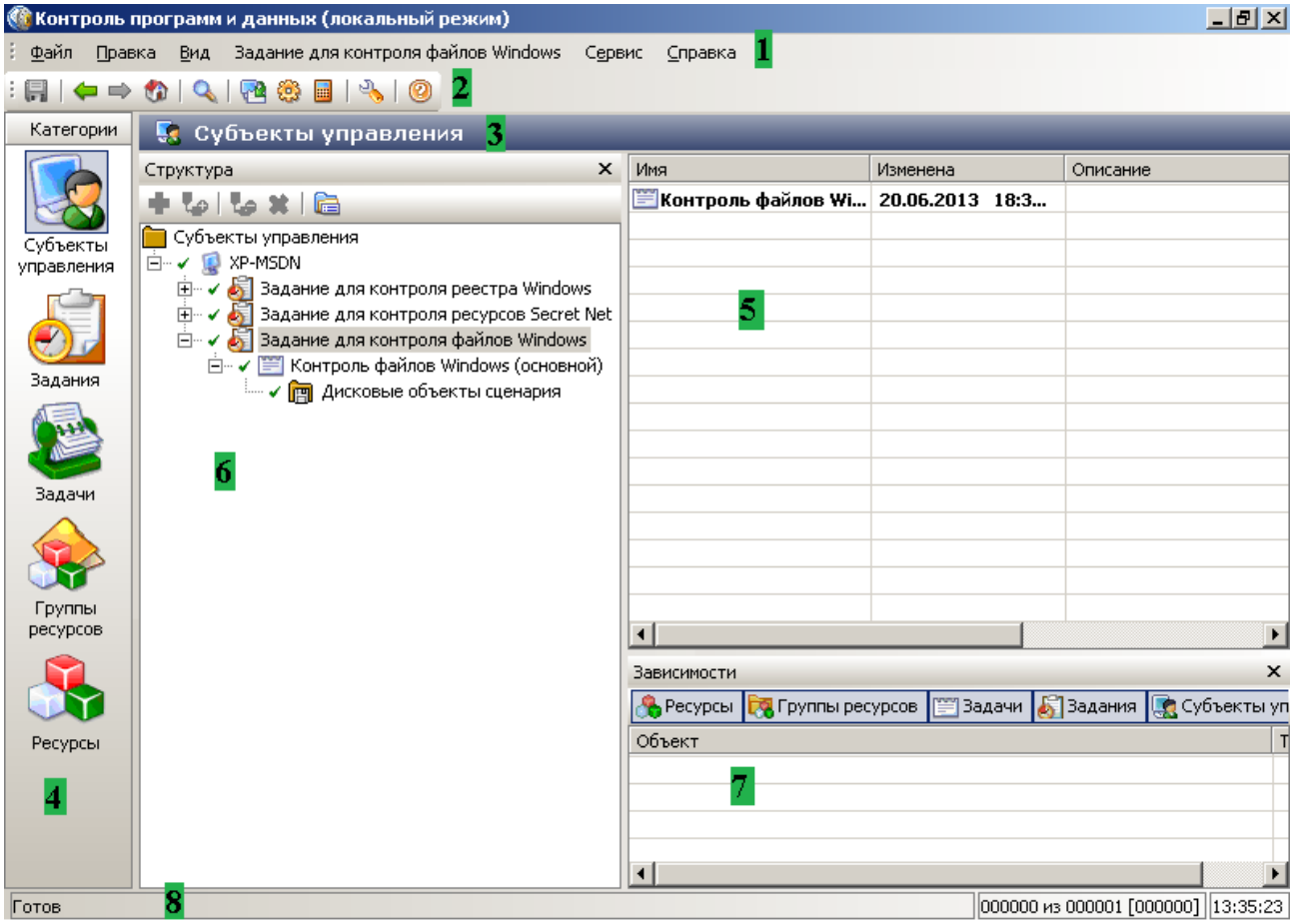


Рисунок 2 – Окно программы “Контроль программ и данных”

Требования для выполнения работы

Для начала работы необходимо иметь установленную систему виртуализации VMware Player, VMware Workstation или Virtual Box, а также скачать архив с виртуальной машиной «Secret Net Client». Скачанный архив необходимо разархивировать.

Убедитесь, что вы запускаете виртуальную машину на системе виртуализации, соответствующей названию скачанного архива.

Желательно убедиться, что в настройках виртуальной машины выбран тип сетевого адаптера «Только для узла» («Host-only») в случае, если используется система виртуализации VMware. При наличии на хосте оперативной памяти большого объема, можно увеличить выделяемый виртуальной машине объем ОЗУ (по умолчанию установлен 256 МБ).

Ход работы

1. Запустите виртуальную машину «Secret Net Client». Для настройки конфигурации виртуальной машины VMware задаст вопрос о том была ли она скопирована или перемещена

(рис. 3), выберите вариант «I Moved It» (виртуальная машина перемещена). После загрузки операционной системы войдите под локальной учетной записью «**Администратор**», пароль 12345 (рис. 4). Будет необходимо выбрать параметр «Вход в: XP-MSDN (этот компьютер)». После этого будет выведено сообщение об изменении аппаратной конфигурации. Снимите блокировку рабочей станции (Да) и выполните следующее:

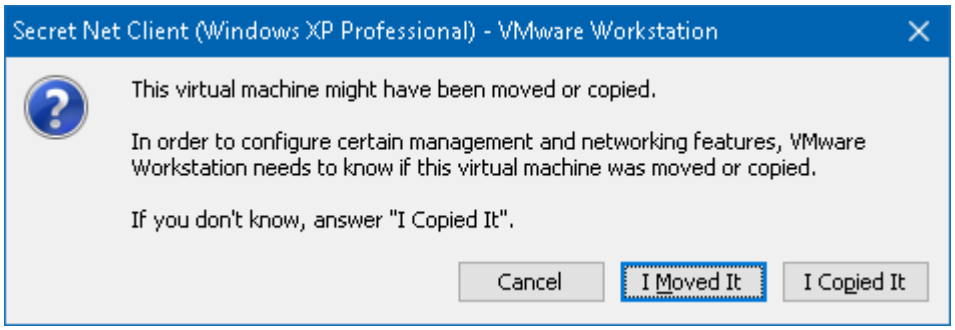


Рисунок 3 – Запрос конфигурации при запуске виртуальной машины

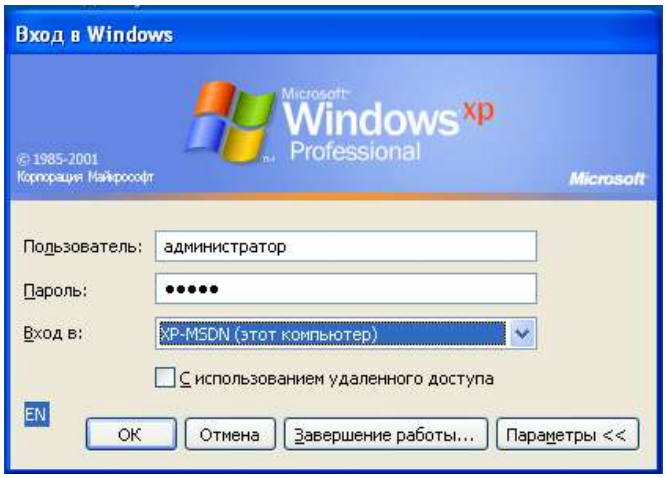


Рисунок 4 – Вход в систему под локальной учетной записью

Откройте свойства учетной записи **Администратор** (Мой компьютер- Управление - Локальные пользователи- Пользователи - Администратор). Измените уровень допуска на строго конфиденциально (Вкладка Secret Net 7 - Доступ), разрешите управление категориями конфиденциальности, вывод и печать конфиденциальных документов (рис. 5). Создайте учетные записи **user** и **conf**. Настройте пользователю **conf** категорию доступа конфиденциально и добавьте возможность печати конфиденциальных документов (рис. 6). Для пользователя **user** по умолчанию задан уровень допуска «Неконфиденциально».

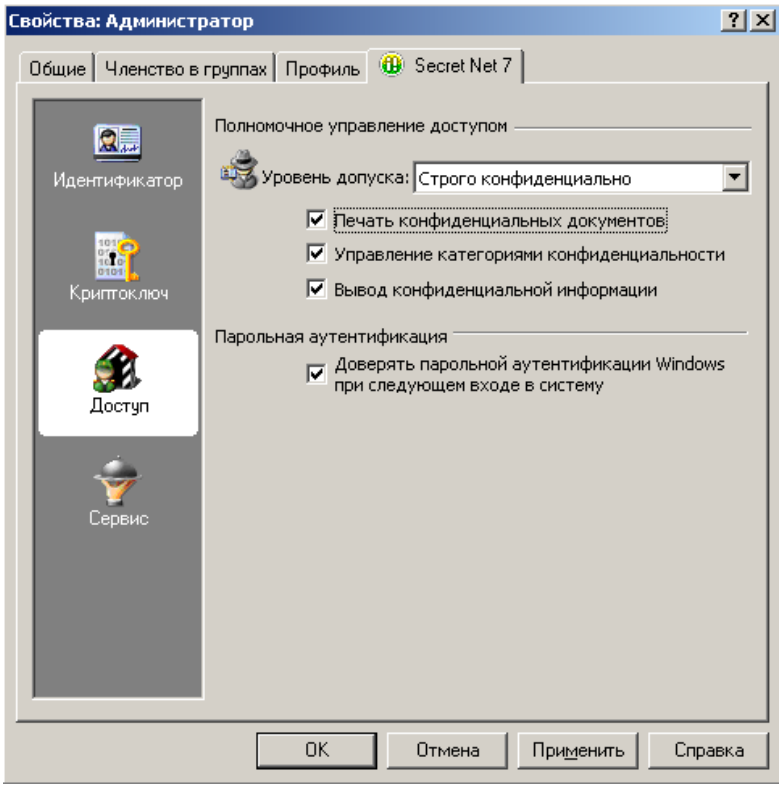


Рисунок 5 – Параметры управления полномочным доступом для пользователя Администратор

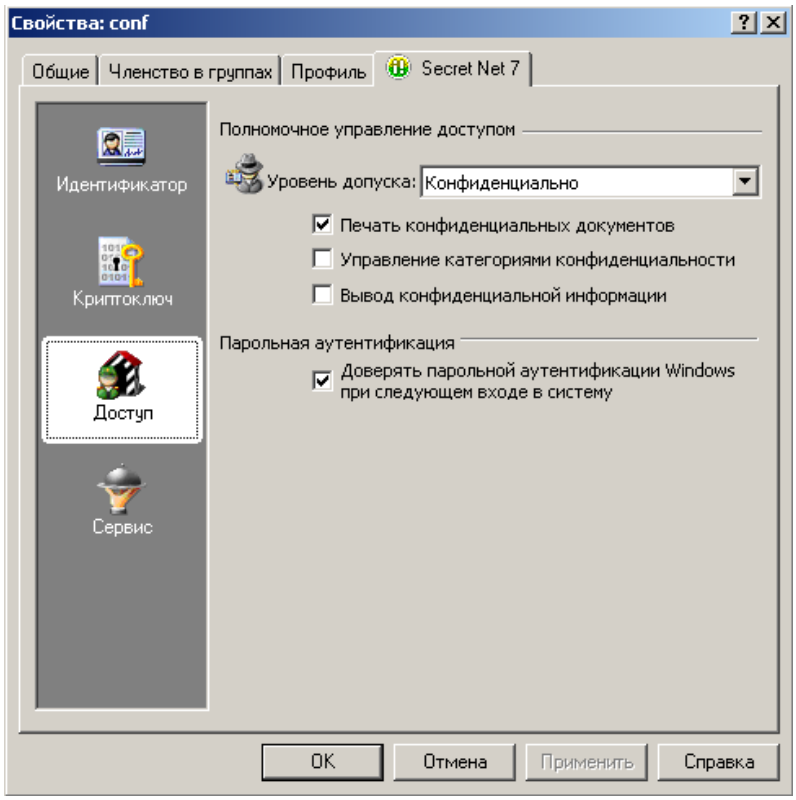


Рисунок 6 – Параметры управления полномочным доступом для пользователя conf

Измените разрешения на доступ к диску «D:\» (Диск D – Свойства – Безопасность – Все – Полный доступ). Измените у папки «D:\temp» категорию конфиденциальности на «Конфиденциально», изменив категорию и у всех вложенных файлов (рис. 14). Отдельно файлу «D:\temp\Неконф.txt» задайте категорию «Неконфиденциально».

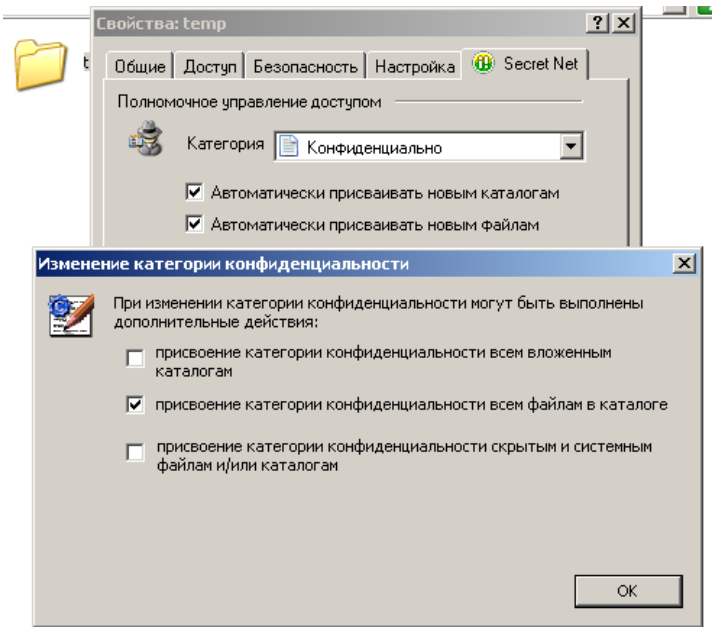


Рисунок 14 – Изменение уровня конфиденциальности папки temp

Настройка механизмов контроля целостности и замкнутой программной среды

8. Войдите под учетной записью **Администратор**. Для запуска программы необходимо выбрать следующую команду «Пуск \Все программы \Код Безопасности \SecretNet \Контроль программ и данных».

Перед тем как произвести построение фрагмента модели данных системой проводится анализ размещения программного обеспечения и данных на защищаемом компьютере, формируются требования к настройке контроля целостности и замкнутой программной среды, который включает в себя:

- сведения о защищаемом компьютере (установленное ПО, пользователи и их функциональные обязанности, задачи, решаемые пользователями в рамках бизнес-процессов);

- перечень ресурсов, подлежащих контролю целостности;

- перечень программ, с которыми разрешено работать разным группам пользователей;

- задачи (список задач и их краткое описание).

Для построения фрагментов модели данных в программе КЦ-ЗПС выбираем команду «Файл \Новая модель данных». В ней предоставляется возможность детальной настройки параметров для формирования новой модели данных (рис. 18). Нажмите ОК для создания стандартной модели (для тех файлов, где появятся ошибки выберите вариант снять с контроля). В эту модель можно добавить файлы операционной системы и Secret Net для контроля их целостности и создания ЗПС. Помимо стандартных задач, в модель можно добавить задачи, сформированные на основе ресурсов приложений. Добавление таких задач осуществляется с помощью параметра «Добавить другие задачи из списка». После успешного формирования модели данных в основном окне программы управления КЦ-ЗПС появится новая структура, включающая в себя субъект «Компьютер» с назначенными для него заданиями.

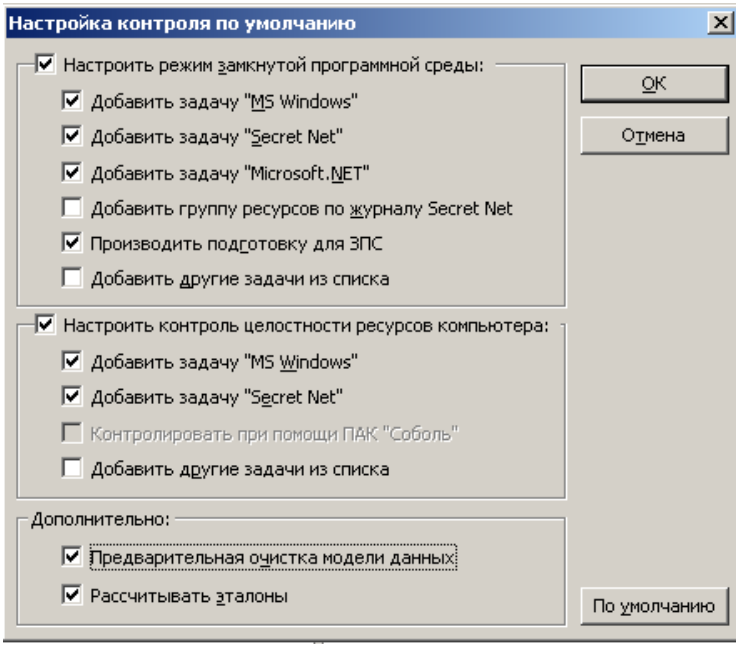


Рисунок 18 – Настройка контроля целостности и ЗПС для стандартных объектов.

9. После того, как произойдет подготовка ресурсов для использования замкнутой программной среды, в левой части окна выберите категорию «Задания» и выберите в меню «Задания \Создать задание». На экране появится диалог выбора типа задания. Выбираем «Замкнутая программная среда» и нажимаем на кнопку «ОК» (рис 19). Затем введите имя задания и продолжите работу, нажав на кнопку «ОК».

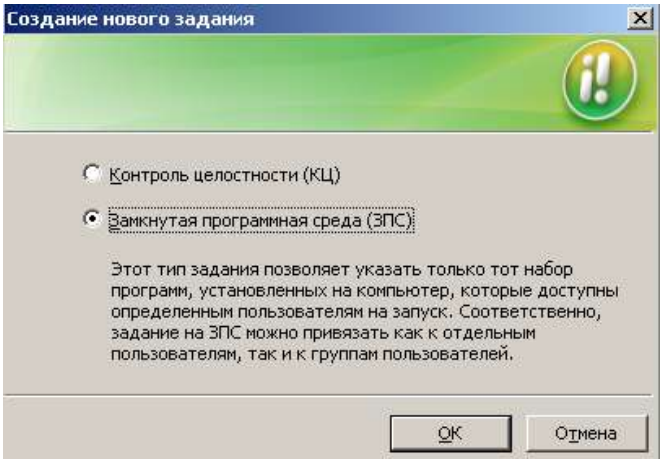


Рисунок 19 – Выбор типа задания

После чего, новое задание будет отображаться в окне структуры (рис).

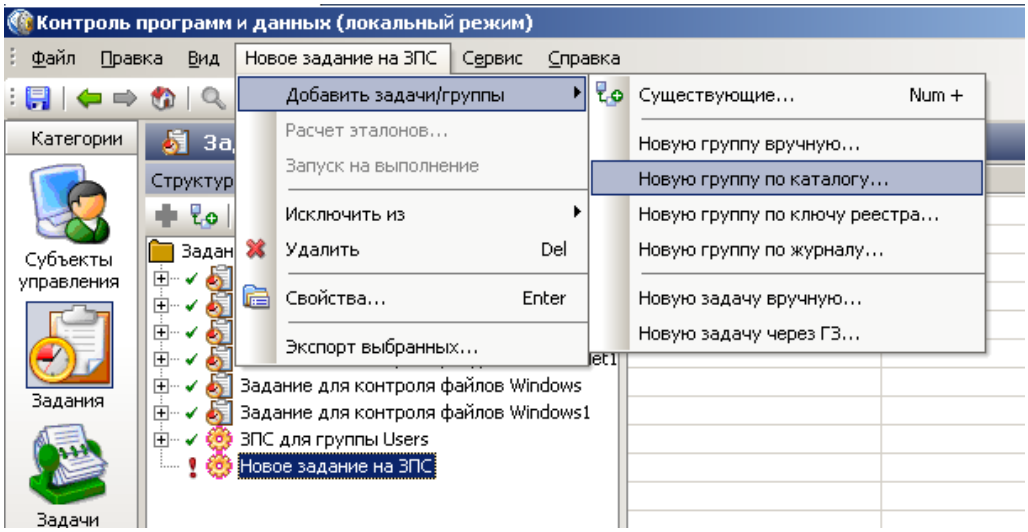


Рисунок 20 – Добавление группы ресурсов в задание на ЗПС

10. Выделите созданное задание на ЗПС. Открыв правой кнопкой мыши контекстное меню выберите «Добавить задачи \группы-Новую группу по каталогу…» (рис. 20). В окне выбора добавьте каталог «C:\Program Files\Movie Maker» и нажмите «ОК». На панели категорий выберите «Субъекты управления» и нажмите «Добавить в список» (рис.21). Введите имя выбираемого объекта «**user**» и нажмите «ОК» (рис. 22).

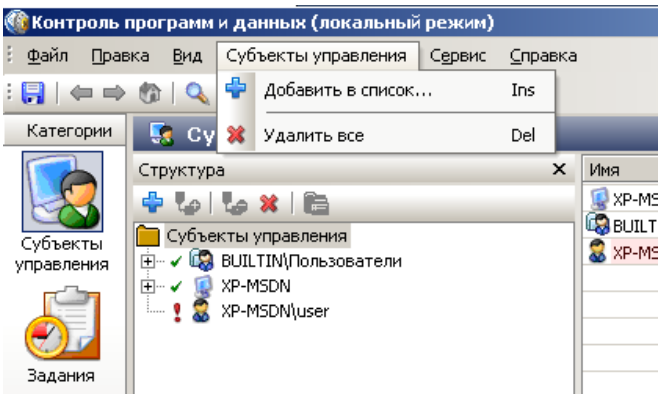


Рисунок 21 – Добавление контролируемого пользователя

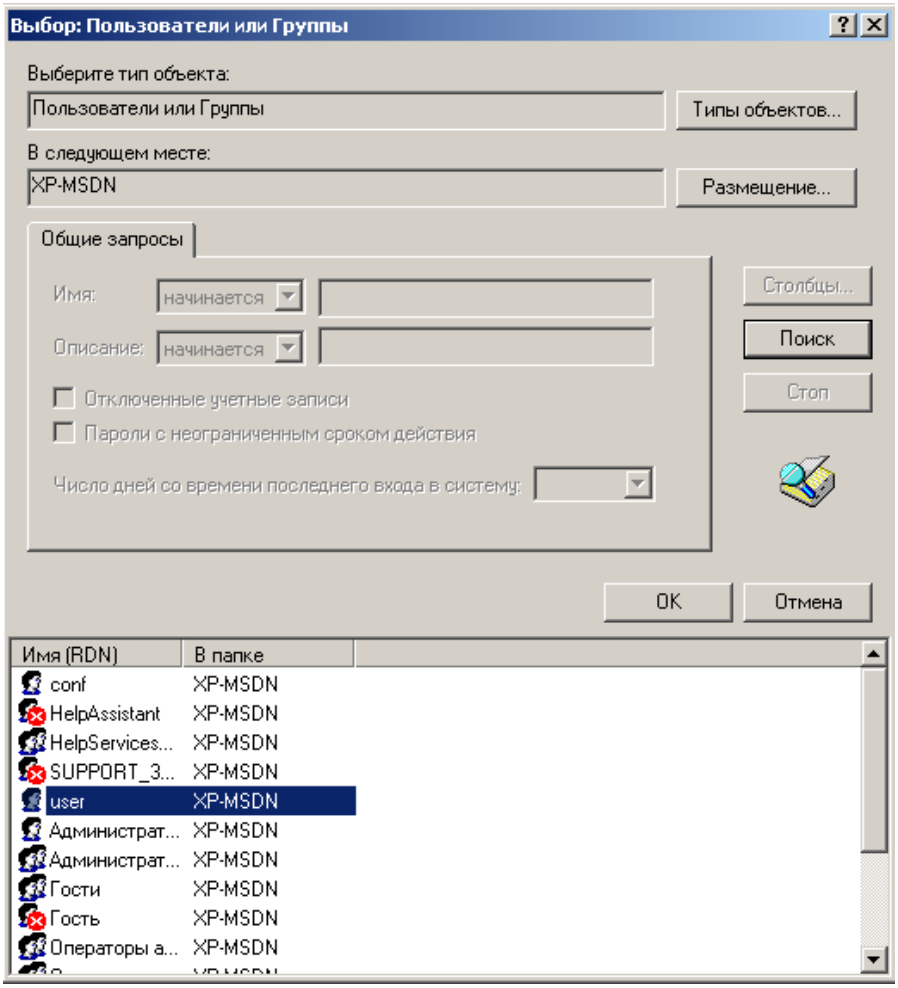


Рисунок 22 – Выбор пользователя user

11. Выделите добавленного пользователя. В меню выберите «XP-MSDN\user>Добавить задания > Существующие...», в открывшимся окне выберите «Новое задание на ЗПС» и нажмите «ОК». Теперь пользователя **user** выбранный каталог будет входить в ЗПС, а следовательно, программы находящиеся в каталоге будут разрешены к запуску. Для того, чтобы ЗПС функционировала необходимо включить «Жесткий режим». Для этого необходимо выполнить следующее:

- выбрать категорию «Субъекты управления» на панели категорий.

- выбрать в дополнительном окне структуры группу «XP-MSDN», вызовите контекстное меню и выберите команду «Свойства». В появившемся окне перейдите к вкладке «Режимы» (рис.23).

- установите отметку в поле «Режим ЗПС включен» и удалите отметку в поле «Мягкий режим».

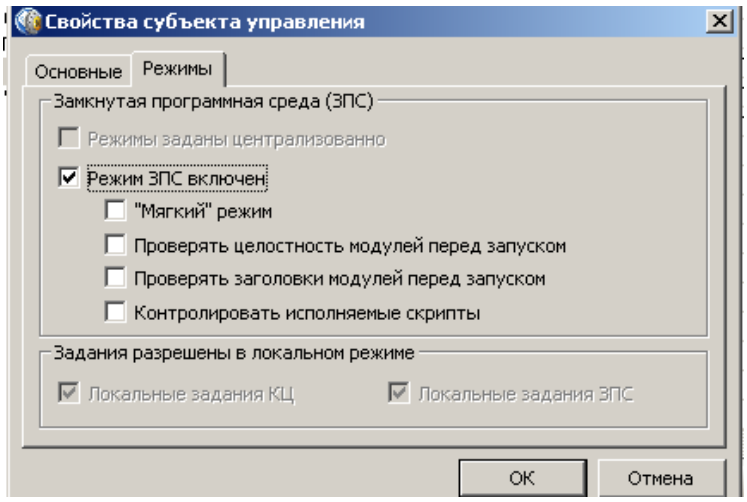


Рисунок 23 – Настройка режима ЗПС

После проделанных действий замкнутая программная среда будет работать в «Жестком режиме». То есть будут разрешены для запуска только те программы, которые добавлены в задания на ЗПС. На учетную запись «**Администратор**» ЗПС не действует, так как в групповых политиках была задана данная привилегия.

12. Закройте программу, сохранив модель. Войдите под учетной записью «**user**». Попробуйте поработать в операционной системе, результаты зафиксируйте в отчете. Интерфейс Windows должен отображаться некорректно, так как не все файлы, нужные для корректной работы системы были добавлены в ЗПС. Для того чтобы это исправить необходимо обучить модель в «мягком» режиме.

Войдите под учетной записью «**Администратор**» и включите «мягкий» режим работы ЗПС (как в п. 11). Сохраните модель. Войдите под учетной записью **user** и запустите Movie Maker («C:\Program Files\Movie Maker\moviemk.exe»). Теперь все необходимые для корректной работы программы будут записаны в журнал Secret Net.

Войдите под учетной записью **Администратор** и добавьте в задание на ЗПС файлы из журнала Secret Net: под учетной записью **Администратор** откройте Контроль программ и данных, выберите Файл-Новая модель данных, задав режим ЗПС с добавлением группы ресурсов по журналу Secret Net (рис. 24). В этом случае Secret Net разрешит запускаться программам, записи о попытках запуска которых отмечены журналах Secret Net. Файлы без ЭЦП игнорировать. Далее включите жесткий режим ЗПС (как в п.11) и сохраните модель.

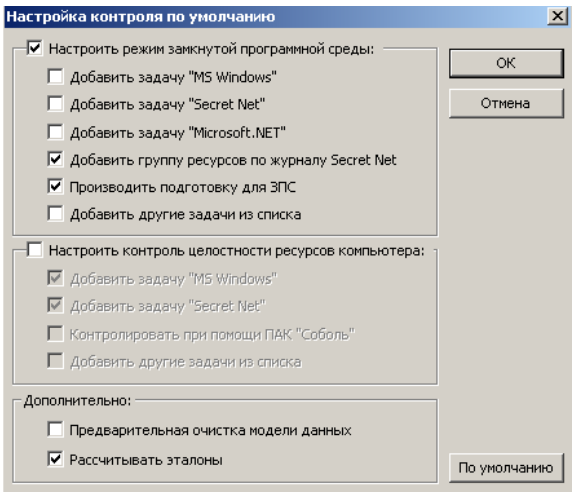


Рисунок 24 – Добавление группы ресурсов по журналу Secret Net

Войдите под учетной записью **user**. Запустите программу Windows Movie Maker и убедитесь в возможности ее запуска.

Запустите Windows Media Player(«C:\Program Files\Windows Media Player\wmplayer.exe»). Попробуйте запустить другие программы. Результаты зафиксируйте в отчете. После проверок выключите ЗПС.

Настройка контроля целостности

Контроль целостности настраивается для тех файлов, для которых критична их неизменность. Сюда могут входить исполняемые файлы и библиотеки операционной системы и другие важные файлы.

13. Войдите под учетной записью «**Администратор**». Запустите программу «Пуск \Все программы\Код Безопасности\Secret Net\Контроль программ и данных». Выберите категорию «Задания» и выберите в меню «Задания \Создать задание». На экране появится диалог выбора типа задания. Выбираем «Контроль целостности» и нажимаем на кнопку «ОК» (рис.25).

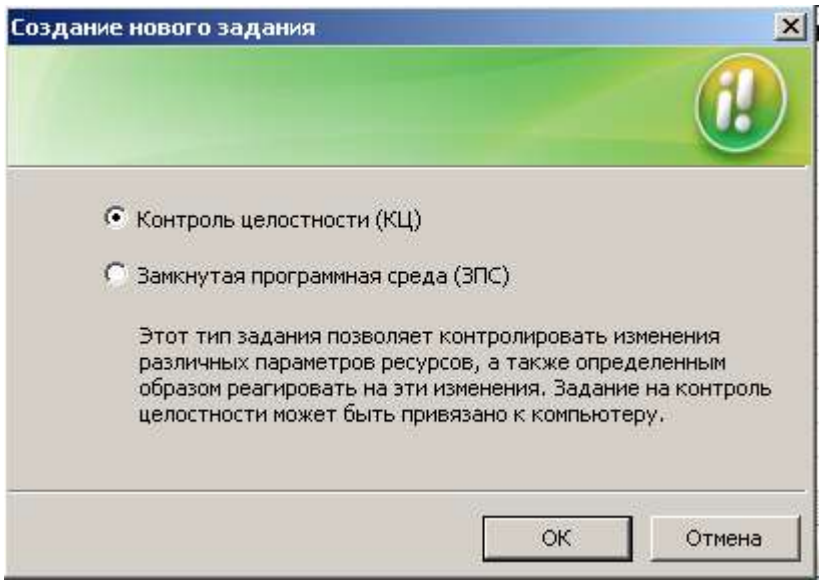


Рисунок 25 – Создание задания на КЦ

После того, как выбран тип «Контроль целостности», появится окно «Создание нового задания на КЦ» (рис.26). В данном окне задайте имя «Новое задание на КЦ». В методе контроля ресурсов выберите «Содержимое», а для параметра «Реакция на отказ» выставить значение «Заблокировать компьютер». Ниже приведены описания методов контроля и то, что будет проверяться.

Методы контроля:

- Содержимое. Проверяется целостность содержимого ресурсов;
- Атрибуты. Проверяются стандартные атрибуты, установленные для ресурсов;
- Права доступа. Проверяются категории конфиденциальности, установленные для ресурсов;
- Существование. Проверяется наличие ресурсов по заданному пути.

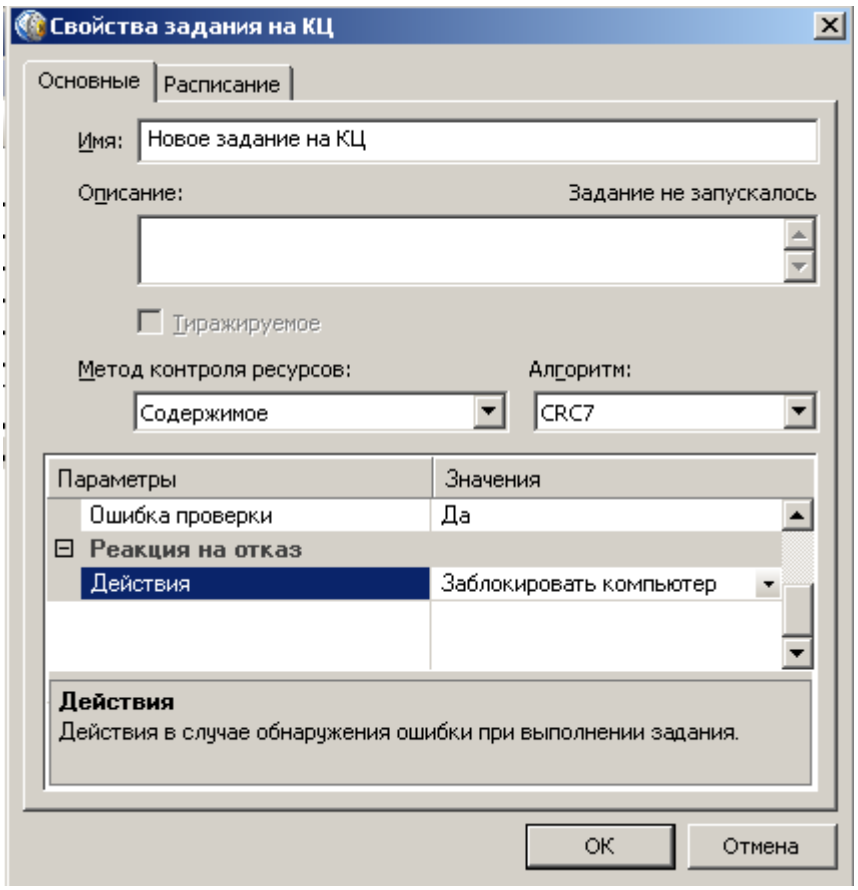


Рисунок 26 – Окно настроек задания на контроль целостности

Перейдите к вкладке «Расписание» (рис.27). Во вкладке «Расписание» выберите поля «При загрузке ОС», «При входе». Также можно настроить по каким дням и месяцам будет выполняться контроль целостности. Для этого установите КЦ с июня по декабрь и с понедельника по воскресенье и нажмите кнопку «ОК».

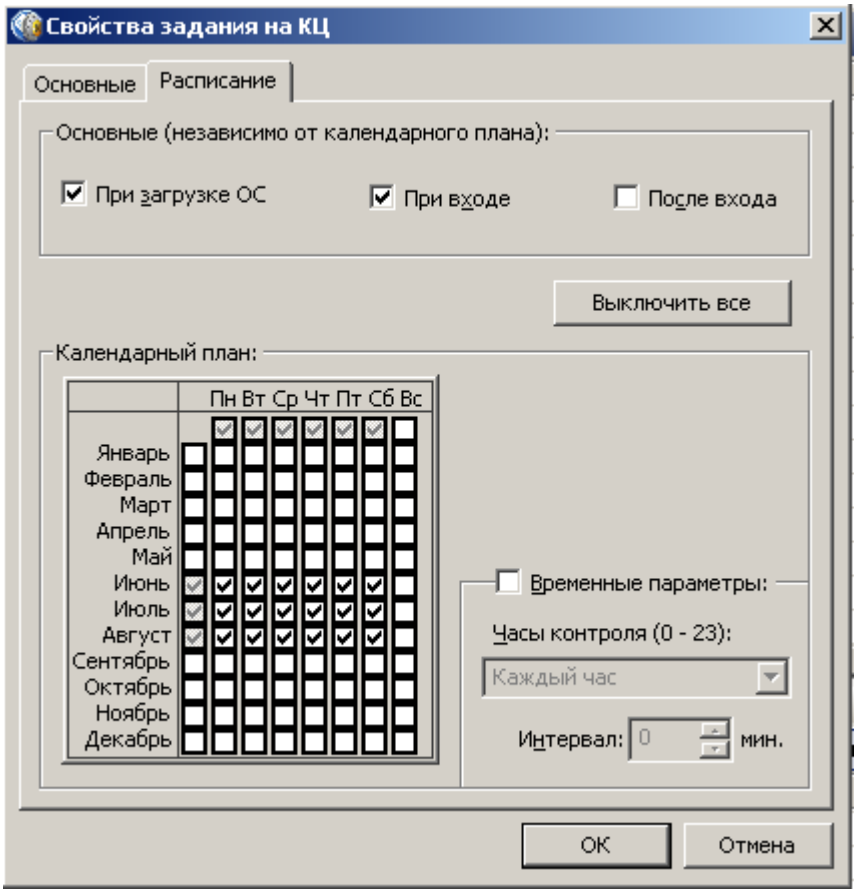


Рисунок 27 – Настройка расписания контроля целостности

14. Необходимо задать контроль целостности для данного компьютера. Для этого перейдите к вкладке «Субъекты управления», выберите «XP-MSDN» и вызовите контекстное меню и добавьте задание «Новое задание на КЦ». Перейдите к категории «Задания», вызовите контекстное меню нового задания на КЦ и добавьте ресурс по каталогу «D:\Temp». Произведите расчет эталонов для файлов, заданных на контроль целостности: В контекстном меню «Нового задания на КЦ» – Расчет эталонов (или Сервис – Эталоны – Расчет, если нужно рассчитать все эталоны). Установите галочку оставлять старые и нажмите ОК. Сохраните изменения выбрав в меню «Файл» - «Сохранить». Зайдите под учетной записью «**conf**» и измените содержимое файла «Конф.txt» в папке «Temp» находящейся на диске «D:\». Попробуйте заново войти в систему под учетной записью «**conf**». Результаты зафиксируйте в отчете.

Для того, чтобы компьютер каждый раз не блокировался по причине нарушения целостности, войдите под учетной записью Администратор и пересчитайте эталоны для созданного задания на КЦ. Тем самым мы обновляем эталоны для измененных файлов, находящихся на контроле целостности.

Задание:

Проделайте ход работы, зафиксировав полученные результаты в отчете. Создайте учетную запись, соответствующую имени в кафедральной сети (либо из ФИО). В зависимости от номера варианта задайте учетной записи пользователя категорию конфиденциальности:

- Четный – «Строго конфиденциально»;
- Нечетный, делится на 3 – «Конфиденциально»;
- Нечетный, остальные – «Не конфиденциально».

Для данной учетной записи проделайте следующие действия:

1. Создайте замкнутую программную среду в «жестком режиме» для ресурса «C:\Program Files \Internet Explorer» для созданной учетной записи пользователя.

2. Настройте контроль целостности для ресурса «D:\Полный доступ». Попытайтесь подменить содержащийся в данной папке файл «notepad.exe» файлом «C:\Windows\Regedit.exe». Проверьте работу механизма контроля целостности.

Контрольные вопросы

1. Для чего предназначен механизм контроля целостности (КЦ)?

2. Для чего предназначен механизм замкнутой программной среды?

3. Чем отличается «мягкий» режим ЗПС от «жесткого»?

4. Перечислите методы контроля целостности, используемые Secret Net.

5. Перечислите реакции на нарушение целостности файлов.

6. Для каких файлов следует настраивать контроль целостности?

Лабораторная работа № 18
Централизованная защита от вирусов в локальной сети

Цель лабораторной работы

Целью лабораторной работы является ознакомление с программным продуктом Kaspersky Security Center и изучение его основных функциональных возможностей.

Теоретические сведения

Основное назначение Kaspersky Security Center – предоставление администратору инструментов для настройки всех компонентов системы защиты и доступа к детальной информации об уровне безопасности корпоративной сети. Kaspersky Security Center является единым средством для централизованного управления большим набором средств защиты в организации, предоставляемым «Лабораторией Касперского». Набор программных продуктов, которыми можно управлять при помощи Kaspersky Security Center, включает в себя решения для защиты рабочих станций, серверов и мобильных устройств (рисунок 1):

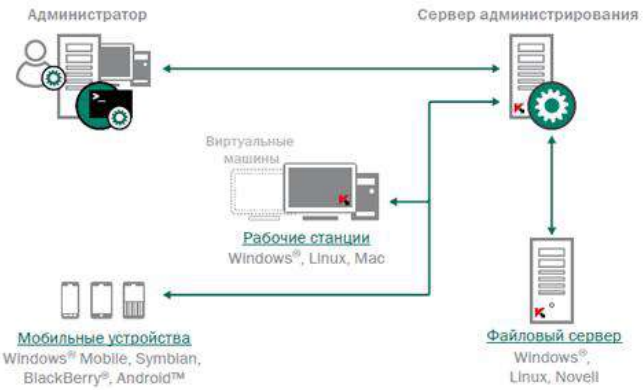


Рисунок 1 – Логика использования Kaspersky Security Center при защите сети организации.

Kaspersky Security Center является не отдельной программой, а комплексом программных средств, который включает в себя (рисунок 2):

–сервер администрирования – служба, отвечающая за управление безопасностью. Является основным модулем Kaspersky Security Center и хранит всю информацию об управляемых компьютерах в базе данных (MS SQL Server или MySQL). Помимо основного сервера администрирования можно организовать иерархическую структуру серверов администрирования для работы через них с удаленными частями локальной сети или локальной сетью обслуживаемой организации. Это особенно актуально для компаний,

структура которых является распределенной. В этом случае локальные пользователи обращаются только к своему серверу.

–консоль администрирования – модуль, реализованный в виде оснастки для Microsoft Management Console и предназначенный для управления сервером администрирования;

–веб-консоль – веб-приложение, имеющее аналогичное консоли администрирования предназначение. Различие заключается в том, что веб-консоль позволяет получать доступ к серверу администрирования через браузер, используя веб-интерфейс. Однако, по сравнению с той же консолью администрирования, имеет ограниченные возможности по управлению;

–агент администрирования Kaspersky Security Center – программа, предназначенная для взаимодействия между сервером администрирования и клиентскими компьютерами. Она устанавливается на клиентские системы и позволяет получать информацию о текущем состоянии программ и о событиях, произошедших на клиентских компьютерах, отправлять и получать команды управления, а также обеспечивает функционирование агента обновлений.

–модули управления программами – модули, которые устанавливаются на рабочее место администратора. Предназначение – получение доступа к программным продуктам «Лаборатории Касперского» в организации через консоль администрирования.

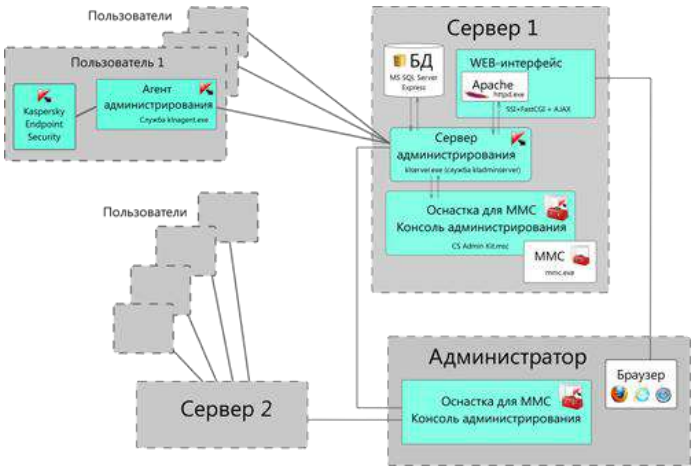


Рисунок 2 – Структурная схема взаимодействия компонентов Kaspersky Security Center.

Из схемы видно, что администратор имеет возможность работать посредством оснастки с несколькими серверами администрирования, являющимися, к примеру, серверами компании, расположенными в разных офисах. Кроме того, администратор имеет возможность получить доступ к серверу администрирования через интернет-

браузер с любого компьютера без необходимости устанавливать на него какие-либо модули, что может быть полезно при необходимости мониторинга системы безопасности. Данный способ доступа также применяется при разворачивании защиты в организации внешним поставщиком услуг, доступ к серверу администрирования которого из защищаемой сети как раз и можно получить при помощи веб-консоли (рисунок 3).

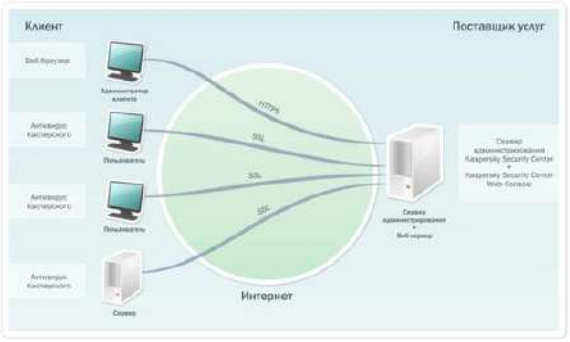


Рисунок 3 – Схема использования веб-консоли.

Kaspersky Security Center позволяет настраивать и управлять компонентами и настройками на клиентских компьютерах. Для каждой группы пользователей или конкретного пользователя администратор может задавать различные настройки следующих компонентов (рисунок 4):

1. Компоненты защиты: файловый антивирус, почтовый антивирус, веб-антивирус, IM-антивирус, сетевой экран, защита от сетевых атак, мониторинг сети, мониторинг системы.

2. Компоненты контроля: контроль запуска программ, контроль активности программ, поиск уязвимостей, контроль устройств, веб-контроль.

Рисунок 4 – Схема компонентов, управляемых Kaspersky Security Center.

Kaspersky Security Center является развитием инструмента Kaspersky Administration Kit. По сравнению с ним в Kaspersky Security Center был добавлен набор новых функций.

Появилась возможность создавать виртуальные серверы администрирования, добавлено управление работой компонентов «Контроль программ», «Контроль уязвимостей», «Веб-контроль» и «Контроль устройств» появилась веб-консоль для управления сервером администрирования через браузер, добавлены функции управления клиентами на виртуальных машинах, появилась возможность централизованно обнаруживать и устранять уязвимости на клиентских компьютерах. Существенно расширены функции инструментов для управления инсталляциями различных компонентов, получения дополнительной информации о контролируемых компьютерах, создания отчетов и работы с учетными записями.

Ход работы

Во время выполнения хода работы следует использовать имена задач, политик и других объектов системы с именами, содержащих в себе **имя учетной записи в кафедральной сети** (либо ФИО).

Запустите серверную и клиентскую виртуальные машины. Войдите в домен под учетной записью Администратор. Запустите консоль Kaspersky Security Center.

Внешний вид консоли Kaspersky Security Center 10 представлен на рисунке 5. Инструменты для системного администрирования интегрированы в различные разделы консоли.

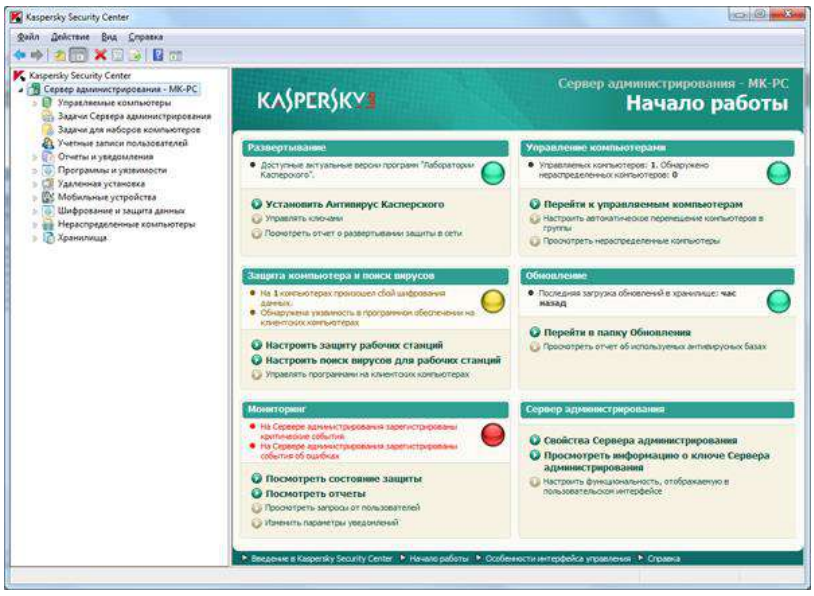


Рисунок 5 – Главное окно при работе с Kaspersky Security Center 10.

Средства системного администрирования

Добавьте клиентский компьютер в список управляемых компьютеров:

1. Выберите раздел “Управляемые компьютеры”:

2. Выберите вкладку Компьютеры и нажмите Добавить компьютеры;
3. Нажмите кнопку “Выбрать компьютеры, обнаруженные в сети сервером администрирования”:
4. Выберите клиентский компьютер из группы Нераспределенные компьютеры.

Одной из задач, решаемых администратором, является установка программного обеспечения на компьютеры в сети. Функции администрирования позволяют создавать инсталляционные пакеты операционных систем и приложений для их централизованной установки на устройства в сети. Работа с этими функциями производится в разделе «Удаленная установка» (рисунок 6).

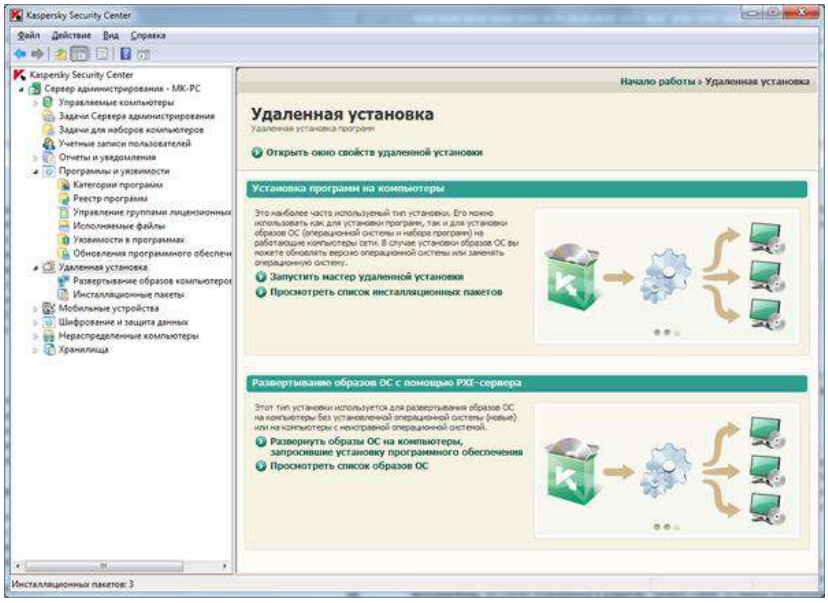


Рисунок 6 – Раздел «Удаленная установка».

Например, чтобы установить программу Kaspersky Endpoint Security на клиентскую машину необходимо:

1. Воспользоваться функцией «Удаленная установка» (Удаленная установка – Запустить мастер удаленной установки).
2. Выберите в списке Kaspersky Endpoint Security.
3. Выберете “Выбрать компьютеры для установки”.
4. Выберите в списке клиентский компьютер.
5. Поставьте галочку “Назначить установку агента администрирования в групповых политиках Active Directory” и нажмите Далее.
6. Оставьте ключ без изменений.
7. Выберите “Перезагрузить компьютер”.
8. Нажмите Далее дважды.
9. Выберите учетную запись Администратор и введите пароль.

10. Запустите установку.

Далее начнется архивация установочного файла для отправки на клиентский компьютер. За ходом установки можно следить во вкладке “Задачи для наборов компьютеров”.

Для установки прикладных программ нужно создать инсталляционные пакеты. При создании нужно выбрать тип сборки – образ операционной системы, программы «Лаборатории Касперского» или произвольное приложение (Удаленная установка – Инсталляционные пакеты – Создать инсталляционный пакет) (рисунок 7).

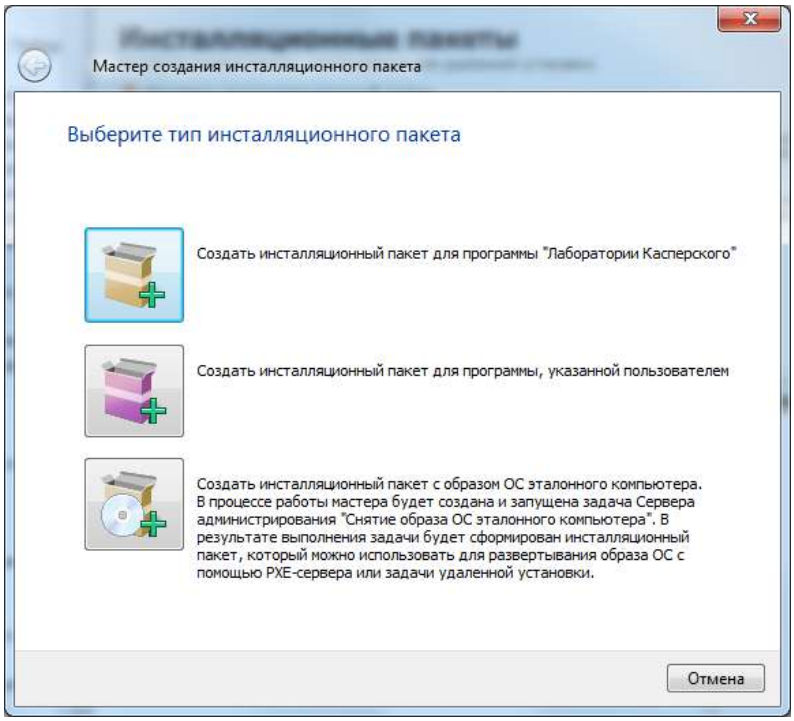


Рисунок 7 – Выбор типа инсталляционного пакета.

Помимо того, что при создании инсталляционного пакета мы можем выбрать любое приложение на компьютере, Kaspersky Security Center 10 предоставляет возможность создать инсталлятор из бесплатных приложений из своей базы данных (7Zip, Adobe Reader, WinZip и т.д., при этом необходимо подключение к Internet) (рисунок 8).

Создайте инсталляционный пакет для программы 7-zip:

1. Выберите создать инсталляционный пакет для программы, указанной пользователем (рис. 7).
2. Введите имя пакета.
3. Выберите файл 7-zip (на рабочем столе).
4. Закончите создание пакета.

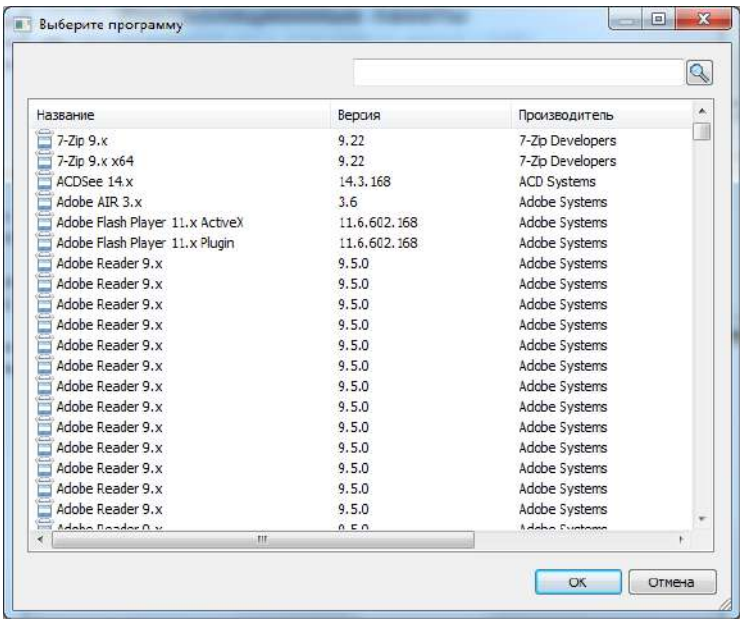


Рисунок 8 – Выбор программы из базы данных «Лаборатории Касперского».

После того как инсталляционный пакет создан, он попадает в хранилище «Инсталляционные пакеты» (Удаленная установка – Инсталляционные пакеты), из которого он может быть установлен на любое количество компьютеров в сети (рисунок 9).

Установите пакет с архиватором 7-zip на клиентский компьютер.

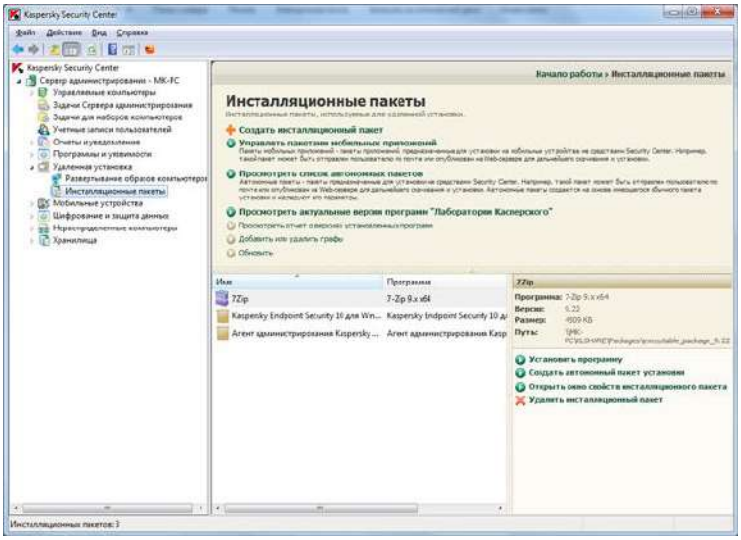


Рисунок 9 – Хранилище «Инсталляционные пакеты».

KSC позволяет создавать и устанавливать на компьютеры образы ОС (**Не выполняется** в рамках данной работы, информация для ознакомления).

Для создания образа операционной системы необходим так называемый «эталонный» компьютер, с которого и будет «сниматься» образ для его дальнейшей установки на другие компьютеры. Чтобы начать работать с образами операционных

систем, вначале нужно установить пакет Windows Automated Installation Kit (WAIK), предназначенный для их установки, настройки и разворачивания.

После этого необходимо создать и запустить задачу для сервера администрирования «Создание инсталляционного пакета на основе образа ОС эталонного компьютера» (Задачи сервера администрирования – Создание образа ОС) (рисунок 10).

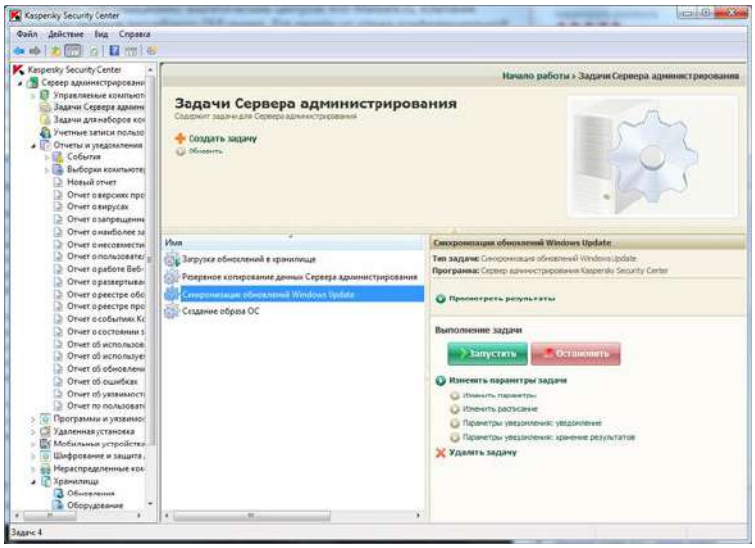


Рисунок 10 – Задача для создания образа операционной системы.

При ее создании нужно указать компьютер для снятия образа; программы Microsoft для включения в образ; категории программного обеспечения, которые нужно обновлять и т.д. (рисунок 11).

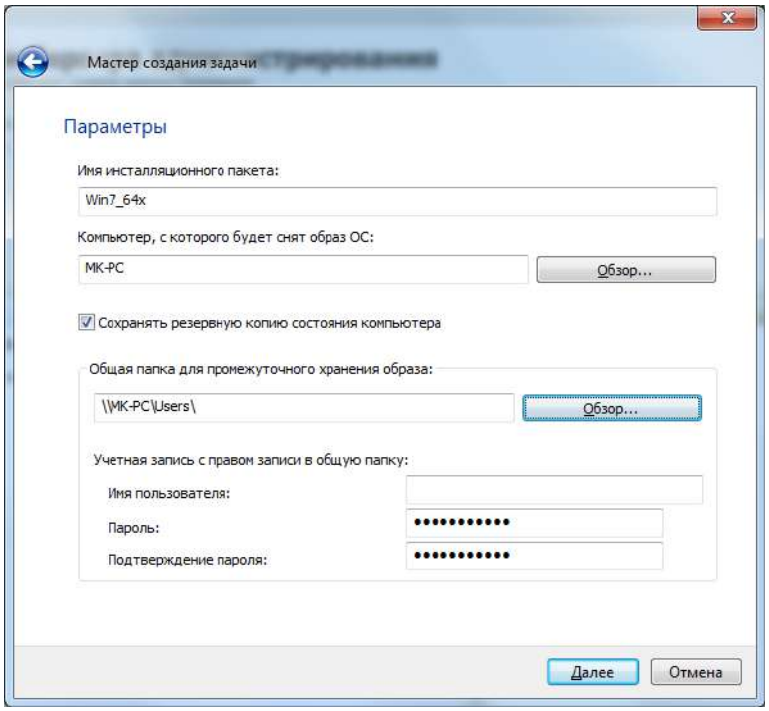


Рисунок 11 – Выбор эталонного компьютера для создания образа операционной системы.

После того как образ был создан, он помещается в хранилище с инсталляционными пакетами, из которого его всегда можно развернуть на выбранных компьютерах. В уже существующие образы администратор может добавлять необходимые для конкретных компьютеров драйвера. Установка образов на компьютеры осуществляется при помощи технологии Preboot eXecution Environment (PXE).

Установка приложений и операционных систем, также как и большинство других действий, производится путем создания необходимого набора задач, запускаемых вручную или по расписанию. Удобной возможностью является удаленное включение компьютеров (WAKE-ON-LINE), позволяющей проводить установку приложений и их обслуживание в нерабочее время, даже если компьютеры уже были выключены сотрудниками.

Примечание: WAKE-ON-LINE – технология, позволяющая удалённо включить компьютер посредством отправки через локальную сеть специальной последовательности байтов (пакета данных).

Инвентаризация

Одной из важных для администратора задач является учет и контроль различных ресурсов. Инструменты для системного администрирования позволяют работать с тремя видами ресурсов – аппаратными устройствами, программным обеспечением и его лицензиями.

Kaspersky Security Center 10 автоматически обнаруживает и ведет учет всех компьютеров и внешних устройств в сети. Это позволяет администратору оперативно реагировать на появления новых устройств (Хранилища – Оборудование) (рисунок 12).

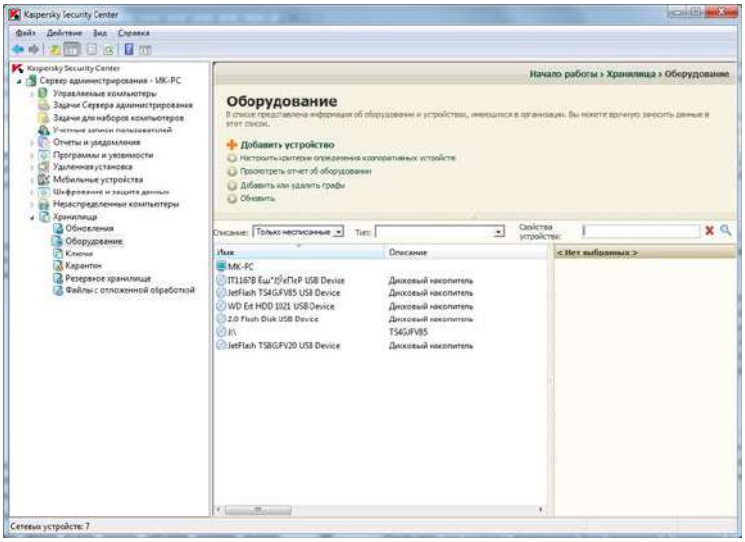


Рисунок 12 – Хранилище оборудования.

Для конкретного компьютера мы можем получить информацию обо всех аппаратных компонентах и подключенных устройствах (Управляемые компьютеры –XP-MSDN – Свойства – Информация о системе – Реестр оборудования). Это может быть полезно при выборе компьютеров, на которые можно устанавливать ресурсоемкие операционные системы или приложения. (рисунок 13).

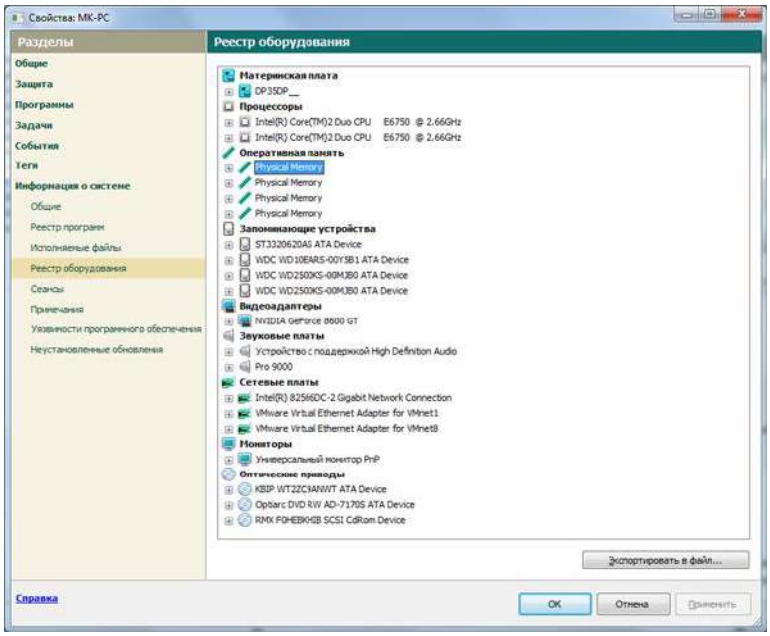


Рисунок 13 – Реестр оборудования.

Для каждого конкретного устройства в его свойствах также можно посмотреть все установленные на нем приложения (Информация о системе – Реестр программ) (рисунок 14). Просмотрите оставшиеся разделы в окне свойств компьютера.

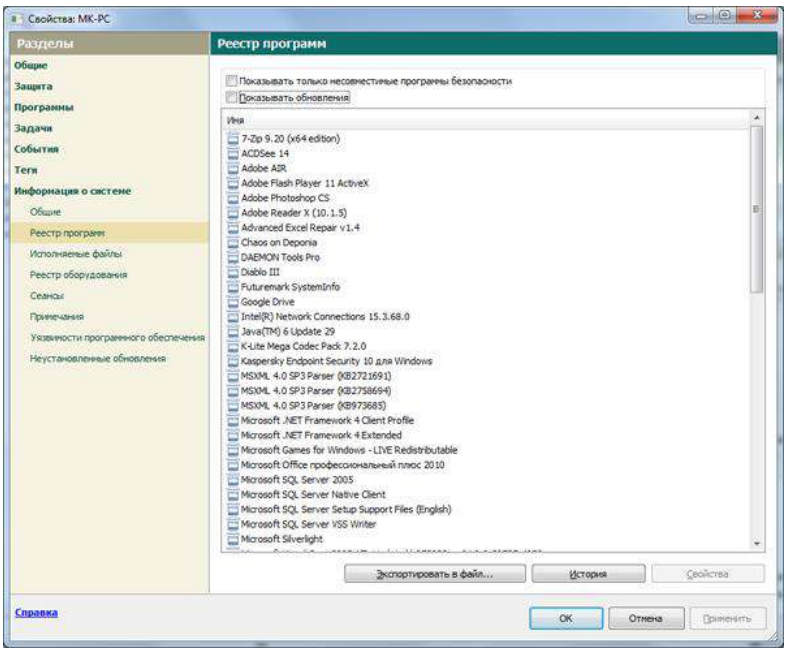


Рисунок 14 – Реестр программ для конкретного устройства.

Реестр программ позволяет контролировать установленное на компьютерах программное обеспечение (Программы и уязвимости – Реестр программ). Данные этого реестра можно использовать для контроля нелицензионных приложений, а также для планирования установки новых лицензионных приложений на компьютеры сотрудников (рисунок 14).

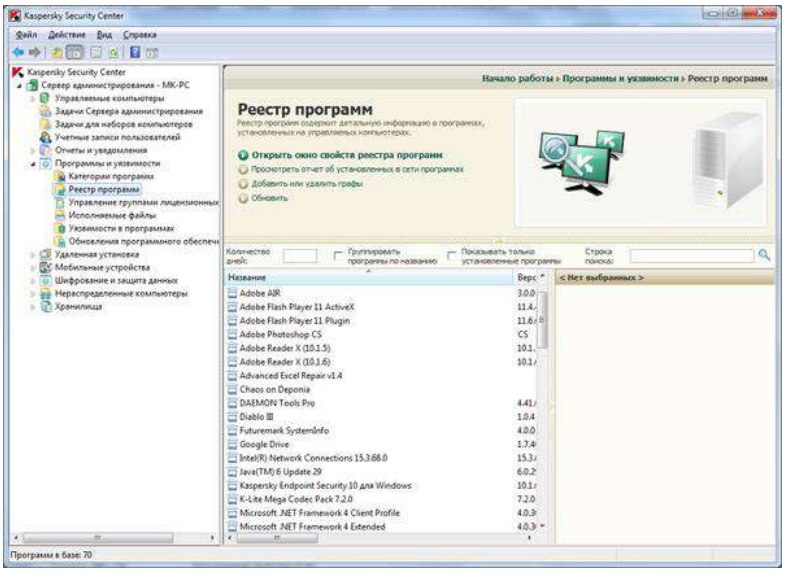


Рисунок 14 – Реестр программ для всех устройств.

Исправление уязвимостей и установка обновлений

Еще одной важной возможностью Kaspersky Security Center 10 является поиск и исправление уязвимостей, а также установка обновлений различных приложений (требуется подключение к Internet). Поиск уязвимости осуществляется при помощи задачи «Поиск уязвимостей и обновлений программ», а закрытие найденных уязвимостей – задачей «Установка обновлений программ и закрытие уязвимостей» (Управляемые компьютеры – Задачи).

Механизм обнаружения и закрытия уязвимостей достаточно прост. Для внесенных в реестр программ проводится сравнение их текущих версий и установленных обновлений с обновлениями, предлагаемыми их разработчиками. Если для какого-либо приложения не установлены последнее обновление, то фиксируется его потенциальная уязвимость и предлагается установить последнее обновление. Закрывать уязвимости можно вручную, анализируя предлагаемые обновления, или можно настроить автоматическое закрытие уязвимостей и разгрузить администратора (рисунок 15).

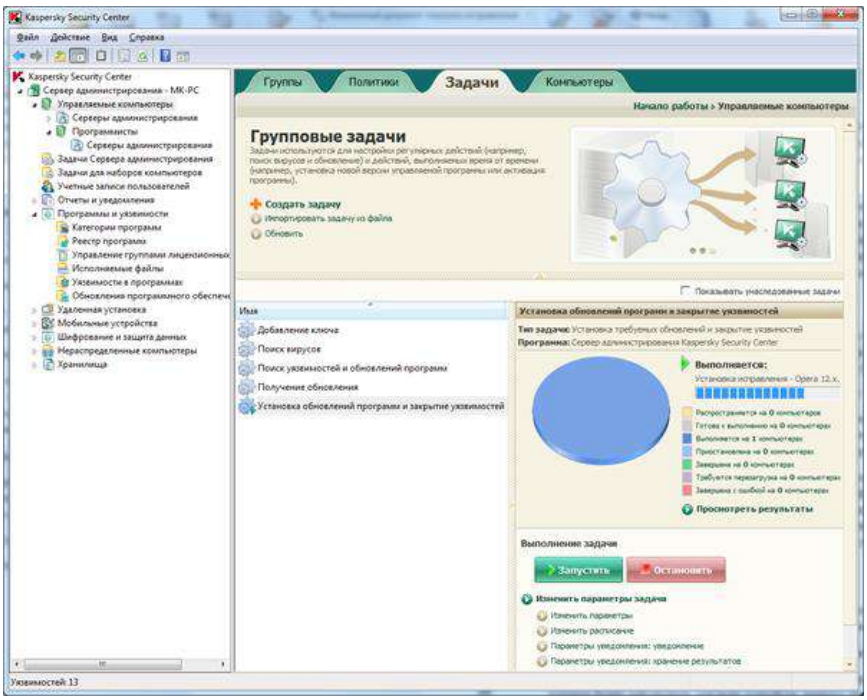


Рисунок 15 – Задача для поиска и закрытия уязвимостей.

После выполнения соответствующей задачи администратор получает список найденных уязвимостей с указанием их критичности и ссылками на их описание (Программы и уязвимости – Уязвимости в программах) (рисунок 16). Чтобы получить более подробную информацию, можно сформировать отчет о выполненной задаче поиска уязвимости (Отчеты и уведомления – Отчет об уязвимостях) (рисунок 17).

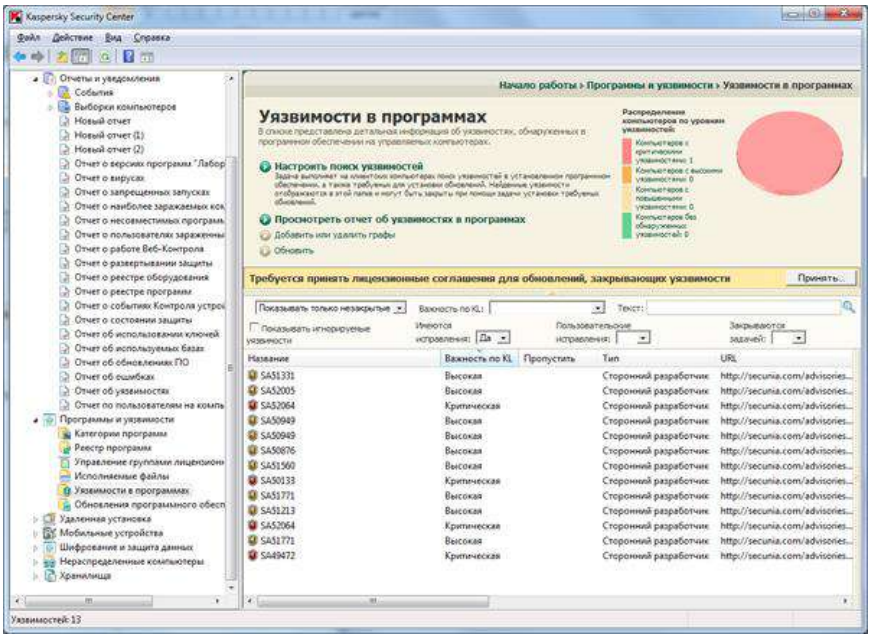


Рисунок 16 – Список найденных уязвимостей.

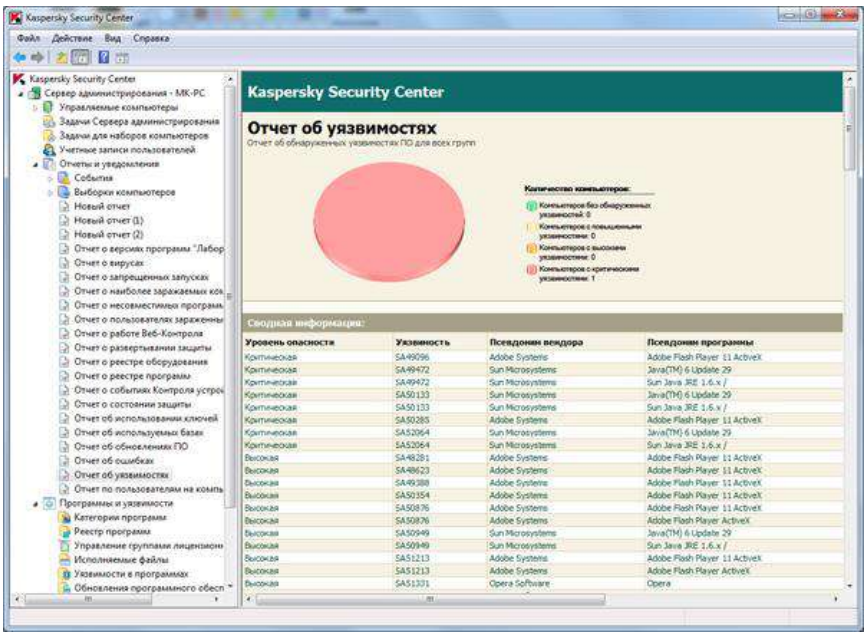


Рисунок 17 – Отчет о поиске уязвимостей.

Аналогично происходит работа с обновлениями программного обеспечения. Создаются и запускаются задачи «Получения обновлений» и «Синхронизация обновлений Windows Update» (Управляемые компьютеры – Задачи). По результатам их работы формируется реестр необходимых обновлений ПО, которые могут быть загружены немедленно или быть отложены до более удобного случая (Программы и уязвимости – Обновления программного обеспечения) (рисунок 18).

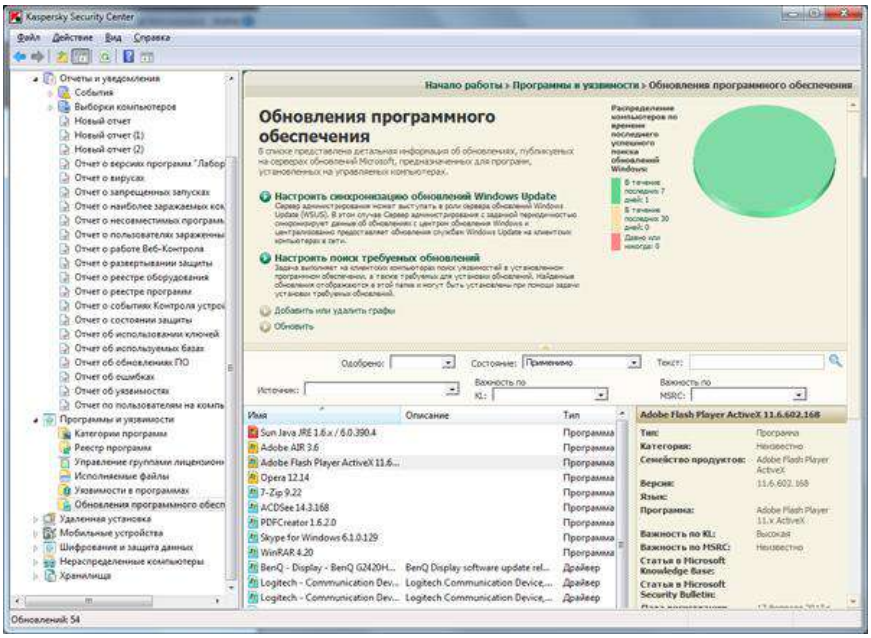


Рисунок 18 – Реестр обновлений программного обеспечения.

Еще одной простой, но в то же время полезной функцией является удаленный доступ к компьютерам в сети. Если у пользователей возникли проблемы или неполадки, администратор может получить управление их компьютерами и решить возникшие

проблемы, не покидая своего рабочего места (Управляемые компьютеры – XP-MSDN – Подключиться к компьютеру – RDP).

Работа с отчетами

Отчеты в Kaspersky Security Center содержат информацию о состоянии системы защиты. Отчеты формируются на основании информации, хранящейся на Сервере администрирования. Можно создавать отчеты для следующих объектов:

- для выборки клиентских компьютеров;

- для компьютеров, входящих в определенную группу администрирования;

- для набора клиентских компьютеров из различных групп администрирования;

- для всех компьютеров в сети (доступно для отчета о развертывании).

В программе имеется набор стандартных шаблонов отчетов, предусмотрена также возможность создания пользовательских шаблонов отчетов. Отчеты отображаются в главном окне программы, в папке дерева консоли **Отчеты и уведомления.** Просмотрите доступные отчеты.

Управление компьютером

Kaspersky Security Center позволяет удаленно управлять клиентскими компьютерами: включать, выключать и перезагружать их. Создайте задачу управления клиентским компьютером:

1. Выберите Управляемые компьютеры – Задачи – Создать задачу.
2. Введите имя задачи.
3. Выберите узел Kaspersky Security Center, раскройте папку Дополнительно и выберите задачу Управление клиентским компьютером.
4. Выберите вариант перезагрузить компьютер.
5. Нажмите Далее, оставив ручной запуск.
6. Поставьте галочку Запустить задачу после завершения работы мастера.

Настройка политик антивируса

Kaspersky Security Center позволяет настраивать параметры работы антивируса через групповые политики. Создайте новую политику:

1. Выберите Управляемые компьютеры – Политики – Создать политику.
2. Введите имя политики.

3. Выберите KES 10 для Windows.
4. Не выбирайте конфигурационный файл.
5. Появится окно с основными подсистемами. Для изменения настроек подсистемы, выберите необходимую подсистему и нажмите Изменить. Отключите Сетевой экран. Выберите основные параметры защиты и поставьте галочку Применять технологию лечения активного заражения.
6. Нажмите далее.
7. Примите участие в программе Kaspersky Security Network.
8. Нажмите кнопку Настройка в группе Уведомления. Просмотрите доступные уведомления.
9. Включите защиту паролем.
10. Выберите Активная политика (Если уже существует аналогичная политика, она будет отключена, а активной станет только что созданная).

Контрольные вопросы

1. Что такое Kaspersky Security Center?
2. В каких режимах может работать Kaspersky Security Center?
3. Что включает в себя Kaspersky Security Center?
4. Какие основные функции в Kaspersky Security Center?
5. Что такое «Сервер администрирования»?
6. Что такое «Агент администрирования»?
7. Что такое «Инсталляционный пакет» и как его создать?
8. Что такое «Удаленная установка» и как ей пользоваться?
9. Как получить информацию о конкретном компьютере в сети?
10. Как осуществляется поиск и устранение уязвимостей?