ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

УПРАВЛЕНИЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ И ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Кафедра «Вычислительные системы и информационная безопасность»

Методические указания

по дисциплине

«Информационная безопасность и защита информации»

Автор

Газизов А.Р.

Ростов-на-Дону, 2014

Аннотация

В компактной форме приводятся краткие теоретические сведения к выполнению лабораторных работ, порядок выполнения лабораторных работ, индивидуальные задания и контрольные вопросы.

Автор

к.п.н.
Газизов А.Р.

Оглавление

ЛАБОРАТОРНАЯ РАБОТА 1
СОЗДАНИЕ КРИПТОГРАФИЧЕСКОГО ПРИЛОЖЕНИЯ

Цель работы: исследовать процедуры шифрования и расшифровки содержимого файла.

Краткие теоретические сведения

В лабораторной работе демонстрируются процедуры шифрования и расшифровки содержимого файла. Примеры кода предназначены для приложений Windows Forms.

Выполняются следующие рекомендации по шифрованию.

– Используется класс **RijndaelManaged**, симметричный алгоритм, для шифрования и расшифровки данных с использованием автоматически генерируемых объектов **Key** и **IV**. Симметричный алгоритм используется для шифрования содержимого файла.

– Используется класс **RSACryptoServiceProvider**, асимметричный алгоритм, для шифрования и расшифровки симметричного ключа, сохраненного в файле вместе с зашифрованными данными. Файл шифруется с помощью **RijndaelManaged**. Использование асимметричных алгоритмов наиболее целесообразно при небольших объемах данных, например, при работе с ключами.

– Для дешифрования файла нужен симметричный ключ, который может быть получен путем дешифрования начала файла с помощью закрытого ключа.

– Без знания закрытого ключа файл не может быть дешифрован.

В таблице 1 перечислены задачи шифрования, рассматриваемые в данной работе.

Таблица 1

Задачи шифрования

Задача	Описание
Создание приложения Windows Forms	Перечисляются элементы управления, необходимые для запуска приложения.
Объявление глобальных объектов	Объявление строковых переменных пути, CspParameters и RSACryptoServiceProvider, получающих глобальный контекст класса Form.

Создание асимметричного ключа	Создается пара ключей, состоящая из асимметричного открытого и закрытого ключа, которой присваивается имя контейнера ключа.
Шифрование файла	Вывод диалогового окна для выбора файла, подлежащего шифрованию, и шифрование файла.
Расшифровка файла	Вывод диалогового окна для выбора зашифрованного файла, подлежащего расшифровке, и расшифровка файла.
Получение закрытого ключа	Получение полной пары ключей с помощью имени контейнера ключа.
Экспорт открытого ключа	Сохранение ключа в XML-файл только с открытыми параметрами.
Импорт открытого ключа	Загрузка ключа из XML-файла в контейнер ключа.
Тестирование приложения	Перечень процедур для тестирования приложения.

Создание приложения Windows Forms

Большинство примеров кода в представляют собой обработчики событий для кнопочных элементов управления. В таблице 2 приводится список элементов управления, необходимых для работы примера приложения, а также их имена, соответствующие примерам кода.

Таблица 2

Элементы управления, необходимые для работы примера приложения

Элемент управления	**Имя**	**Свойство Text (при необходимости)**
Form	**Form1**	**Шифрование файлов**
Button	buttonEncryptFile	Encrypt File
Button	buttonDecryptFile	Decrypt File
Button	buttonCreateAsmKeys	Create Keys
Button	buttonExportPublicKey	Export Public Key

Button	buttonImportPublicKey	Import Public Key
Button	buttonGetPrivateKey	Get Private Key
Label	label1	
OpenFileDialog	openFileDialog1	
OpenFileDialog	openFileDialog2	

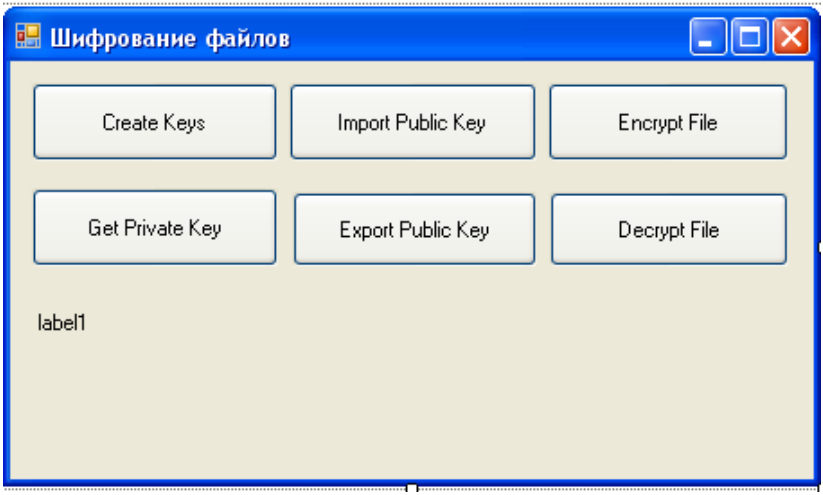

Рис. 1. Форма программы для шифрования файлов

Добавьте в код формы ссылки на компоненты следующим образом:

- using System.IO;
- using System.Security.Cryptography.

Объявление глобальных объектов

Добавьте следующие поля в форму. При необходимости отредактируйте строковые переменные среды и настроек.

```
// Declare CspParmeters and RsaCryptoServiceProvider
// objects with global scope of your Form class.
CspParameters cspp = new CspParameters();
RSACryptoServiceProvider rsa;
// Path variables for source, encryption, and
// decryption folders. Must end with a backslash.
const string EncrFolder=@"c:\Encrypt\"; //Директория для шифрованного файла
```

const string DecrFolder=@"c:\Decrypt\";//Директория для дешифрованного файла

const string SrcFolder=@"c:\docs\"; //Директория для исходного файла

// Public key file //Файл с открытым ключом

const string PubKeyFile = @"c:\encrypt\rsaPublicKey.txt";

// Key container name for private/public key value pair.

//Имя контейнера для хранения пары: открытый/закрытый ключ

const string keyName = "Key01".

Чтобы создать обработчики событий для кнопок, дважды щелкните по ним в конструкторе Visual Studio.

Создание асимметричного ключа

При выполнении данной задачи создается асимметричный ключ, с помощью которого производится шифрование и дешифрование симметричного ключа RijndaelManaged. Этот ключ использовался для шифрования содержимого файла, и с его помощью на элементе управления label1 отображается имя контейнера ключа.

Добавьте следующий код в качестве обработчика события Click кнопки Create Keys (buttonCreateAsmKeys_Click).

```
private void buttonCreateAsmKeys_Click(object sender, System.EventArgs e)
{
   // Stores a key pair in the key container.
   cspp.KeyContainerName = keyName;
   //Генерируем открытый и закрытый ключи и сохраняем в контейнере Key01
   rsa = new RSACryptoServiceProvider(cspp);
   rsa.PersistKeyInCsp = true;
    //Выводим на экран информацию о названии контейнера и типе ключа
   if (rsa.PublicOnly == true)
     label1.Text = "Key: " + cspp.KeyContainerName + " - Public Only";
   else
     label1.Text = "Key: " + cspp.KeyContainerName + " - Full Key Pair";
}
```

Шифрование файла

Для выполнения этой задачи используются два метода: обработчик события для кнопки Encrypt File (buttonEncryptFile_Click) и метод EncryptFile. Первый метод используется для вывода диалогового окна выбора файла и передачи имени файла второму методу, который выполняет шифрование.

Зашифрованное содержимое, ключ и вектор инициализации сохраняются в объект FileStream (файл), называемый пакетом шифрования.

Метод EncryptFile выполняет следующие действия.

1. Создает симметричный алгоритм RijndaelManaged для шифрования содержимого.
2. Создает объект RSACryptoServiceProvider и устанавливает для шифрования ключа RijndaelManaged.
3. Использует объект CryptoStream для чтения и шифрования объекта FileStream исходного файла в виде байтовых блоков в объект назначения FileStream для зашифрованного файла.
4. Определяет длину зашифрованного ключа и вектора инициализации и создает байтовые массивы соответствующей длины.
5. Записывает ключ, вектор инициализации и значения их длин в пакет шифрования.
6. Пакетом шифрования используется следующий формат:
   - длина ключа, байты 0-3;
   - длина вектора инициализации, байты 4-7;
   - зашифрованный ключ;
   - вектор инициализации;
   - зашифрованный текст.

Значения длины ключа и вектора инициализации могут использоваться для определения начальных точек и длин всех частей пакета шифрования, которые затем могут использоваться при расшифровке файла.

Добавьте следующий код в качестве обработчика события Click кнопки Encrypt File (buttonEncryptFile_Click).

```
private void buttonEncryptFile_Click(object sender, System.EventArgs e)
{
    if (rsa == null)
        MessageBox.Show("Key not set.");
    else
    {
        // Display a dialog box to select a file to encrypt.
        openFileDialog1.InitialDirectory = SrcFolder;
        if (openFileDialog1.ShowDialog() == DialogResult.OK)
```

```
            {
                string fName = openFileDialog1.FileName;
                if (fName != null)
                {
                    FileInfo fInfo = new FileInfo(fName);
                    // Pass the file name without the path.
                    string name = fInfo.FullName;
                    EncryptFile(name);
                }
            }
        }
    }
```

Добавьте следующий метод EncryptFile в форму.

```
private void EncryptFile(string inFile)
{
    // Create instance of Rijndael for
    // symetric encryption of the data.
    RijndaelManaged rjndl = new RijndaelManaged();
    rjndl.KeySize = 256;
    rjndl.BlockSize = 256;
    rjndl.Mode = CipherMode.CBC;
    ICryptoTransform transform = rjndl.CreateEncryptor();
    // Use RSACryptoServiceProvider to
    // enrypt the Rijndael key.
    // rsa is previously instantiated:
    //    rsa = new RSACryptoServiceProvider(cspp);
    byte[] keyEncrypted = rsa.Encrypt(rjndl.Key, false);

    // Create byte arrays to contain
    // the length values of the key and IV.
    byte[] LenK = new byte[4];
    byte[] LenIV = new byte[4];

    int lKey = keyEncrypted.Length;
    LenK = BitConverter.GetBytes(lKey);
    int lIV = rjndl.IV.Length;
    LenIV = BitConverter.GetBytes(lIV);

    // Write the following to the FileStream for the encrypted file
(outFs):
    // - length of the key (длина шифрованного симметрично-
го ключа – 4 байта)
```

```
            // - length of the IV (длина вектора инициализации – 4 байта)
            // - ecrypted key (зашифрованный открытым ключом симметричный ключ)
            // - the IV (вектор инициализации)
            // - the encrypted cipher content (шифрованный файл)

            int startFileName = inFile.LastIndexOf("\\") + 1;
           // Change the file's extension to ".enc"
            string outFile = EncrFolder + inFile.Substring(startFileName, inFile.LastIndexOf(".")- startFileName) + ".enc";

            using (FileStream outFs = new FileStream(outFile, FileMode.Create))
            {
                outFs.Write(LenK, 0, 4);
                outFs.Write(LenIV, 0, 4);
                outFs.Write(keyEncrypted, 0, lKey);
                outFs.Write(rjndl.IV, 0, lIV);

                // Now write the cipher text using
                // a CryptoStream for encrypting.
                using (CryptoStream outStreamEncrypted = new CryptoStream(outFs, transform, CryptoStreamMode.Write))
                {
                   // By encrypting a chunk at
                   // a time, you can save memory
                   // and accommodate large files.
                   int count = 0;
                   int offset = 0;

                   // blockSizeBytes can be any arbitrary size.
                   int blockSizeBytes = rjndl.BlockSize / 8;
                   byte[] data = new byte[blockSizeBytes];
                   int bytesRead = 0;

                   using (FileStream inFs = new FileStream(inFile, FileMode.Open))
                   {
                      do
                      {
                         count = inFs.Read(data, 0, blockSizeBytes);
```

```
                    offset += count;
                    outStreamEncrypted.Write(data, 0, count);
                    bytesRead += blockSizeBytes;
                }
                while (count > 0);
            inFs.Close();
            }
            outStreamEncrypted.FlushFinalBlock();
            outStreamEncrypted.Close();
        }
        outFs.Close();
    }
}
```

Расшифровка файла

Для выполнения этой задачи используются два метода: обработчик события для кнопки Decrypt File (buttonEncryptFile_Click) и метод DecryptFile. Первый метод используется для вывода диалогового окна выбора файла и передачи имени файла второму методу, который выполняет расшифровку.

Метод Decrypt выполняет следующие действия:

1. Создает симметричный алгоритм RijndaelManaged для расшифровки содержимого.
2. Считывает первые восемь байтов объекта FileStream зашифрованного пакета в байтовые массивы для получения значений длин зашифрованного симметричного ключа и вектора инициализации.
3. Извлекает ключ и вектор инициализации из пакета шифрования в байтовые массивы.
4. Создает объект RSACryptoServiceProvider и устанавливает для расшифровки ключа RijndaelManaged.
5. Использует объект CryptoStream для чтения и расшифровки зашифрованного текста пакета шифрования FileStream в виде байтовых блоков и загрузки их в объект FileStream для расшифрованного файла. По завершении этой операции расшифровка считается выполненной.

Добавьте следующий код в качестве обработчика события Click кнопки Decrypt File.

```
private void buttonDecryptFile_Click(object sender, EventArgs e)
{
    if (rsa == null)
```

```
            MessageBox.Show("Key not set.");
        else
        {
            // Display a dialog box to select the encrypted file.
            openFileDialog2.InitialDirectory = EncrFolder;
            if (openFileDialog2.ShowDialog() == DialogResult.OK)
            {
                string fName = openFileDialog2.FileName;
                if (fName != null)
                {
                    FileInfo fi = new FileInfo(fName);
                    string name = fi.Name;
                    DecryptFile(name);
                }
            }
        }
    }
```

Добавьте следующий метод DecryptFile в форму.

```
    private void DecryptFile(string inFile)
    {
        // Create instance of Rijndael for
        // symetric decryption of the data.
        RijndaelManaged rjndl = new RijndaelManaged();
        rjndl.KeySize = 256;
        rjndl.BlockSize = 256;
        rjndl.Mode = CipherMode.CBC;

        // Create byte arrays to get the length of
        // the encrypted key and IV.
        // These values were stored as 4 bytes each
        // at the beginning of the encrypted package.
        byte[] LenK = new byte[4];
        byte[] LenIV = new byte[4];

        // Consruct the file name for the decrypted file.
        string outFile = DecrFolder + inFile.Substring(0, in-
File.LastIndexOf(".")) + ".txt";

        // Use FileStream objects to read the encrypted
        // file (inFs) and save the decrypted file (outFs).
        using (FileStream inFs = new FileStream(EncrFolder + inFile,
```

```
FileMode.Open))
            {
                inFs.Seek(0, SeekOrigin.Begin);
                inFs.Seek(0, SeekOrigin.Begin);
                inFs.Read(LenK, 0, 3);
                inFs.Seek(4, SeekOrigin.Begin);
                inFs.Read(LenIV, 0, 3);

                // Convert the lengths to integer values.
                int lenK = BitConverter.ToInt32(LenK, 0);
                int lenIV = BitConverter.ToInt32(LenIV, 0);

                // Determine the start postition of
                // the ciphter text (startC)
                // and its length(lenC).
                int startC = lenK + lenIV + 8;
                int lenC = (int)inFs.Length - startC;

                // Create the byte arrays for
                // the encrypted Rijndael key,
                // the IV, and the cipher text.
                byte[] KeyEncrypted = new byte[lenK];
                byte[] IV = new byte[lenIV];

                // Extract the key and IV
                // starting from index 8
                // after the length values.
                inFs.Seek(8, SeekOrigin.Begin);
                inFs.Read(KeyEncrypted, 0, lenK);
                inFs.Seek(8 + lenK, SeekOrigin.Begin);
                inFs.Read(IV, 0, lenIV);
                Directory.CreateDirectory(DecrFolder);
                // Use RSACryptoServiceProvider
                // to decrypt the Rijndael key.
                byte[] KeyDecrypted = rsa.Decrypt(KeyEncrypted, false);

                // Decrypt the key.
                ICryptoTransform transform =
rjndl.CreateDecryptor(KeyDecrypted, IV);

                // Decrypt the cipher text from
                // from the FileSteam of the encrypted
```

```
            // file (inFs) into the FileStream
            // for the decrypted file (outFs).
            using (FileStream outFs = new FileStream(outFile, File-
Mode.Create))
            {

                int count = 0;
                int offset = 0;

                // blockSizeBytes can be any arbitrary size.
                int blockSizeBytes = rjndl.BlockSize / 8;
                byte[] data = new byte[blockSizeBytes];


                // By decrypting a chunk a time,
                // you can save memory and
                // accommodate large files.

                // Start at the beginning
                // of the cipher text.
                inFs.Seek(startC, SeekOrigin.Begin);
                using (CryptoStream outStreamDecrypted = new Cryp-
toStream(outFs, transform, CryptoStreamMode.Write))
                {
                    do
                    {
                        count = inFs.Read(data, 0, blockSizeBytes);
                        offset += count;
                        outStreamDecrypted.Write(data, 0, count);

                    }
                    while (count > 0);

                    outStreamDecrypted.FlushFinalBlock();
                    outStreamDecrypted.Close();
                }
                outFs.Close();
            }
            inFs.Close();
        }
    }
```

Экспорт открытого ключа

В рамках этой задачи ключ, созданный при нажатии кнопки Create Keys, сохраняется в файл. Экспортируются только открытые параметры.

Данная задача воссоздает ситуацию, в которой Алиса предоставляет Бобу открытый ключ, чтобы он мог зашифровывать для нее файлы. Боб и другие лица, имеющие открытый ключ, не смогут расшифровывать их, поскольку они не имеют полной пары ключей с закрытыми параметрами.

Добавьте следующий код в качестве обработчика события Click кнопки Export Public Key (buttonExportPublicKey_Click).

```
void buttonExportPublicKey_Click(object sender, System.EventArgs e)
{
    // Save the public key created by the RSA
    // to a file. Caution, persisting the
    // key to a file is a security risk.
    Directory.CreateDirectory(EncrFolder);
    StreamWriter sw = new StreamWriter(PubKeyFile, false);
    sw.Write(rsa.ToXmlString(false));
    sw.Close();
}
```

Импорт открытого ключа

В рамках данной задачи производится загрузка ключа, имеющего только открытые параметры, который затем устанавливается в качестве имени контейнера ключа. Этот ключ создается при нажатии кнопки Export Public Key.

Данная задача воссоздает ситуацию, в которой Боб загружает ключ Алисы, имеющий только открытые параметры, чтобы зашифровывать для нее файлы.

Добавьте следующий код в качестве обработчика события Click кнопки Import Public Key (buttonImportPublicKey_Click).

```
void buttonImportPublicKey_Click(object sender, System.EventArgs e)
{
StreamReader sr = new StreamReader(PubKeyFile);
string keytxt = sr.ReadToEnd();
rsa = new RSACryptoServiceProvider();
rsa.FromXmlString(keytxt);
rsa.PersistKeyInCsp = true;
```

```
if (rsa.PublicOnly == true)
label1.Text = "Key: " + cspp.KeyContainerName + " - Public Only";
else
label1.Text = "Key: " + cspp.KeyContainerName + " - Full Key Pair";
sr.Close();
 }
```

Получение закрытого ключа

В рамках этой задачи контейнеру ключа присваивается имя, соответствующее имени ключа, созданного при нажатии кнопки Create Keys. Контейнер ключа будет содержать полную пару ключей с закрытыми параметрами.

Данная задача воссоздает ситуацию, в которой Алиса использует свой закрытый ключ для расшифровки файлов, зашифрованных Бобом.

Добавьте следующий код в качестве обработчика события Click кнопки Get Private Key (buttonGetPrivateKey_Click).

```
private void buttonGetPrivateKey_Click(object sender, EventArgs e)
{
   cspp.KeyContainerName = keyName;

   rsa = new RSACryptoServiceProvider(cspp);
   rsa.PersistKeyInCsp = true;

   if (rsa.PublicOnly == true)
      label1.Text = "Key: " + cspp.KeyContainerName + " - Public Only";
   else
      label1.Text = "Key: " + cspp.KeyContainerName + " - Full Key Pair";

}
```

Тестирование приложения

После сборки приложения проведите следующие сценарии тестирования.

Создание ключей, шифрование и расшифровка

1. Нажмите кнопку Create Keys. В метке отобразится имя ключа и будет указано, является ли он полной парой ключей.

2. Нажмите кнопку Export Public Key. Обратите внимание, что при экспорте параметров открытого ключа текущий ключ не меняется.
3. Поместите в директорию c:\docs файл для шифрования.
4. Нажмите кнопку Encrypt File и выберите файл.
5. Нажмите кнопку Decrypt File и выберите последний зашифрованный файл.
6. Проверьте содержимое расшифрованного файла.
7. Закройте и перезапустите приложение, чтобы протестировать извлечение сохраненных контейнеров ключей в следующем сценарии.

Шифрование с открытым ключом

1. Нажмите кнопку Import Public Key. В метке отобразится имя ключа и будет указано, является ли он исключительно открытым.
2. Нажмите кнопку Encrypt File и выберите файл.
3. Нажмите кнопку Decrypt File и выберите последний зашифрованный файл. Эта операция должна завершиться ошибкой, так как необходим закрытый ключ для расшифровки.

В этом сценарии демонстрируется ситуация, когда для шифрования файла, передаваемого другому лицу, имеется только открытый ключ. Обычно для шифрования предоставляется только открытый ключ, а закрытый ключ используется для расшифровки.

Расшифровка при помощи закрытого ключа

1. Нажмите кнопку Get Private Key. В метке отобразится имя ключа и будет указано, является ли он полной парой ключей.
2. Нажмите кнопку Decrypt File и выберите последний зашифрованный файл. Эта операция должна завершиться успешно, так как имеется полная пара ключей для расшифровки.

Контрольные вопросы

1. Какова структура полученного в лабораторной работе зашифрованного файла?
2. Объясните механизм создания асимметричного ключа.
3. Каким образом осуществляется экспорт открытого ключа?
4. Каким образом осуществляется импорт открытого ключа?

ЛАБОРАТОРНАЯ РАБОТА 2
ПОЛИТИКИ ОГРАНИЧЕННОГО ИСПОЛЬЗОВАНИЯ ПРОГРАММ

Цель работы: исследование механизма ограниченного использования программ

Краткие теоретические сведения

Одной из отличительных особенностей **Active Directory** по праву считают механизм групповых политик, обеспечивающий эффективное и централизованное управление многочисленными параметрами операционных систем и приложений. Применение групповых политик позволяет администраторам определять правила, в соответствии с которыми настраиваются параметры рабочей среды как для пользователей, так и для компьютеров. Это позволяет достаточно просто и эффективно поддерживать вычислительную среду предприятия в рабочем состоянии.

Безусловно, к числу важнейших задач администрирования можно отнести обеспечение безопасности системы в целом. Не последнюю роль в этом играет процесс контроля программ, выполняемых на компьютерах домена. Наиболее яркий пример необходимости в нем – создание рабочей среды, исключающей возможность запуска вредоносного программного обеспечения, игр, новая версия используемого ПО вызывает конфликты с другими приложениями.

Решение таких задач с помощью политик ограниченного использования программ предоставляет администратору способ идентификации программ, выполняемых на компьютере домена и создание правил, устанавливающих возможность их выполнения. Использование таких политик возможно на операционных системах, начиная с Windows Server 2003 и Windows XP.

Вкратце, собственно сам механизм применения групповой политики выглядит следующим образом. Вначале администратор создает *объект групповой политики* (GPO), содержащий определенный набор параметров рабочей среды. Этот объект может содержать настройки, применяемые как компьютеру, так и к пользователю. Далее, с помощью связывания (или привязки, linking) этот объект ассоциируется с одним или несколькими элементами дерева Active Directory. При загрузке компьютера, входящего в домен, выполняется запрос списков групповой политики у контроллера домена. Контроллер пересылает необходимые списки в

том порядке, в котором они должны применяться на компьютере. Когда пользователь осуществляет вход в систему, выполняется еще один запрос о необходимых объектах групповой политики, которые затем применяются к пользователю, выполнившему вход в систему (рис. 1).

В общем рассмотрении механизм работы политик ограничения запуска программ достаточно прост. Для начала они активируются при создании нового объекта групповой политики или редактировании существующего. Затем выбирается уровень необходимой безопасности. Уровень безопасности – это **базовая модель контроля за исполнением программ**, или, другими словами – правило по умолчанию (рис. 2).

Затем настраиваются параметры политики – к каким типам файлов будет применяться политика, будет ли она распространяться на локальных администраторов компьютеров, кто сможет определять, что подписанному содержимому можно доверять. После этого создаются сами правила, запрещающие или разрешающие выполнение программ, идентифицированных правилом.

Активирование политики ограниченного использования программ

Создайте объект групповой политики или откройте в редакторе существующий. Откройте ветвь **Конфигурация компьютера** или **Конфигурация пользователя** (в зависимости от того, к чему необходимо будет применить политику). Найдите и выберите раздел **Конфигурация Windows – Параметры безопасности – Политики ограниченного использования программ** (рис. 3).

Рис. 1. Механизм применения групповой политики.

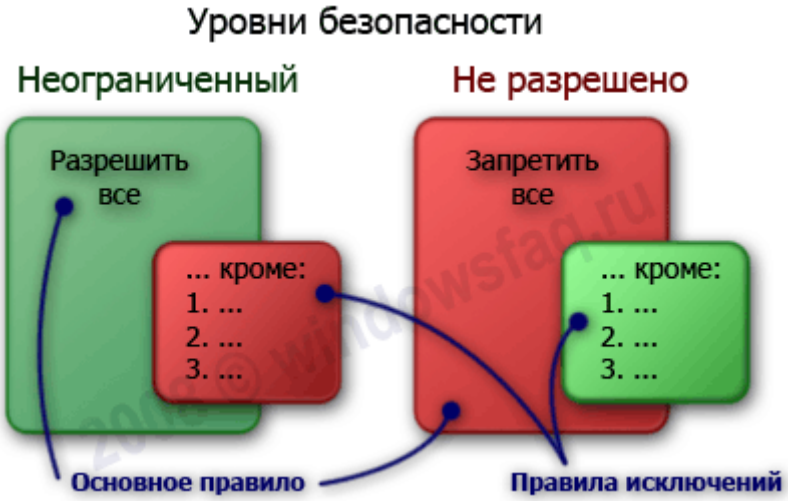

Рис. 2. Механизм работы политик ограничения запуска программ.

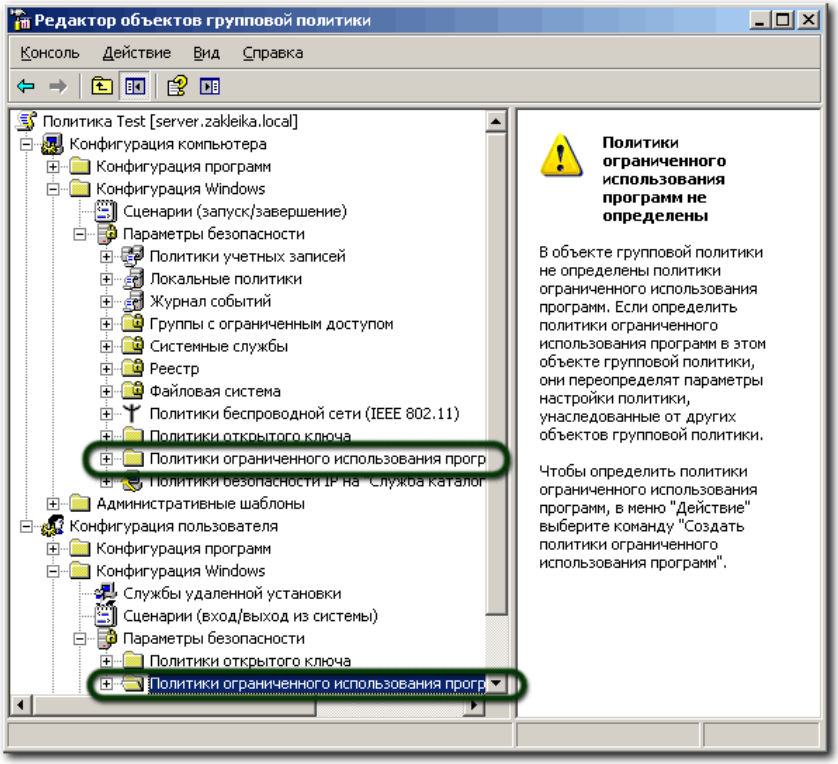

Рис. 3.

Если политики еще не были определены, в окне редактора вы увидите предупреждение, что в случае их назначения новые правила перекроют параметры политик, унаследованных от других объектов GPO. Поскольку именно это мы и собираемся сделать, выбираем в меню **Действие** команду **Создать политики ограниченного использования программ**.

Переходим в раздел **Уровни безопасности**. Действующий уровень отмечен иконкой с галочкой. По умолчанию им является уровень **Неограниченный** (рис. 4).

Этот уровень разрешает запуск любых программ, кроме явно запрещенных правилами. Особого смысла в использовании такого уровня безопасности нет, кроме случаев, когда необходимо запретить использование небольшого количества программ, не представляющих явную угрозу безопасности для вычислительной системы (например, пасьянс). Для обеспечения действенного за-

прета на использование нежелательных программ необходимо использовать уровень безопасности **Не разрешено**. Для изменения уровня необходимо сделать двойной щелчок мышью на нужном параметре и в открывшемся окне нажать кнопку **По умолчанию**, или, щелкнув правой кнопкой мыши выбрать в контекстном меню команду **По умолчанию** (рис. 5).

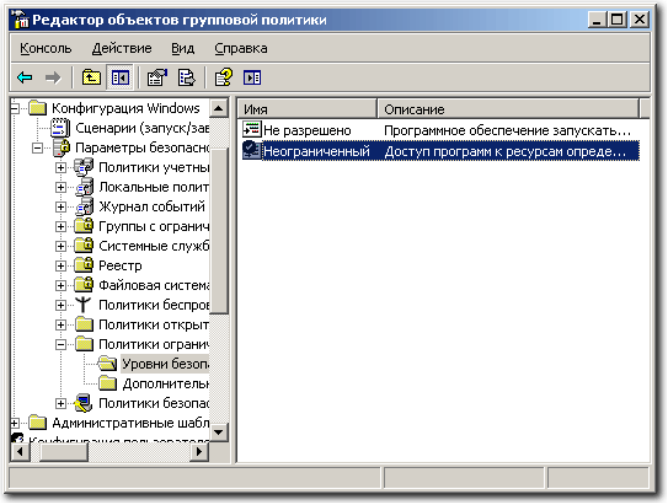

Рис. 4.

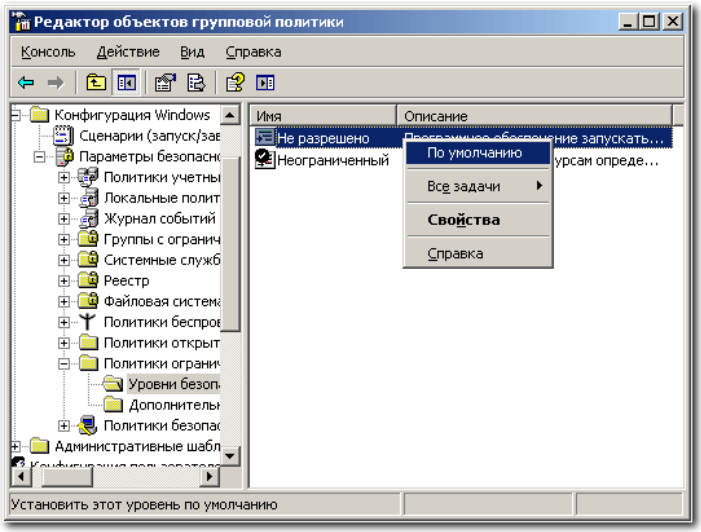

Рис. 5.

Общие параметры настроек политики

В узле **Политики ограниченного использования программ** расположены общие параметры настроек, определяющих применение политик (рис. 6).

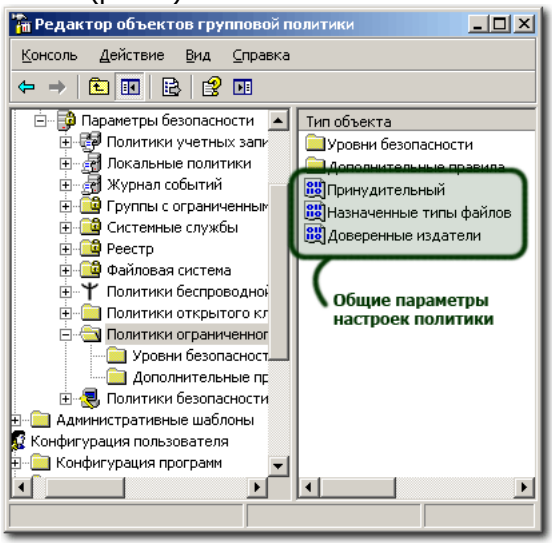

Рис. 6.

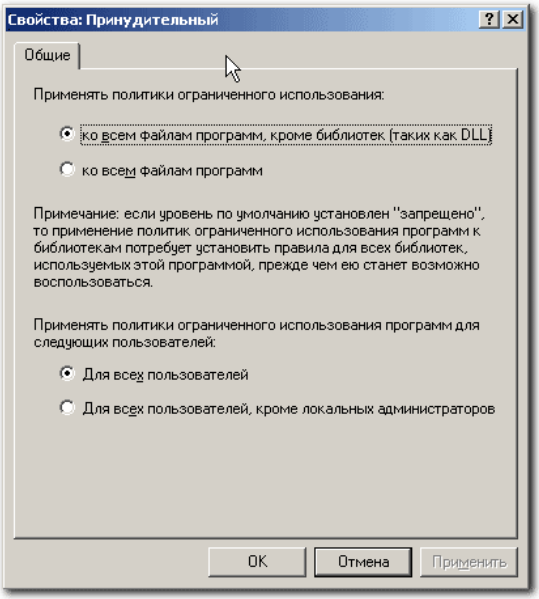

Рис. 7.

Принудительное использование

Первый параметр определяет, следует ли проверять библиотеки DLL, и возможность применения ограничений, накладываемых политикой на локальных администраторов компьютеров. DLL – это библиотеки динамической компоновки, которые являются частью некоторых исполняемых программ. По умолчанию, проверка DLL отключена (рис. 7).

Без особой нужды нет необходимости переключать этот параметр в положение проверки всех файлов программ. Причин для этого несколько. Во-первых, при большом количестве исполняемых файлов и «прицепленных» к ним библиотек (а в Windows их предостаточно) резко снижается производительность системы – параметры политики будут просматриваться при каждом вызове программой библиотеки DLL. Во-вторых, если исполнение файла будет запрещено политикой, то не возникнет и необходимости проверки сопутствующих библиотек.

Второй параметр позволяет исключить локальных администраторов компьютеров из списка пользователей, к которым будет применяться политика. Он используется только для политик компьютера. Включается, если необходимо позволить локальным администраторам запускать любые приложения. Более предпочтительный способ предоставить эту возможность – либо временное перемещение учетной записи компьютера в организационную единицу, на которую не распространяются данные политики, либо убрать разрешение **Применение групповой политики** в свойствах группы GPO, в состав которой входят администраторы.

Назначенные типы файлов

Здесь перечисляются все типы файлов, ассоциированные с их расширением, которые политика будет идентифицировать как исполняемый код. Список редактируемый – вы можете исключать из него перечисленные типы, а также добавлять новые.

Доверенные издатели

Эта группа параметров позволяет настраивать реагирование политики на элементы управления **ActiveX®** и другое подписанное содержимое.

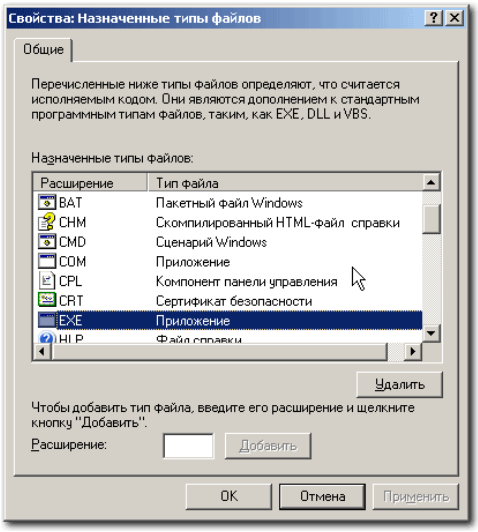

Рис. 8.

Здесь можно указать, кто будет принимать решение о доверии подписанному содержимому (лучше оставить это право администраторам предприятия), а также задать параметры проверки сертификатов – проверить, не отозван ли сертификат, и удостовериться, что он не просрочен.

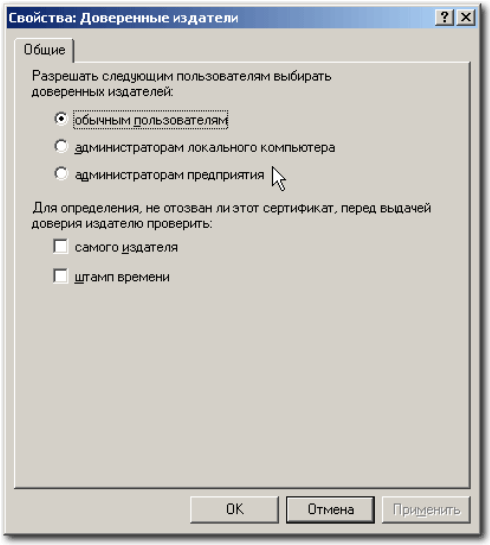

Рис. 9.

Создание правил политики

Правило политики ограниченного использования программ – это и есть тот механизм, с помощью которого программа «опознается». Правило определяет, разрешить или запретить выполнение программы, соответствующей указанным в нем условиям. Для сопоставления программы и условия можно использовать четыре параметра исполняемого файла - или, другими словами, применять один из четырех типов правил:

– Зона.
– Путь.
– Сертификат.
– Хеш.

Для создания нового правила необходимо перейти в раздел **Дополнительные правила**, щелкнув по нему мышью в списке объектов редактора групповой политики, и затем выбрав в меню **Действие** (или в меню, открываемом правым щелчком мыши) необходимый тип правила.

Правило зоны

Дабы избежать некоторой двусмысленности, сразу оговоримся, что речь пойдет о зонах, используемых **Internet Explorer**. Этот тип правила позволяет задать зону Интернета и установить для нее правило – разрешить запуск или запретить его.

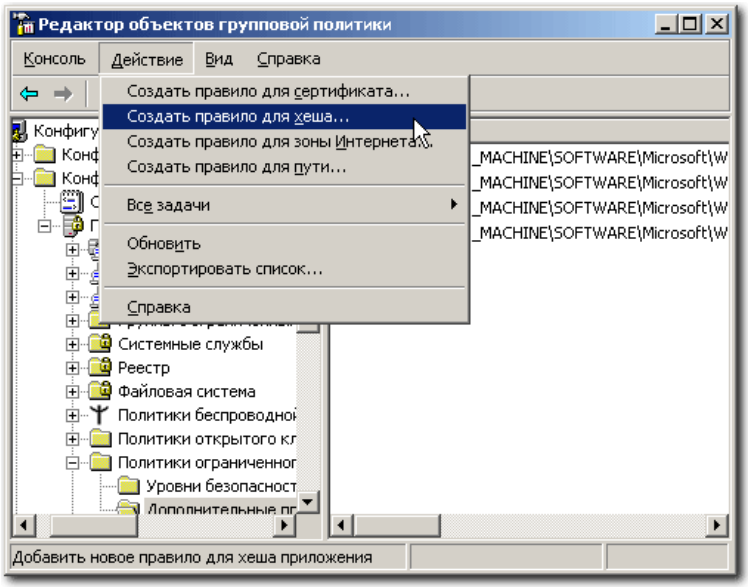

Рис. 10.

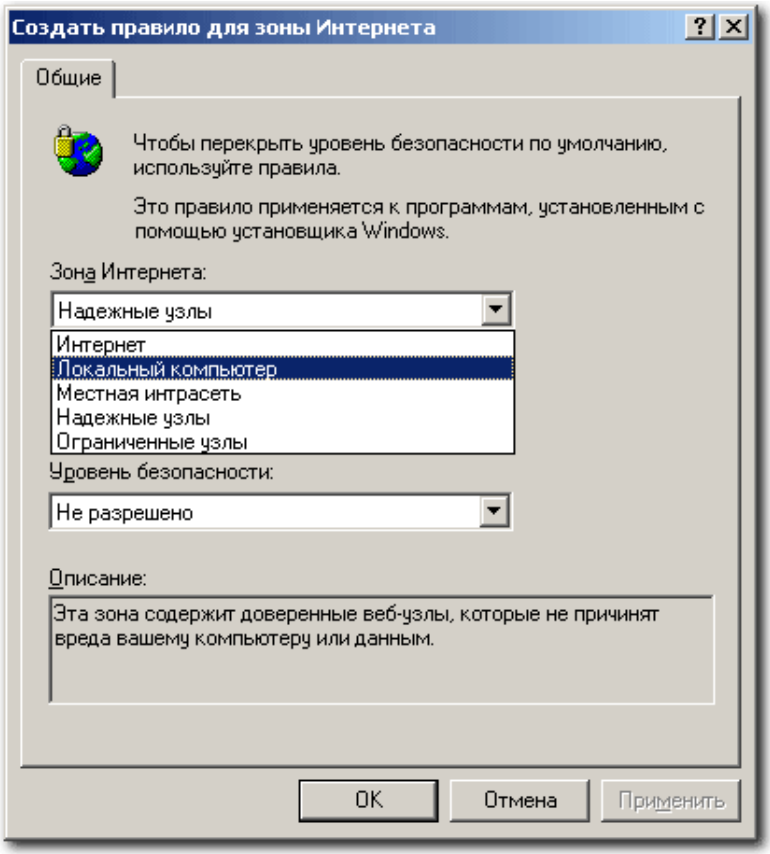

Рис. 11.

Главный минус, делающий его практически бесполезным – применяется только к файлам пакетов установщика Windows (Windows Installer, расширение *.msi).

Правило пути

Идентифицирует исполняемое приложение по его местоположению. Может содержать имя каталога или полный путь к исполняемой программе. Используется как локальный путь, так и универсальный путь в формате UNC. Допустимо применение переменных среды и подстановочных знаков «?» для любого единичного символа и «*» для любого количества символов.

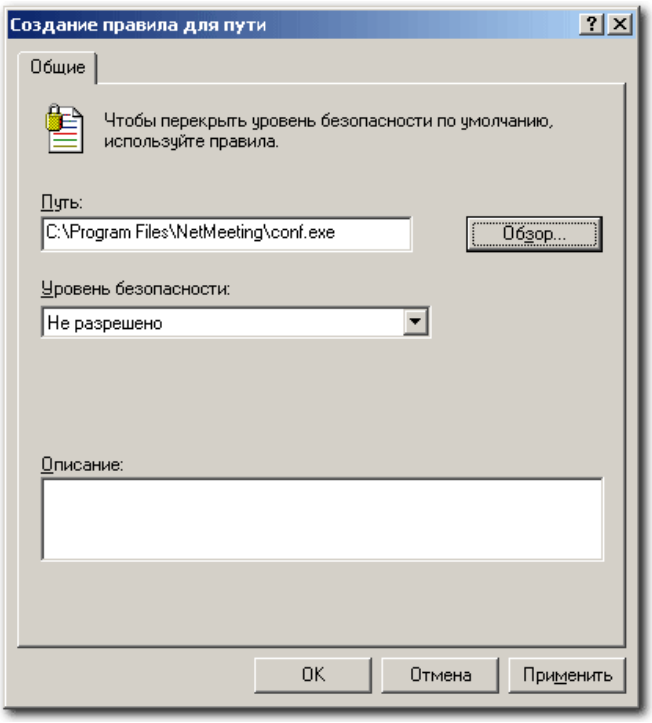

Рис. 12.

Путь можно ввести вручную в соответствующее поле или воспользоваться кнопкой Обзор.

Кроме указания самих путей в явном виде, допускается указание *пути в реестре*. Такая возможность полезна в том случае, когда у пользователя существует возможность установить приложение в неопределенное заранее место файловой системы компьютера, а программа хранит пути к своим рабочим каталогам в реестре. Правило будет просматривать соответствующую ветвь реестра, и при его совпадении будет производиться заданное в правиле действие – разрешение или запрет на запуск. Путь в реестре должен быть заключен между знаками «%». Он может содержать в окончании пути подстановочные знаки и использовать переменные среды. Не допускается использовать сокращения *HKLM* и *HKCU* (должен использоваться полный формат в виде *HKEY_LOCAL_MACHINE*), путь не должен заканчиваться символом «\» непосредственно перед закрывающим знаком «%» в правиле. Параметр реестра может быть типа *REG_SZ* или *REG_EXPAND_SZ*. По умолчанию, при активиро- вании политик ограниченного

использования программ создается четыре разрешающих правила пути в реестре.

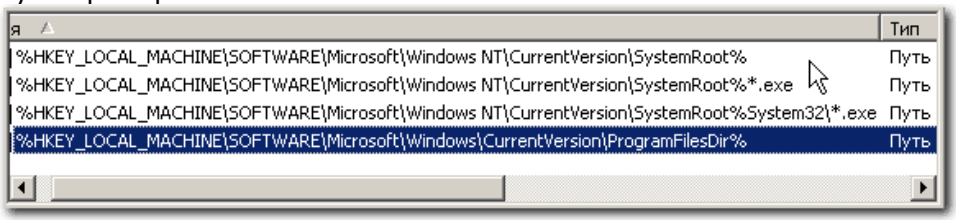

Рис. 13.

Они позволяют выполнить гарантированный запуск необходимых для работы ОС программ и служб, и при необходимости могут быть отредактированы. Если программа соответствует сразу нескольким определенным правилам пути, высший приоритет будет иметь то из них, которое наиболее точно описывает данную программу.

Очень удобное для использования правило пути имеет один существенный недостаток, значительно ограничивающий его применение. Поскольку оценка программы производится только по ее местоположению, придется постоянно учитывать права доступа пользователя к файловой системе. Если учетная запись пользователя позволяет копировать и переименовывать файлы, он с легкостью может обойти это правило, просто переименовав приложение, а затем переместив его в нужное место файловой системы.

Правило сертификата

Устанавливаются для файлов, имеющих цифровую подпись издателя. Для создания правила нажмите кнопку Обзор и укажите необходимый сертификат.

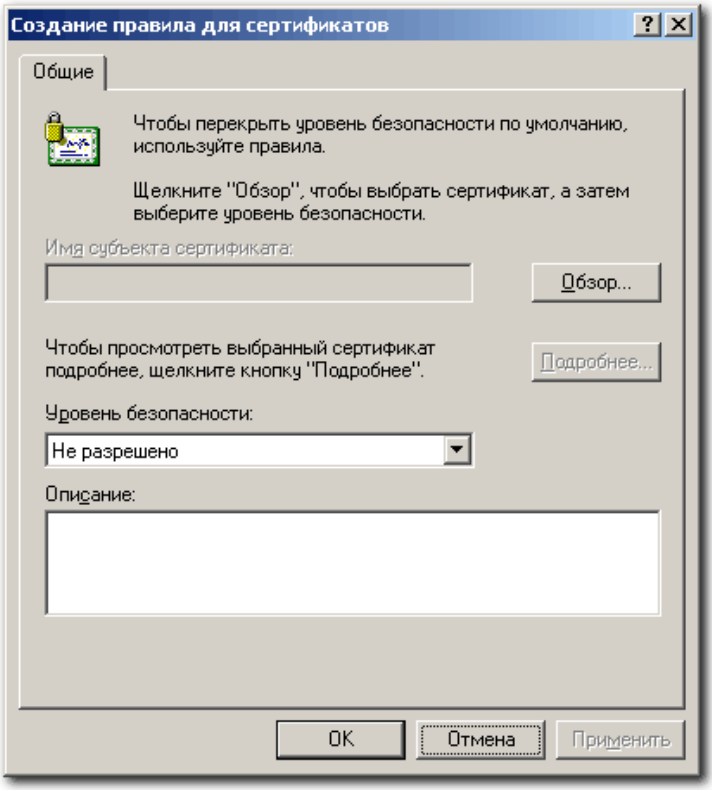

Рис. 14.

Способ идентификации программ с помощью сертификатов достаточно надежен, но и у него существуют минусы. Во-первых, он требует применения центров сертификации. Во-вторых, невозможно установить разные значения правил для программ одного издателя. Например, тот же пасьянс из стандартных игр Windows таким правилом запретить не получится, поскольку оно запретит и запуск ключевых компонентов всей операционной системы.

Правило хеша

Пожалуй, самое «полезное» правило. Для идентификации файла используется его *хеш*. Хеш – это цифровой «отпечаток» файла, получаемый преобразованием его содержимого в битовую строку фиксированной длины с помощью специальных криптографических функций. Замечательное свойство такого преобразования заключается в том, что хеш однозначно идентифицирует любой файл, независимо от его названия и месторасположения.

Любое, самое незначительное изменение кода файла приводит к изменению его хеша. И наоборот, два абсолютно идентичных файла имеют одинаковый хеш.

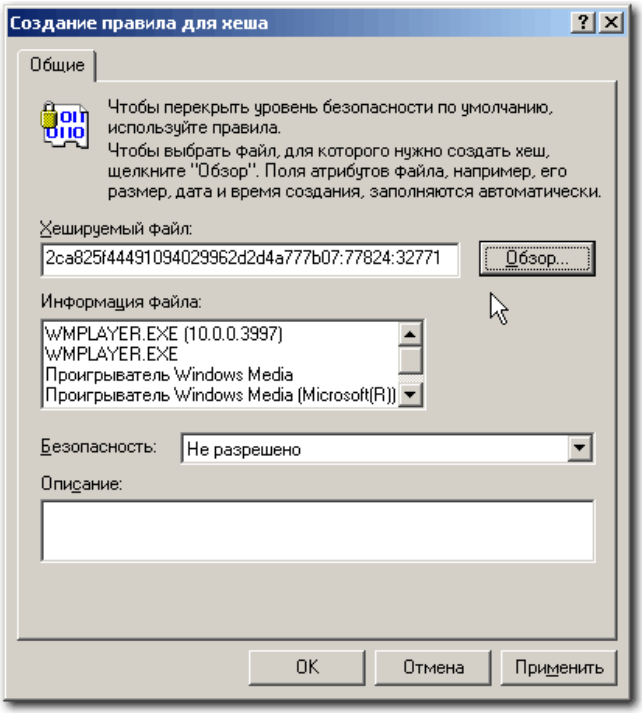

Рис. 15.

Для вычисления хеша файла укажите путь к нему, нажав кнопку **Обзор**. Если файл расположен на другом компьютере, необходимо обеспечить к нему доступ с той машины, где настраивается политика. Вы можете, например, подключить как сетевой диск стандартный общий ресурс вида *||COMP_NAME|C$*. После расчета хеша в поле **Хешируемый файл** появятся его значение, длина файла и код алгоритма хеширования, разделенные двоеточием.

Идентификация файла по его хешу является наиболее предпочтительной, позволяя однозначно определять файл. Его недостаток – это большой первоначальный объем работы, который необходимо проделать при создании нового набора правил. Этот тип правил используется по принципу – «один файл, одно правило». Более того, различные версии одной программы имеют

различное значение хеша. При достаточно большом объеме разрешенных для исполнения программ эта задача может в чем-то напоминать перепись населения. Впрочем, об упрощении процесса сбора информации о запускаемых программах мы расскажем чуть ниже.

Область действия политик ограниченного использования программ и приоритет правил

Действие политик ограниченного использования программ не распространяется на:

- Программы, запущенные от имени учетной записи SYSTEM.
- Драйверы и другие приложения уровня ядра.
- Макросы внутри документов Microsoft Office.
- Программы, написанные для общей многоязыковой библиотеки времени выполнения (Common Language Runtime) – эти программы используют политику безопасности доступа кода (Code Access Security Policy).

Приоритет применения правил выглядит так (по мере *убывания* приоритета):

- Правило для хеша.
- Правило для сертификата.
- Правило для пути.
- Правило для зоны Интернета.
- Правило по умолчанию.

Планирование создания правил политики

Планируя применение политик ограниченного использования программ, всегда полезно и настоятельно рекомендуется предварительно провести их «обкатку» в тестовой среде. Ввиду сложности структуры на первоначальном этапе возможны ошибки, которые, конечно, лучше исправлять не на рабочей системе. В случае «срабатывания» правила политики в локальный журнал компьютера заносится событие. Код содержит тип правила, его вызвавшего (865 - уровень безопасности по умолчанию, 866 - правило для пути, 867 - правило для сертификата, 868 - правило для зоны Интернета или правило для хеша).

При создании политики, имеющей уровень безопасности Не разрешено, необходимо будет определить, какой код может быть разрешен для запуска пользователем. Как отмечалось выше, эта задача может быть достаточно трудоемкой. Для облегчения процесса инвентаризации программ можно задействовать их отслеживание с помощью расширенного ведения журнала. Этот способ достаточно прост и эффективен.

На тестовом компьютере активируется политика ограничения программ, и в качестве уровня безопасности устанавливается параметр Неограниченный. Все дополнительные правила из политики удаляются. Суть в том, что, несмотря на отсутствие ограничений, при активировании политики можно включить функцию расширенного ведения журнала, в который будет заноситься информация о запущенных программах. Выполнив на тестовом компьютере запуск минимально необходимого пользователю набора программ, а затем, проанализировав этого журнал, можно разработать все необходимые правила для политики.

Для включения режима расширенного ведения журнала на тестовом компьютере создайте параметр реестра в ветви *HKLM|SOFTWARE|Policies|Microsoft|Windows|Safer|CodeIdentifiers* с именем *LogFileName*. Его значение должно содержать путь к каталогу, где будет расположен файл журнала. Содержимое журнала выглядит следующим образом:

winlogon.exe (PID = 452) identified C:\WINDOWS\system32\userinit.exe as Unrestricted using path rule, Guid = {191cd7fa-f240-4a17-8986-94d480a6c8ca}

Эта запись «переводится» так: родительский процесс *winlogon.exe*, имеющий значение идентификатора (PID) *452*, выполнил запуск *C:|Windows|system32|userinit.exe*; правило, вызвавшее «срабатывание» - правило для пути с уровнем безопасности *Неограниченный (Unrestricted)*, имеет код GUID *{191cd7fa-f240-4a17-8986-94d480a6c8ca}*. Каждое правило имеет свой идентификатор **GUID**. После того, как политика ограниченного использования программ применена, ее конфигурация хранится в системном реестре. Список контроля доступа, защищающий разделы реестра, позволяет только администраторам и учетной записи SYSTEM изменять ее. Политика пользователя хранится в разделе *HKCU|Software|Policies|Microsoft|Windows|*, политика компьютера хранится в разделе *HKLM|SOFTWARE|Policies|Microsoft|Windows|*.

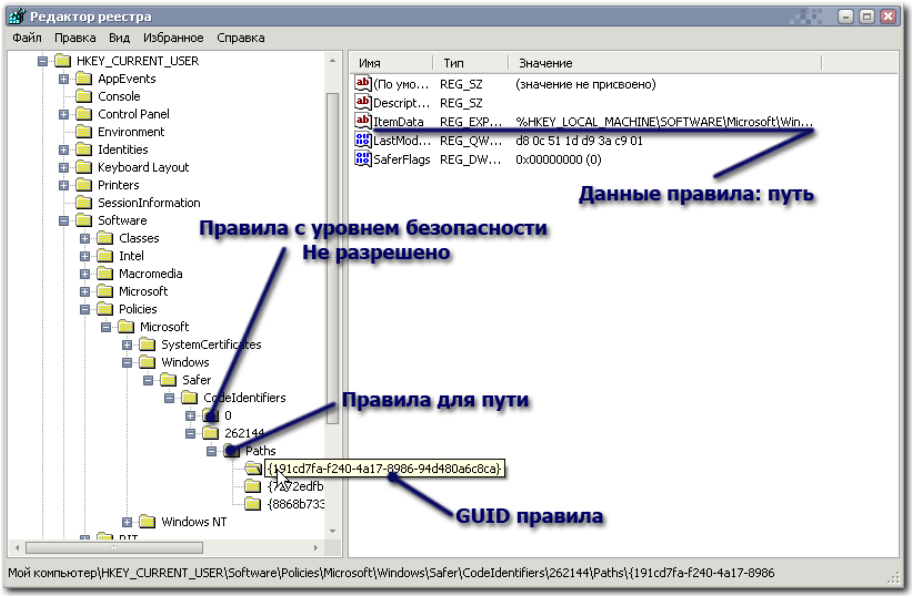

Рис. 16.

В случае каких-либо ошибок можно найти правило по его коду GUID и выяснить причину ошибки. По окончании отладки всех правил, на рабочей системе ведение журнала желательно прекратить, удалив параметр *LogFileName* из реестра для уменьшения использования дискового пространства и снижения быстродействия системы. В случае, если политика содержит параметры только для компьютера или пользователя, для ускорения обработки политики следует отключить неиспользуемые компоненты GPO.

Также для определения тех программ, которым потребуется создать разрешающие правила, можно воспользоваться утилитой *msinfo32.exe*. Для этого запустите все необходимые приложения, после этого нажмите кнопку **Пуск**, выберите **Выполнить** и введите команду msinfo32.exe. В окне программы msinfo32 разверните узел **Программная среда** и выберите **Выполняемые задачи**.

Настоятельно рекомендуется не изменять базовую доменную политику безопасности, а создавать новые объекты групповой политики. Это позволит в случае каких-либо непредвиденных ситуаций редактировать вновь созданные GPO, не затрагивая параметры безопасности всего домена. Следует учесть, что политика ограниченного использова- ния программ при входе в си-

стему пользователя, являющегося локальным администратором, в безопасном режиме не обрабатывается. Это дает возможность исправить политику, вызывающую проблемы.

Применение политик возможно и на компьютерах с ОС Windows, не являющихся членами домена. Например, можно создать шаблон безопасности на основе политики, а затем, после его переноса на необходимый компьютер, применить этот шаблон к локальной политике безопасности. В этом случае следует убедиться, что политика позволит произвести запуск утилиты Secedit, с помощью которой можно будет в дальнейшем обновить политику или отменить изменения.

При планировании применения политики ограниченного использования программ приходится учитывать множество аспектов, в том числе не явных. Поэтому еще раз обращаем внимание на то, что их настройку лучше производить в тестовой среде. Это позволит убедиться, что политика обеспечивает запуск необходимых приложений (например, используемые антивирусные программы), и запрещает исполнение нежелательного ПО. Такое использование позволит значительно снизить риск выполнения на компьютере вредоносных программ и упростит его дальнейшее администрирование.

Задание для выполнения

Создадим OU (пусть это будет Test Unit), поместим в него учетные записи компьютера и пользователя.

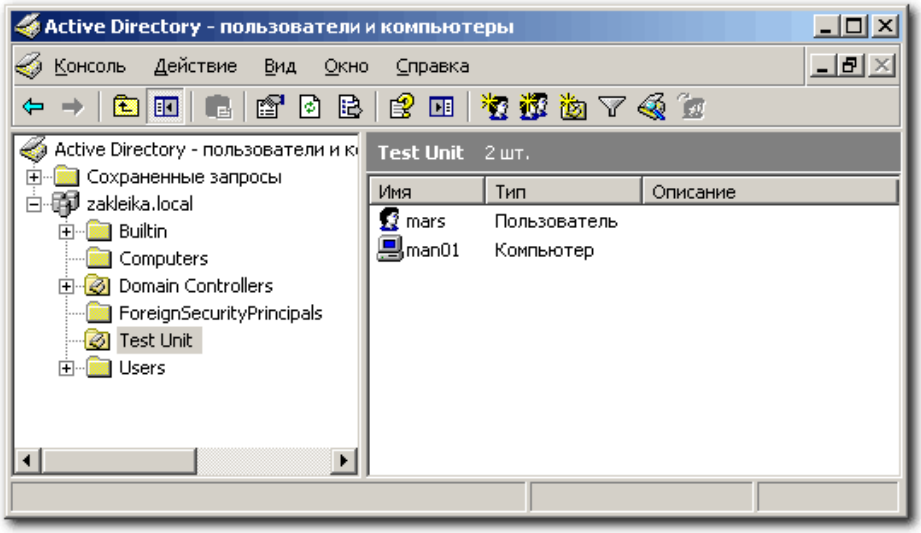

Рис. 17.

Для управления групповой политикой будет использоваться консоль gpmc. Создаем GPO – правой кнопкой мыши щелкаем на Test Unit, выбираем команду **Свойства**, в открывшемся окне переходим на вкладку **Group Policy**. Открываем консоль gpmc, еще раз делаем правый щелчок на Test Unit, и выбираем в меню команду **Создать и связать GPO здесь… (Create and Link a GPO Here)**. Указываем имя для создаваемой политики, нажимаем кнопку **ОК**. Выбираем созданную политику, щелкаем по ней правой кнопкой мыши и указываем команду **Редактировать (Edit)**.

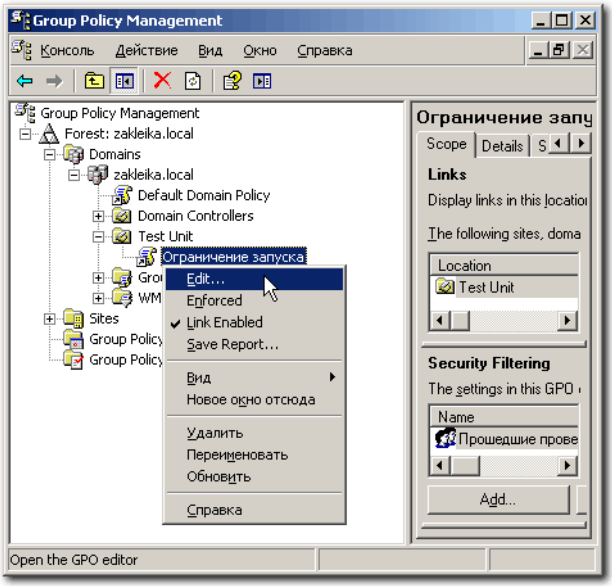

Рис. 18.

Откроется редактор объектов групповой политики. Сначала создадим политику, применяемую к компьютеру. Мы собираемся запретить всем пользователям на компьютерах группы Test Unit запуск любых программ, кроме Internet Explorer. Переходим в раздел **Конфигурация компьютера** – **Конфигурация Windows** – **Параметры безопасности** – **Политики ограниченного использования программ**. В меню **Действие** (или с помощью правой кнопки мыши) выбираем команду **Новые политики**. Переходим в раздел **Уровни безопасности**, включаем **Не разрешено**. Учитывая, что автоматически были созданы дополнительные правила, удаляем их. Для обеспечения входа пользователя в систему понадобится установить разрешения для неко-

торых программ. В моем случае (тестовая система с «чистой» установкой), необходимо, как минимум, разрешить запуск *winlogon.exe*, *userinit.exe* (для Vista это будут *logonui.exe* и *userinit.exe*) и *explorer.exe* из системной папки *%windir%|system32*. В другой ситуации, возможно, потребуются дополнительные разрешения - например, может возникнуть необходимость обработки сценариев, расположенных на сервере при входе пользователя в систему. Создаем для них правила пути, параметры которых вы можете увидеть на рисунке 19.

Теперь создадим правило, разрешающее запуск Internet Explorer. Чтобы не дать возможности пользователю подмены файла и не зависеть от его расположения в файловой системе, будем использовать правило хеша. Подключаем на сервере, где мы производим настройку групповой политики диск С тестового компьютера. В редакторе объектов групповой политики в меню **Действие** выбираем команду **Создать правило для хеша**. Нажимаем кнопку **Обзор**, переходим в папку *Program Files|Internet Explorer* расположенную на тестовом компьютере и указываем файл *IEXPLORE.EXE*.

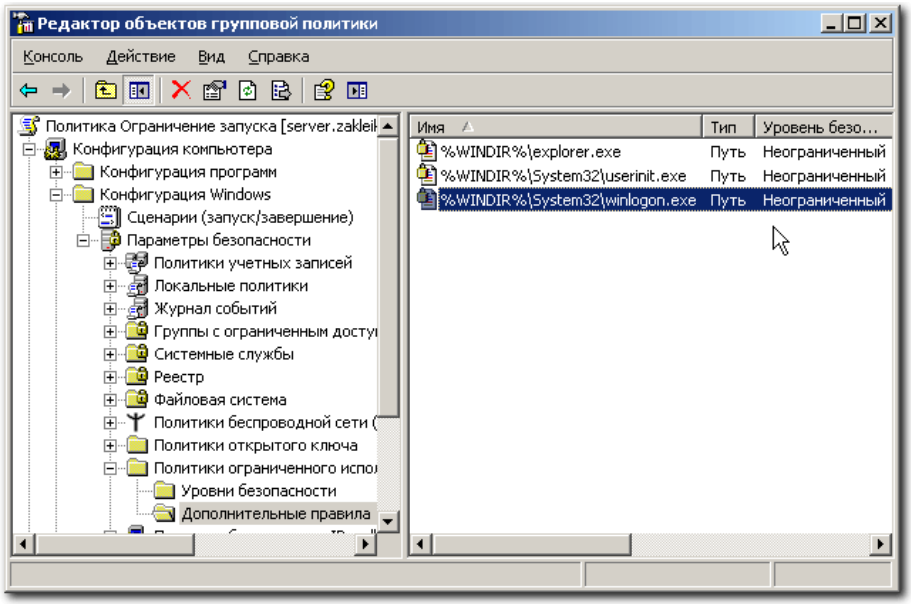

Рис. 19.

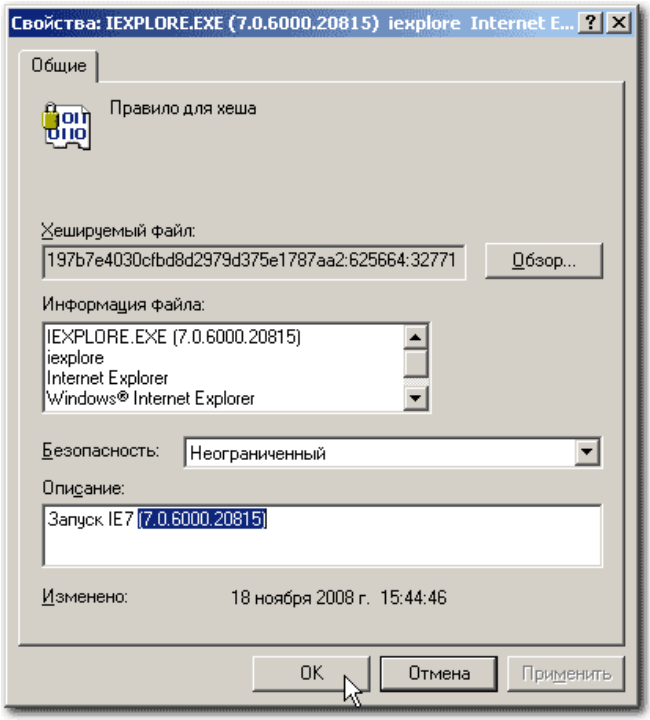

Рис. 20.

Чтобы потом не путаться, указываем в поле **Описание** название программы и ее версию. Отправляемся к тестируемому компьютеру проверять, что получилось. Для применения политик перезагружаем компьютер или выполняем на нем команду *gpupdate /force*. Пробуем запустить что-нибудь.

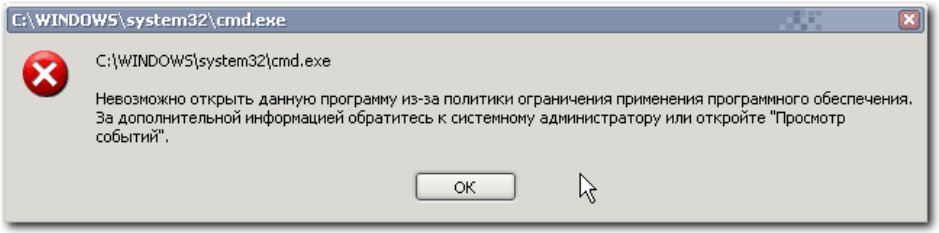

Рис. 21.

Запрет работает. Но щелчок по ярлыку IE на рабочем столе его тоже не запускает (хотя прямой запуск из Проводника в рабо-

чей папке IE сработает). Отменяем действие политики, чтобы посмотреть журнал ее применения (иначе Блокнот тоже не запустится). Наткнувшись на строчку вида

explorer.exe (PID = 372) identified C:\Documents and Settings\администратор\Рабочий стол\Запустить обозреватель Internet Explorer.lnk as Disallowed using default rule, Guid = {11015445-d282-4f86-96a2-9e485f593302}

вспоминаем, что ярлыки (то есть файлы с расширением .lnk) также расцениваются как исполняемый код. Поскольку у нас разрешен Проводник, нет особой нужды запрещать запуск ярлыков, тем более, что мы разрешаем запускать лишь определенные программы. Поэтому просто удалим тип LNK из списка назначенных типов файлов.

Напомним, что обновление параметров групповой политики происходит при загрузке компьютера, а обработка параметров, относящихся к пользователю – при его входе в систему. Принудительно обновить параметры групповой политики можно с помощью команды *gpupdate /force*. Утилита *gpupdate.exe* также является исполняемым кодом, и это следует учесть в период тестирования. Чтобы не перезагружать компьютер каждый раз после изменения параметров групповой политики для проверки работы правил, добавим *gpupdate.exe* в список разрешенных приложений. Разрешим еще запуск Блокнота и Калькулятора с помощью правил хеша. Все правила выглядят так:

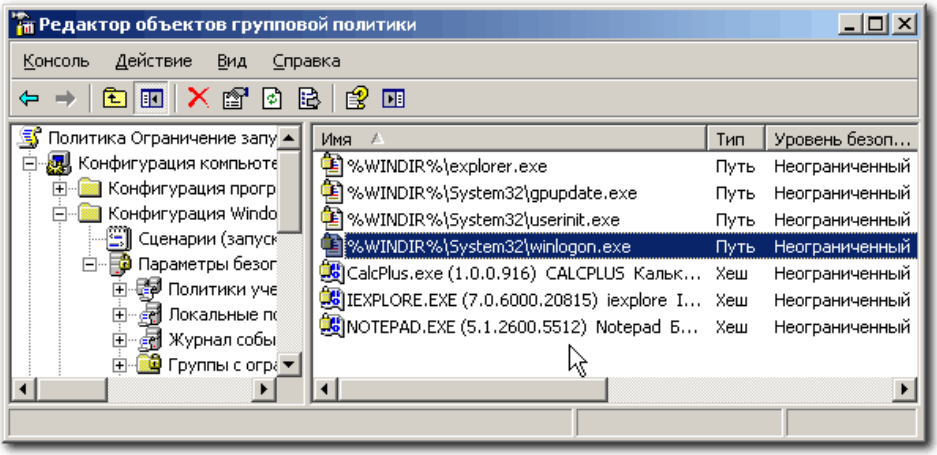

Рис. 22.

В дополнение к ограничениям, можно заставить какую-либо программу из разрешенных к запуску автоматически стартовать

при входе пользователя в систему. Для этого в разделе **Административные шаблоны** – **Система** – **Вход в систему** редактора политики выберите параметр **Запускать указанные программы при входе в систему**. Переведите переключатель в положение **Включен**, нажмите кнопку **Показать**. В открывшемся окне нажмите кнопку **Добавить** и укажите полный путь к программе (если она расположена в *system32*, достаточно указать только имя файла).

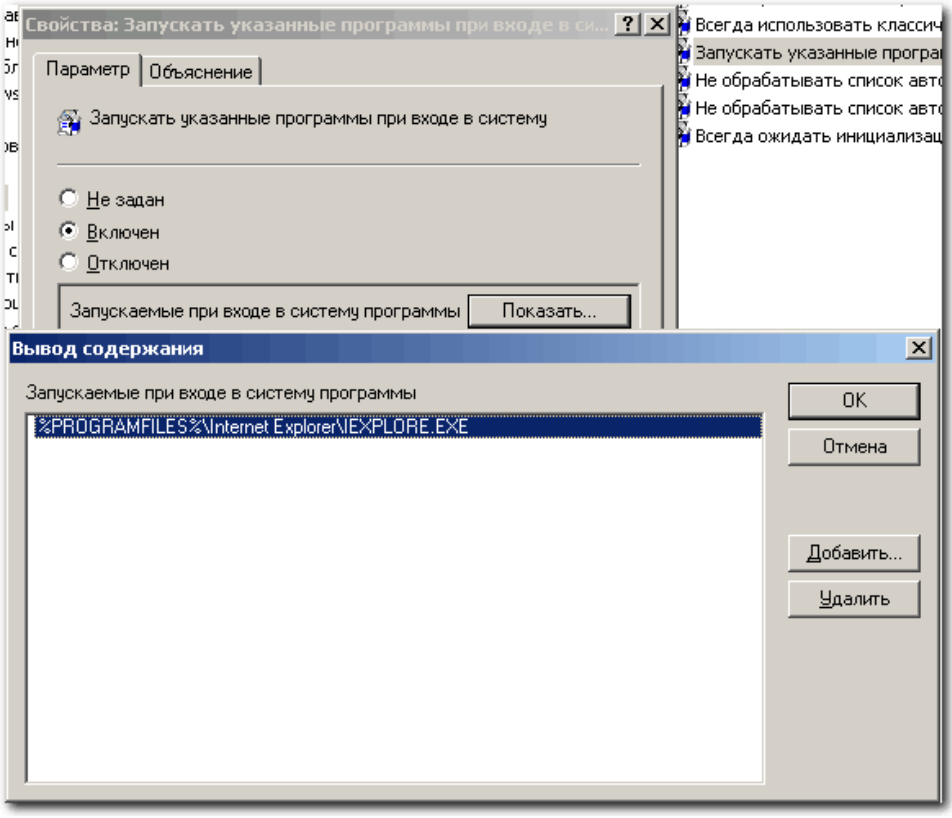

Рис. 23.

Компьютер теперь представляет собой подобие терминала, на котором любой пользователь (включая администраторов) может выполнить только те программы, для которых были созданы правила политики ограниченного использования программ. Даже выбрав в меню разрешенной программы команду Открыть и указав в диалоге исполняемый файл, который не указан в пра-

вилах, его запуск будет запрещен.

В следующем примере мы изменим настройки политики, применяя ее лишь к тем пользователям, которые входят в Test Unit. Для этого создаем одноименные параметры в ветви **Параметры пользователя**, а настройки из ветви **Параметры компьютера** удаляем. Если вы отключали обработку параметров пользователя для ускорения обработки политики, ее необходимо будет включить (наоборот, теперь, если параметры компьютера не используются, можно отключить их обработку). Перезагрузим компьютер, и попробуем войти с учетными записями пользователей, которые принадлежат OU Test Unit, и которые в него не входят. Ниже показан экран, который увидит пользователь с учетной записью, входящей в Test Unit.

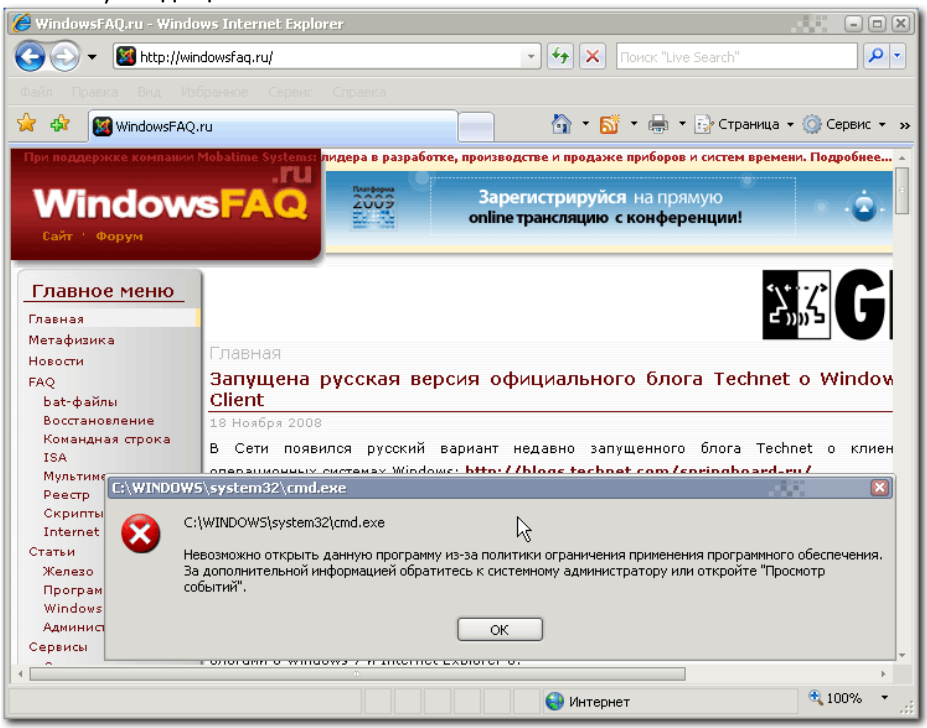

Рис. 24.

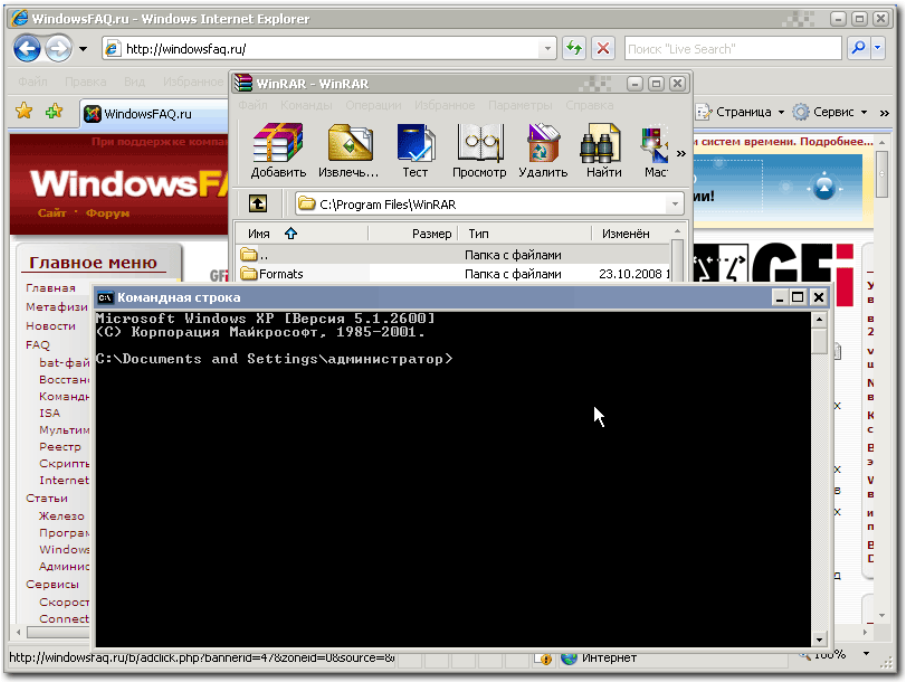

Рис. 25.

А здесь – пользователь, не входящий в Test Unit, не будет попадать под действие политики ограниченного использования программ.

Контрольные вопросы

1. Каково назначение Политики ограниченного использования программ?
2. Какие виды Политики ограниченного использования программ существуют?
3. Какие преимущества и недостатки имеются у Правила сертификата и Правила хеша?

ЛАБОРАТОРНАЯ РАБОТА 3
ПОЛИТИКИ УЧЕТНЫХ ЗАПИСЕЙ

Цель работы: исследование политики учетных записей

Краткие теоретические сведения

Применение **«Политики учетных записей»** распространено в предприятиях с доменной средой. Для обеспечения безопасности ваших компьютеров, применение политик этой группы на компьютерах, не входящих в доменную среду (например, использование политик на вашем домашнем компьютере) поможет вам существенно повысить безопасности компьютера.

Без сомнения, корпоративные учетные записи представляют огромный интерес для хакеров, которых может заинтересовать хищение корпоративной информации, а также получение доступа к компьютерам вашего предприятия. Поэтому, одним из решений, позволяющих существенно обезопасить инфраструктуру предприятия, является использование безопасных сложных паролей для снижения возможности проникновения злоумышленниками. Рекомендуется **заставить** пользователей использовать сложные пароли, включая буквы разных регистров, цифры, а также специальные символы для паролей к своим учетным записям и ни в коем случае не оставлять свои пароли у всех на виду, не записывать их на бумагу и не размещать на своем рабочем месте, рядом с компьютером, а тем более – не закреплять их на своих мониторах. Также пользователи обязаны менять свои пароли по истечению срока, который вы установите. Например, указав срок действия пароля в 30 дней, по его истечению перед входом пользователя в свою учетную запись, отобразится диалог с требованием изменения текущего пароля.

Политики, предназначенные для управления учетными записями, в редакторе управления групповыми политиками находятся в узеле **Конфигурация компьютера\Параметры безопасности\Политики учетных записей**. Рассмотрим подробно каждую политику безопасности, которая применяется для управления паролями и блокировкой учетных записей пользователей.

Политика паролей

При помощи этого узла вы можете изменять настройки паролей учетных записей пользователей, которые состоят как в домене, так и в рабочих группах. В организациях вы можете применять одинаковые политики паролей для всех пользователей, входящих в домен или только для отдельных групп при помощи

оснастки **«Консоль управления групповыми политиками»**. В узле **«Политика паролей»** вы можете использовать до шести политик безопасности, при помощи которых можно указать наиболее важные параметры безопасности, применяемые для управления паролями учетных записей. Настоятельно рекомендую не игнорировать данные политики. Даже если вы уговорите своих пользователей использовать сложные пароли, не факт, что они действительно будут это делать. Если вы правильно настроите все шесть политик безопасности, расположенных в этом узле, безопасность паролей пользователей вашей организации значительно повысится. Применив все политики, пользователям действительно придется создавать безопасные пароли, в отличие от тех, которые они считают «сложными». Доступны следующие политики безопасности:

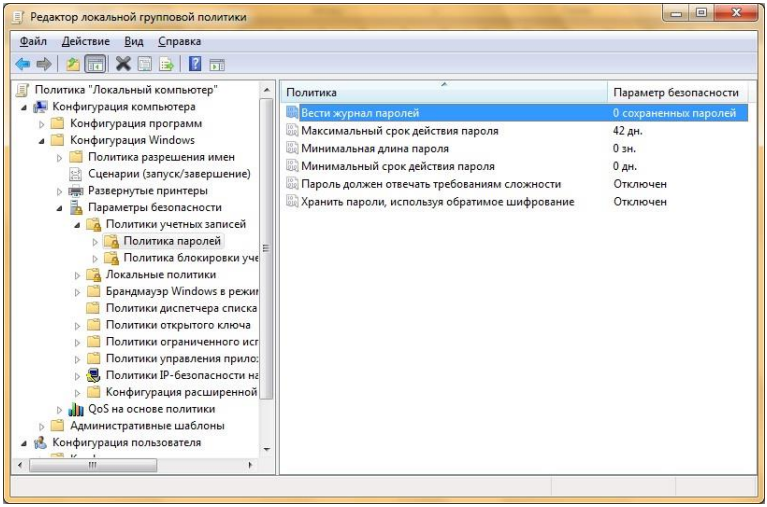

Рис. 1. Узел «Политика паролей»

Вести журнал паролей. Насколько не был бы ваш пароль безопасным, злоумышленник рано или поздно сможет его подобрать. Поэтому необходимо периодически изменять пароли учетных записей. При помощи этой политики вы можете указать количество новых паролей, которые назначаются для учетных записей до повторного использования старого пароля. После того как эта политика будет настроена, контроллер домена будет проверять кэш предыдущих хэш-кодов пользователей, чтобы в качестве нового пароля пользователи не могли использовать старый. Число

паролей может варьироваться от 0 до 24. Т.е., если вы указали в качестве параметра число 24, то пользователь сможет использовать старый пароль с 25-ого раза.

Максимальные срок действия пароля. Эта политика указывает период времени, в течение которого пользователь может использовать свой пароль до последующего изменения. По окончанию установленного срока пользователь обязан изменить свой пароль, так как без изменения пароля войти в систему ему не удастся. Доступные значения могут быть установлены в промежутке от 0 до 999 дней. Если установлено значения равное 0, срок действия пароля неограничен. В связи с мерами безопасности желательно отказаться от такого выбора. Если значения максимального срока действия пароля варьируется от 1 до 999 дней, значение минимального срока должно быть меньше максимального. Лучше всего использовать значения от 30 до 45 дней.

Минимальная длина пароля. При помощи этой политики вы можете указать минимальное количество знаков, которое должно содержаться в пароле. Если активировать этот параметр, то при вводе нового пароля количество знаков будет сравниваться с тем, которое установлено в этой политике. Если количество знаков будет меньше указанного, то придется изменить пароль в соответствии с политикой безопасности. Можно указать значение политики от 1 до 14 знаков. Оптимальным значением для количества знаков для пароля пользователей является 8, а для серверов от 10 до 12.

Минимальный срок действия пароля. Многие пользователи не захотят утруждать себя запоминанием нового сложного пароля и могут попробовать сразу при вводе изменить такое количество новых паролей, чтобы использовать свой хорошо известный первоначальный пароль. Для предотвращения подобных действий была разработана текущая политика безопасности. Вы можете указать минимальное количество дней, в течение которого пользователь должен использовать свой новый пароль. Доступные значения этой политики устанавливаются в промежутке от 0 до 998 дней. Установив значение равное 0 дней, пользователь сможет изменить пароль сразу после создания нового. Необходимо обратить внимание на то, что минимальный срок действия нового пароля не должен превышать значение максимального срока действия.

Пароль должен отвечать требованиям сложности. Это одна из самых важных политик паролей, которая отвечает за то, должен ли пароль соответствовать требованиям сложности

при создании или изменении пароля. В связи с этими требованиями, пароли должны:

– содержать буквы верхнего и нижнего регистра одновременно;

– содержать цифры от 0 до 9;

– содержать символы, которые отличаются от букв и цифр (например, !, @, #, $, *);

– Не содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков.

В том случае, если пользователь создал или изменил пароль, который соответствует требованиям, то пароль пропускается через математический алгоритм, преобразовывающий его в хэш-код (также называемый односторонней функцией), о котором шла речь в политике **«Вести журнал паролей».**

Хранить пароли, используя обратимое шифрование. Для того чтобы пароли невозможно было перехватить при помощи приложений, Active Directory хранит только хэш-код. Но если перед вами встанет необходимость поддержки приложений, использующих протоколы, требующие знание пароля пользователя для проверки подлинности, вы можете использовать текущую политику. Обратимое шифрование по умолчанию отключено, так как, используя эту политику, уровень безопасности паролей и всего домена в частности значительно понижается. Использование этой функции аналогично хранению пароля в открытом виде.

Политика блокировки учетной записи

Даже после создания сложного пароля и правильной настройки политик безопасности, учетные записи ваших пользователей все еще могут быть подвергнуты атакам недоброжелателей. Например, если вы установили минимальный срок действия пароля в 20 дней, у хакера достаточно времени для подбора пароля к учетной записи. Узнать имя учетной записи не является проблемой для хакеров, так как, зачастую имена учетных записей пользователей совпадает с именем адреса почтового ящика. А если будет известно имя, то для подбора пароля понадобится какие-то две-три недели.

Групповые политики безопасности Windows могут противостоять таким действиям, используя набор политик узла **«Политика блокировки учетной записи»**. При помощи данного набора политик, у вас есть возможность ограничения количества некорректных попыток входа пользователя в систему. Разумеется, для ваших пользователей это может быть проблемой, так как не у

всех получится ввести пароль за указанное количество попыток, но зато безопасность учетных записей перейдет на «новый уровень». Для этого узла доступны только три политики, которые рассматриваются ниже.

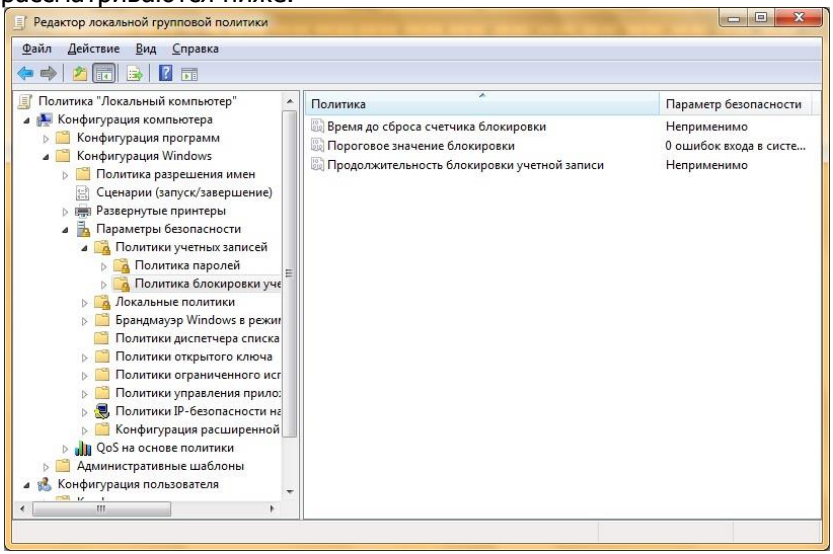

Рис. 2. «Политика блокировки учетной записи».

Время до сброса счетчиков блокировки. Active Directory и групповые политики позволяют автоматически разблокировать учетную запись, количество попыток входа в которую превышает установленное вами пороговое значение. При помощи этой политики устанавливается количество минут, которые должны пройти после неудачной попытки для автоматической разблокировки. Вы можете установить значение от одной минуты до 99999. Это значение должно быть меньше значения политики **«Продолжительность блокировки учетной записи»**.

Пороговое значение блокировки. Используя эту политику, вы можете указать количество некорректных попыток входа, после чего учетная запись будет заблокирована. Окончание периода блокировки учетной записи задается политикой **«Продолжительность блокировки учетной записи»** или администратор может разблокировать учетную запись вручную. Количество неудачных попыток входа может варьироваться от 0 до 999. Я рекомендую устанавливать допустимое количество от трех до семи попыток.

Продолжительность блокировки учетной записи. При

помощи этого параметра вы можете указать время, в течение которого учетная запись будет заблокирована до ее автоматической разблокировки. Вы можете установить значение от 0 до 99999 минут. В том случае, если значение этой политики будет равно 0, учетная запись будет заблокирована до тех пор, пока администратор не разблокирует ее вручную.

Политика Kerberos

В доменах Active Directory для проверки подлинности учетных записей пользователей и компьютеров домена используется протокол Kerberos. Сразу после аутентификации пользователя или компьютера, этот протокол проверяет подлинность указанных реквизитов, а затем выдает особый пакет данных, который называется **«Билет предоставления билета (TGT – Ticket Granting Ticket)»**. Перед подключением пользователя к серверу для запроса документа на контроллер домена пересылается запрос вместе с билетом TGT, который идентифицирует пользователя, прошедшего проверку подлинности Kerberos. После этого контроллер домена передает пользователю еще один пакет данных, называемый билетом доступа к службе. Пользователь предоставляет билет на доступ службе на сервере, который принимает его как подтверждение прохождения проверки подлинности.

Данный узел вы можете обнаружить только на контроллерах домена. Доступны следующие пять политик безопасности:

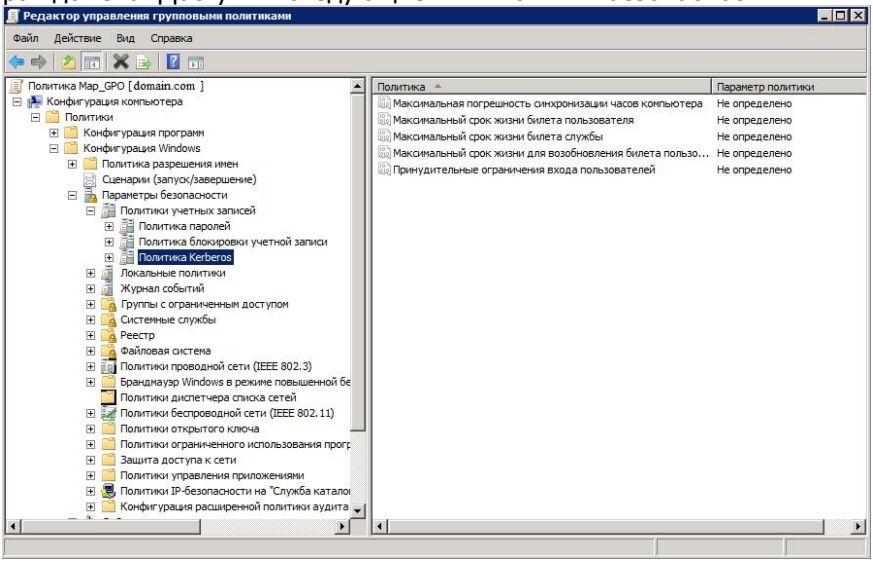

Рис. 3. «Политика Kerberos».

Максимальная погрешность синхронизации часов компьютера. Для предотвращения «атак повторной передачи пакетов» существует текущая политика безопасности, которая определяет максимальную разность времени, допускающую Kerberos между временем клиента и временем на контроллере домена для обеспечения проверки подлинности. В случае установки данной политики, на обоих часах должны быть установлены одинаковые дата и время. Подлинной считается та отметка времени, которая используется на обоих компьютерах, если разница между часами клиентского компьютера и контроллера домена меньше максимальной разницы времени, определенной этой политикой.

Максимальный срок жизни билета пользователя. При помощи текущей политики вы можете указать максимальный интервал времени, в течение которого может быть использован билет представления билета (TGT). По истечении срока действия билета TGT необходимо возобновить существующий билет или запросить новый.

Максимальный срок жизни билета службы. Используя эту политику безопасности, сервер будет выдавать сообщение об ошибке в том случае, если клиент, запрашивающий подключение к серверу, предъявляет просроченный билет сеанса. Вы можете определить максимальное количество минут, в течение которого полученный билет сеанса разрешается использовать для доступа к конкретной службе. Билеты сеансов применяются только для проверки подлинности на новых подключениях к серверам. После того как подключение пройдет проверку подлинности, срок действия билета теряет смысл.

Максимальный срок жизни для возобновления билета пользователя. С помощью данной политики вы можете установить количество дней, в течение которых может быть восстановлен билет предоставления билета.

Принудительные ограничения входа пользователей. Эта политика позволяет определить, должен ли центр распределения ключей Kerberos проверять каждый запрос билета сеанса на соответствие политике прав, действующей для учетных записей пользователей.

Заключение

В наше время все чаще приходится заботиться о безопасности учетных записей, как для клиентских рабочих мест вашей организации, так и домашних компьютеров. Недоброжелателями, которые хотят получить контроль над вашим компьютером могут

быть не только хакеры, расположенные в тысячах и сотнях тысяч километров от вас, но и ваши сотрудники.

Порядок выполнения работы

1. Настройка Политики учетных записей (Account Policy)

На этом занятии вы настроите параметры ***Политики учетных записей*** (Account Policy) для вашего компьютера и убедитесь, что параметры заданы корректно.

Настройка минимальной длины пароля

Используете консоль MMC, содержащую оснастку ***Групповая политика*** (Group Policy), созданную ранее для задания минимальной длины пароля, одного из параметров ***Политики учетных записей*** (Account Policy) для вашего компьютера. Проверьте правильность настройки.

Для задания минимальной длины пароля:

1. Войдите в систему под учетной записью, входящей в группу Администраторы. Щелкните ***Пуск*** (Start), щелкните ***Выполнить*** (Run), введите **mmc** и текстовом поле ***Открыть*** (Open) и щелкните ОК., чтобы открыть консоль MMC.

2. В меню ***Консоль®File*** щелкните имя консоли с оснасткой ***Групповая политика*** (Group Policy), созданной и сохраненной при настройке политики аудита.

3. В консоли последовательно разверните разделы ***Политика «Локальный компьютер»*** (Local Computer Policy), ***Конфигурация компьютера*** (Computer Configuration), **Конфигурация Windows** (Windows Settings), ***Параметры безопасности*** (Security Settings) и ***Политики учетных записей*** (Account Policies).

Раздел ***Политики учетных записей*** (Account Policies) содержит два узла: ***Политика паролей*** (Password Policy) и ***Политика блокировки учетной записи*** (Account Lockout Policy).

4. В дереве консоли щелкните ***Политика паролей*** (Password Policy).

5. В правой части окна щелкните правой кнопкой мыши параметр ***Мин. длина пароля*** (Minimum Password Length), затем щелкните пункт контекстного меню ***Свойства*** (Properties).

Windows XP Professional отображает диалоговое окно Свойства***: Мин. длина пароля*** (Minimum Password Length Properties).

6. В поле ***Длина пароля не менее*** (Password Must Be At Least) введите 8, чтобы установить минимальную длину пароля равной восьми символам, а затем щелкните ОК.

7. Щелкните в меню ***Консоль*** пункт ***Выход*** (Exit) для завершения работы с консолью MMC.

8. В диалоговом окне ***Сохранить параметры консоли*** (Save Console Settings To Local Group Policy) щелкните кнопку ***Нет*** (No).

Проверка минимальной длины пароля

1. Щелкните ***Пуск*** (Start), а затем –***Панель управления*** (Control Panel).

2. Щелкните категорию ***Учетные записи пользователей*** (User Accounts), затем –***Создание учетной записи*** (Create A New Account).

3. В текстовом поле ***Введите имя для новой учетной записи*** (Type A Name For The New Account) введите Userl3 и щелкните кнопку ***Далее*** (Next).

4. Щелкните переключатель ***Ограниченная учетная запись*** (Limited), а затем –кнопку ***Создать учетную запись*** (Create Account).

5. Щелкните значок учетной записи User 13, а затем –***Изменение пароля*** (Change The Password).

6. В текстовых полях ***Введите новый пароль*** (Type A New Password) и ***Введите новый пароль для подтверждения*** (Type The New Password Again To Confirm) введите **water**.

7. Щелкните кнопку ***Сменить пароль*** (Change Password). Откроется диалоговое окно ***Учетные записи пользователей*** (User Accounts) с сообщением, что новый пароль не соответствует требованиям политики паролей. Этот тест показывает, что вы правильно настроили параметр, определяющий минимальную длину пароля.

8. Щелкните ОК, чтобы закрыть окно сообщений ***Учетные записи пользователей*** (User Accounts).

9. Щелкните кнопку ***Отмена*** (Cancel), чтобы закрыть окно ***Изменение пароля учетной записи*** **User13** (Change Userl3's Password).

10. Закройте окно ***Что вы хотите изменить в учетной записи пользователя Userl3*** (What Do You Want To Change About UserB's Account), а затем –***Панель управления*** (Control Panel).

2. Настройка и проверка дополнительных параметров политики учетных записей

Настройка параметров политики учетных записей

1. Средствами созданной в консоли MMC консоли ***Политика «Локальный компьютер»*** (Local Group Policy) настройте

следующие параметры ***Политики учетных записей*** (Account Policy):

– пользователь должен сменить не менее пяти различных паролей, прежде чем сможет повторно использовать старый пароль;

– после смены пароля должно пройти 24 часа, прежде чем пользователь сможет снова сменить пароль;

– пользователь должен менять свой пароль каждые три недели.

2. Закройте консоль MMC.

Проверка параметров политики учетных записей

1. Войдите в систему под учетной записью **User13**, не вводя пароль. Windows XP Professional откроет окно с сообщением, что вы должны сменить свой пароль при первом входе в систему.

2. Щелкните ОК, чтобы закрыть окно сообщений.

3. Нажмите Tab, чтобы перейти к полю ***Новый пароль*** (New Password), поле ***Старый пароль*** (Old Password) оставьте пустым.

4. В текстовых полях ***Новый пароль*** (New Password) и ***Подтверждение*** (Confirm New Password) введите hotwater и щелкните ОК. Windows XP Professional отобразит окно сообщений ***Смена пароля*** (Change Password) с сообщением, что пароль был успешно изменен.

5. Щелкните ОК, чтобы закрыть окно сообщений ***Смена пароля*** (Change Password).

6. Щелкните Пуск (Start), а затем –***Панель управления*** (Control Panel).

7. Щелкните категорию ***Учетные записи пользователей*** (User Accounts), а затем ***Изменить мой пароль*** (Change My Password).

8. В текстовом поле ***Введите текущий пароль*** (Type Your Current Password) введите **hotwater**.

9. В текстовом поле ***Введите новый пароль*** (Type A New Password) и ***Введите пароль для подтверждения*** (Type The New Password Again To Confirm) введите chocolate.

10. Щелкните кнопку ***Сменить пароль*** (Change Password).

Все ли успешно? Почему да или почему нет?

11. Закройте все открытые окна и завершите работу с системой.

3. Настройка Политики блокировки учетной записи (Account Lockout Policy)

Настройте параметры ***Политики блокировки учетной***

записи (Account Lockout Policy), а затем проверите правильность заданных параметров.

1. Зарегистрируйтесь под учетной записью, входящей в группу ***Администраторы*** (Administrators).

2. Щелкните ***Пуск*** (Start), затем –***Выполнить*** (Run).

3. В текстовом поле ***Открыть*** (Open) введите **mmc** и нажмите **Enter**.

4. Откройте созданную вами консоль групповой политики.

5. В дереве консоли дважды щелкните раздел ***Политика учетных записей*** (Account Policies).

6. Щелкните ***Политика блокировки учетной записи*** (Account Lockout Policy).

7. Настройте параметры ***Политики блокировки учетной записи*** (Account Lockout Policy) в соответствии со следующими требованиями:

– учетная запись пользователя должна блокироваться после четырех неудачных попыток входа в систему;

– учетные записи должны оставаться заблокированными, пока их не разблокирует администратор.

Примечание: Если появляется диалоговое окно ***Предлагаемые изменения значений*** (Suggested Value Changes), щелкните OK и удостоверьтесь, что установленные значения правильны.

8. Закончите сеанс работы с Windows XP Professional.

Проверка параметров Политики блокировки учетной записи (Account LockoutPolicy)

1. Попробуйте четыре раза войти в систему под учетной записью **User13**с паролем **chocolate**.

2. Попробуйте еще раз войти в систему под учетной записью **User13** с паролем **chocolate**. Откроется диалоговое окно с сообщением, что учетная запись пользователя заблокирована.

3. Щелкните OK и войдите в систему под учетной записью, входящей в группу ***Администраторы*** (Administrators).

Вы можете настроить права пользователя на компьютере, работающем под управлением Windows XP Professional, применив оснастку ***Групповая политика*** (Group Policy), как описано далее.

1. Щелкните ***Пуск*** (Start), затем –***Выполнить*** (Run). Введите **mmc** в текстовом поле ***Открыть (***Open) и щелкните OK, чтобы открыть пустую консоль MMC.

2. В меню ***Консоль*** (File) щелкните пункт ***Добавить или удалить оснастку*** (Add/Remove Snap-In), а затем щелкните кнопку ***Добавить*** (Add).

3. В диалоговом окне ***Добавить изолированную оснаст-***

ку (Add Standalone Snap-In) щелкните значок оснастки ***Групповая политика*** (Group Policy), а затем –кнопку ***Добавить*** (Add).

Откроется окно ***Выбор объекта для настройки групповой политики*** (Select Group Policy Object), в котором можно настроить фокус-оснастки ***Групповая политика*** (Group Policy) на локальный или на удаленный компьютер. Флажок ***Разрешить изменение фокуса «Оснастки групповой политики» при запуске из командной строки*** (Allow The Focus Of The Group Policy Snap-In To Be Changed When Launching From The Command Line) позволяет настроить консоль MMC таким образом, что каждый раз при запуске консоли MMC будет появляться предложение выбрать фокус групповой политики.

4. Щелкните кнопку ***Готово (***Finish), чтобы установить оснастку ***Групповая политика*** (Group Policy), оставив выбранную по умолчанию привязку к локальному компьютеру, и сохраните созданную консоль.

5. В дереве консоли разверните раздел ***Политика «Локальный компьютер»*** (Local Computer Policy), затем – ***Конфигурация компьютера*** (Computer Configuration), ***Конфигурация Windows*** (Windows Settings), ***Параметры безопасности*** (Security Settings) и ***Локальные политики*** (Local Policies), а затем щелкните узел ***Назначение прав пользователя*** (User Right Assignments).

6. В правой части окна выберите одно из прав пользователя, которое вы собираетесь настраивать и в меню ***Действие*** (Action) щелкните пункт ***Свойства*** (Properties).

7. Консоль отобразит список групп и пользователей, для которых назначено это право. Чтобы добавить группу или учетную запись пользователя, щелкните кнопку ***Добавить*** (Add). Для удаления группы или пользователя щелкните запись группы или пользователя, а затем –кнопку ***Удалить*** (Remove).

Оснастка Групповая политика (Group Policy) отображает назначенные права пользователей

Для обновления групповой политики в командной строке выполните команду **gpupdate**.

Указания по выполнению отчета

Отчет должен содержать:

- название работы;
- цель работы;
- порядок действий по выполнению лабораторной работы;
- устанавливаемые в процессе работы параметры;

– выводы по результатам проделанной работы.

Контрольные вопросы

1. Как настроить длину пароля? Почему необходимо ограничивать нижнее значение длины пароля?
2. Как проверить установленные параметры политики паролей?
3. Какие дополнительные параметры политики учетных записей можно настроить? Как это сделать?
4. Как настроить политику блокировки учетной записи? В каком случае это бывает нужно?
5. Если компьютер работает в сети и заблокирована Ваша учетная запись – можно ли войти в сеть с другого компьютера? Почему?
6. Запустите консоль Локальная политика безопасности из меню Администрирование.
7. Разверните узел Политика паролей.
8. Задайте максимальный срок действия пароля, равный 7 дням.
9. Задайте минимальную длину пароля, равную 7 символам.
10. Задайте минимальный срок действия пароля, равный 1 дню.
11. Включите параметр, требующий безопасных паролей.
12. Настройте систему на хранение 10 последних паролей.
13. Разверните узел Политика блокировки учетных записей.
14. Установите пороговое значение блокировки, равное 3.
15. Установите время блокировки, равное 15 минутам.
16. Установите время сброса счетчика неверных попыток, равное 5 минутам.
17. В командной строке выполните команду gpupdate.

ЛАБОРАТОРНАЯ РАБОТА 4
РЕАЛИЗАЦИЯ ПОЛИТИКИ БЕЗОПАСНОСТИ В ЗАЩИЩЕННЫХ ВЕРСИЯХ ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS

Цель работы: получение навыков по созданию политики аудита и управлению аудитом ресурсов и событий защищенной операционной системы Windows-XP.

Краткие теоретические сведения

Аудит – одна из функций групповой политики Windows XP Professional. Подсистема аудита (auditing) –это инструмент, предназначенный для поддержания безопасности в сети и позволяющий отслеживать действия пользователей, а также действия операционной системы Windows XP Professional, называемые событиями (events). Средствами аудита можно задать режим, при котором Windows XP Professional регистрирует события в журнале безопасности (security.log). В нем хранятся записи об успешных и неудачных попытках входа в систему и о таких событиях, как создание, открытие и закрытие файлов или других объектов. Запись аудита в журнале безопасности содержит данные о:

– выполненных операциях;

– пользователях, выполнивших операцию;

– успешном или неуспешном выполнении операции, кроме того, указывается время, когда произошло данное событие.

Политика аудита (audit policy) задает типы событий системы безопасности, которые Windows XP Professional регистрирует в журнале безопасности каждого компьютера. Журнал безопасности позволяет отслеживать заданные события.

Система Windows XP Professional регистрирует событие в журнале безопасности того компьютера, на котором событие происходит. Так, каждый раз, когда кто-нибудь пытается войти в систему и попытка входа оказывается неудачной, Windows XP Professional регистрирует событие в журнале безопасности данного компьютера.

Можно настроить политику аудита для данного компьютера на выполнение следующих операций:

– выявление успешных или неудачных действий, например попыток входа пользователей в систему или отдельного пользователя прочитать указанный файл, изменения учетной записи пользователя или принадлежности к группе, изменение парамет-

ров безопасности;

– исключение или минимизация риска неавторизованного использования ресурсов.

Для просмотра событий, зарегистрированных системой Window-XP Professional в журнале безопасности, используется утилита. Просмотр событий (Event Viewer). Можно также сохранять файлы журнала в архиве для выяснения закономерностей за указанный период времени –например, чтобы определить частоту использования принтеров или файлов или выявление попыток неавторизованного использования ресурсов.

При планировании политики аудита нужно определить, какие события следует регистрировать и на каких компьютерах надо установить аудит. По умолчанию аудит отключен.

Можно регистрировать следующие типы событий:

– попытки доступа к файлам и папкам;

– вход в систему и выход из нее;

– выключение компьютера с Windows XP Professional;

– запуск компьютера с Windows XP Professional;

– изменения учетных записей пользователей и групп;

– попытки изменения объектов Active Directory (только если компьютер с Windows XP Professional является частью домена).

После того как типы регистрируемых событий заданы, нужно определить, регистрировать ли успешные действия, неудавшиеся попытки или оба вида событий.

Отслеживание успешных действий дает информацию о том, как часто система Windows XP Professional или пользователи обращаются к конкретным файлам, принтерам или другим объектам; эта информация пригодится для планирования ресурсов.

Регистрация неудачных попыток позволяет выявить слабые места в защите системы. Так, если зафиксировано несколько неудачных попыток входа в систему под определенным именем пользователя, особенно в нерабочее время, можно предположить, что неавторизованный пользователь пытается «взломать» систему. Кроме того, при выборе политики аудита руководствуйтесь правилами:

– Определите, нужно ли отслеживать закономерности загрузки системы. Если да, то предусмотрите сохранение журналов событий в архиве. Это позволит контролировать распределение загрузки по времени и заранее планировать увеличение ресурсов системы.

– Часто просматривайте журналы безопасности. Обязательно установите расписание и регулярно просматривайте журналы

безопасности, так как выполнение аудита само по себе не предупреждает о слабых местах в защите системы.

– Задайте информативную и работоспособную политику аудита. Всегда регистрируйте попытки доступа к жизненно важным и конфиденциальным данным. Регистрируйте только те события, которые дают существенную информацию. Это снижает потребление ресурсов компьютера до минимума и упрощает поиск нужной информации. Регистрация большого числа событий может привести к чрезмерной трате системных ресурсов Windows XP Professional.

Аудит – мощный инструмент для отслеживания событий, происходящих на компьютерах в вашем офисе. Прежде чем применять аудит, следует продумать требования к нему и установить политику аудита. Далее можно выполнять аудит файлов, папок и принтеров.

На компьютерах с Windows XP Professional политики аудита устанавливаются для каждого компьютера в отдельности. Для установки и администрирования аудита необходимо:

– иметь право пользователя Управление аудитом и журналом безопасности (Manage Auditing And Security Log) на том компьютере, на котором планируется установить политику аудита или просмотреть журнал безопасности. По умолчанию в Windows XP Professional такие права имеет группа Администраторы (Administrators);

– разместить файлы и папки, аудит которых планируется, на томах с файловой системой NTFS.

Настройка аудита выполняется в два этапа.

1. Задание политики аудита. Политика аудита разрешает аудит объектов, но не инициирует аудит заданных объектов.

2. Разрешения аудита заданных ресурсов. Для файлов, папок, принтеров и объектов Active Directory назначаются конкретные события, подлежащие регистрации. После этого Windows XP Professional начинает отслеживать заданные события и регистрировать их в журнале.

На первом этапе установки политики аудита в Windows XP Professional необходимо выбрать типы событий, подлежащих регистрации. Для каждого регистрируемого события в параметрах указывается, какие попытки следует отслеживать –успешные или неудачные. Политика аудита на локальном компьютере устанавливается средствами оснастки Групповая политика, которую можно запустить, используя Консоль управления MMC (Microsoft

Management Console) и добавив в консоль оснастку Групповая политика (Group Policy). В таблице 4.1 перечислены типы событий, регистрируемые в Windows XP Professional.

Таблица 4.1

Типы событий, регистрируемых Windows XP Professional

Событие	Описание
Вход в систему под заданной учетной записью	Контроллер домена получил запрос на проверку учетной записи пользователя (применяется только в тех случаях, когда компьютер с Windows XP Professional входит в домен Microsoft Windows 2000)
Управление учетными записями	Администратор создал, изменил или удалил учетную запись пользователя или группу. Некоторая учетная запись была переименована, отключена или включена, или для нее был назначен или изменен пароль
Доступ к службе каталогов	Пользователь получил доступ к объекту Active Directory. Для регистрации событий этого типа нужно сконфигурировать аудит для определенных объектов Active Directory (Active Directory можно применять, только если компьютер с Windows XP Professional входит в домен Microsoft Windows 2000)
Вход в систему	Пользователь локально вошел в систему или вышел из нее, или подключился к компьютеру через сеть (или отключился от него)
Доступ к объектам	Пользователь получил доступ к файлу, папке или принтеру. Определенные файлы, папки или принтеры должны быть настроены для аудита. В этом случае регистрируется доступ пользователей к файлам, папкам и принтерам
Изменение системной политики	Изменены пользовательские параметры безопасности, права пользователя или политика аудита
Использование привилегий	Пользователь применил права, например изменил системное время (в этом случае не подразумеваются права, связанные с регистрацией в системе или с выходом из нее)

Отслеживание процесса	Программа выполнила действие. Эта информация важна главным образом для программистов, которым нужно детально проследить выполнение программы
Системные события	Пользователь перезапустил или выключил компьютер, или произошло событие, повлиявшее на безопасность Windows XP Professional или на журнал безопасности. Например, журнал аудита переполнился и Windows XP Professional начинает игнорировать поступающие сообщения о событиях

После настройки параметров политики аудита имейте в виду, что изменения в политике аудита компьютера вступают в силу только после перезагрузки.

Если требуется выявить слабые места в защите корпоративной сети, можно установить аудит файлов и папок, расположенных на разделах NTFS. Для аудита доступа пользователей к файлам и папкам прежде всего следует настроить политику аудита на регистрацию доступа к объектам, в том числе файлов и папок. При настройке политики аудита на регистрацию доступа к объектам включается аудит конкретных файлов и папок. При этом также указывается, какие виды доступа, пользователи и группы подлежат аудиту.

В таблице 4.2 перечислены действия пользователей, вызывающие соответствующие события, что поможет определить, в каких случаях следует включать аудит этих событий.

Таблица 4.2

События для файлов и папок, вызываемые действиями пользователей.

Событие	Действие пользователя, вызвавшее событие
Переход в папку/Выполнение файла (Traverse Folder/Execute File)	Запуск программы или получение доступа к папке при смене текущей папки
Получение списка файлов/Чтение данных (List Folder/Read Data)	Просмотр содержимого файла или папки
Чтение атрибутов (Read Attributes)	Просмотр атрибутов файла или папки

Чтение расширенных атрибутов (Read Extended Attributes)	Просмотр атрибутов файла или папки
Создание файлов/Запись данных (Create Files/Write Data)	Изменение содержимого файла или создание новых файлов в папке
Создание папок/Добавление данных (Create Folders/Append Data)	Создание папок внутри папок
Запись атрибутов (Write Attributes)	Изменение атрибутов файла или папки
Запись расширенных атрибутов (Write Extended Attributes)	Изменение атрибутов файла или папки
Удаление вложенных папок и файлов (Delete Subfolders And Files)	Удаление файла или папки внутри папки
Удаление (Delete)	Удаление файла или папки
Чтение разрешений (Read Permissions)	Просмотр прав владельца файла на файл или папку
Смена разрешений (Change Permissions)	Изменение прав доступа к файлу или папке
Смена владельца (Take Ownership)	Изменить право владельца на файл или папку

При необходимости отслеживать использование конкретных принтеров включите аудит доступа к принтерам. Чтобы включить аудит доступа к принтерам, в политике аудита настройте аудит доступа к объектам, что включает принтеры.

Включите аудит конкретных принтеров и укажите, какие виды .доступа регистрировать и какие пользователи будут иметь доступ. Для выбранного принтера аудит включается в той же последовательности, что и при установке параметров аудита файлов и папок.

В таблице 4.3 перечислены события, аудит которых возможен для принтеров, и соответствующие этим событиям действия пользователей.

Таблица 4.3

События для принтеров, вызываемые действиями пользователей.

Событие	Действие пользователя, вызвавшее событие
Печать (Print)	Печать файла
Управление принтерами (Manage Printers)	Изменение параметров принтера, приостановка печати, разрешение совместного использования принтера, удаление принтера из системы
Управление документами (Manage Documents)	Изменение параметров заданий; приостановка или продолжение печати, изменение порядкового номера в очереди или удаление документов; разрешение совместного использования принтера; изменение параметров принтера
Чтение разрешений (Read Permissions)	Просмотр прав доступа к принтеру
Смена разрешений (Change Permissions)	Изменение прав доступа к принтеру
Смена владельца (Take Ownership)	Смена владельца принтера

Утилита Просмотр событий (Event Viewer) применяется для решения различных задач администрирования, в том числе для просмотра журналов аудита, созданных в результате установки политики аудита и обновляемых при возникновении заданных событий. Утилиту Просмотр событий (Event Viewer) также используют для просмотра содержимого файлов журнала безопасности и поиска конкретных событий в файлах журнала.

Утилита Просмотр событий (Event Viewer) необходима для просмотра информации, содержащейся в журналах (logs) Windows XP Professional. По умолчанию эта утилита позволяет просматривать три журнала (таблица 4.4).

Таблица 4.4
Журналы Windows XP Professional

Журнал	Описание
Журнал приложений	Хранит сообщения об ошибках, предупреждения или информацию, генерируемые приложениями, например СУБД или программой электронной почты. События, регистрируемые в журнале, задаются разработчиками соответствующих программ
Журнал безопасности	Содержит информацию об успешных или неудачных попытках выполнения операций, аудит которых включен. Эти события регистрируются Windows XP Professional в соответст-вии с политикой аудита
Системный журнал	Хранит сообщения об ошибках, предупреждения и данные, генерируемые Windows XP Professional. События, регистрируемые в журнале, задаются в Windows XP Professional

Примечание Если установлены дополнительные службы, могут быть добавлены и соответствующие журналы событий.

Просмотр журнала безопасности

В журнале безопасности (security log) хранится информация о событиях, которые отслеживаются политикой аудита, например неудачные и успешные попытки регистрации в системе.

Windows XP Professional регистрирует события в журнале безопасности того компьютера, на котором событие произошло. Эти события можно просматривать с любого компьютера при наличии прав администратора на компьютере, на котором произошло событие. Чтобы просмотреть журнал безопасности удаленного компьютера, откройте консоль MMC и выберите просмотр событий удаленного компьютера.

При первом запуске утилиты Просмотр событий (Event Viewer) автоматически отображаются все события, зарегистрированные в выбранном журнале. Чтобы показать нужные события, можно использовать команду Фильтр (Filter). Кроме того, для поиска конкретных событий применяют команду Найти (Find).

Чтобы выполнить отбор или поиск событий, запустите ути-

литу Просмотр событий (Event Viewer), затем в меню Вид (View) щелкните пункт Фильтр (Filter) или Найти (Find). Параметры в окнах фильтра и поиска практически не отличаются.

В таблице 4.5 перечислены параметры вкладки Фильтр (Filter), используемые для отбора нужных событий, и команды Найти (Find), применяемые для поиска нужных событий.

Сравнивая данные журналов, записанные в разное время, можно выявлять закономерности в работе Windows XP Professional. Их анализ позволяет определять загруженность ресурсов и планировать их расширение. Кроме того, в журналах фиксируются попытки неавторизованного использования ресурсов. Windows XP Professional позволяет изменять размер файлов журнала и задавать действия системы при переполнении журнала.

Таблица 4.5

Параметры для фильтрации и поиска событий.

Параметр	Описание
Типы событий (Event Types)	Типы событий для просмотра
Источник события (Event Source)	Программа или драйвер компонента, вызвавший событие
Категория (Category)	Тип события, например попытка входа, выхода или системное событие
Код события (Event ID)	Идентификационный номер события. Он упрощает сотрудникам службы технической поддержки контроль событий
Пользователь (User)	Имя учетной записи пользователя
Компьютер (Computer)	Имя компьютера
«С» и «До» (From and To)	Интервал времени, за который вы хотите просмотреть события [только на вкладке Фильтр (Filter)]
Восстановить значения по умолчанию (Restore Defaults)	Отменяет все изменения на этой вкладке и восстанавливает значения по умолчанию
Описание (Description)	Текстовый фрагмент в описании события (только в диалоговом окне Найти (Find)

Направление поиска (Search Direction)	Направление, в котором программа поиска будет просматривать журнал (вверх или вниз; только в диалоговом окне Найти (Find)
Найти далее (Find Next)	Программа поиска находит и отображает следующую запись, удовлетворяющую условиям поиска

Параметры каждого журнала аудита можно настраивать в отдельности. Чтобы изменить параметры журнала, выберите его название в окне утилиты Просмотр событий (Event Viewer), а затем в меню Действие (Action) щелкните пункт Свойства (Properties). В диалоговом окне Свойства (Properties) для каждого типа журнала аудита настраиваются следующие параметры:

– предельный размер каждого журнала, который может изменяться от 64 кбайт до 4194240 кбайт (4 Гбайт). По умолчанию размер журнала составляет 512 кбайт;

– действия Windows XP Professional при достижении файлом журнала предельного размера. Чтобы настроить эти действия, выберите один из вариантов, перечисленных в таблице 4.6.

Архивация журналов безопасности позволяет вести учет событий, связанных с безопасностью. На многих предприятиях принято сохранять архивированные журналы в течение некоторого времени, чтобы иметь возможность просмотреть информацию по безопасности за требуемый период.

Чтобы сохранить, очистить или просмотреть архивированный журнал, выберите нужный журнал в окне утилиты Просмотр событий (Event Viewer) и выполните одно из действий, перечисленных в таблице 4.7.

Таблица 4.6

Варианты обработки заполненных файлов журнала аудита.

Параметр	Описание
Удалять старые события по необходимости (Overwrite Events As Needed)	Если установлен этот параметр, можно потерять информацию при переполнении журнала до того, как его сохранят. Однако при этом не требуется обслуживания

Удалять события, произошедшие более, чем V дней назад (Overwrite Events Older Than X Days)	Если установлен этот параметр, можно потерять информацию при переполнении журнала до того, как его сохранят. Будет утрачена только та информация, которая поступила более V дней назад. При применении этого параметра необходимо указать число дней (по умолчанию 7)
Не удалять события (Do Not Overwrite Events)	Если установлен этот параметр, нужно очищать журнал вручную. При заполнении журнала Windows XP Professional прекращает регистрацию событий, сохраняя уже имеющиеся записи журнала безопасности

Таблица 4.7

Действия для архивации, очистки или просмотра файла журнала.

Действие	Выполните
Сохранить журнал в архиве	Щелкните Сохранить файл журнала как (Save Log File As), затем введите имя файла
Очистить журнал	Для очистки журнала щелкните Стереть все события (Clear All Events). При этом Windows XP Professional генерирует запись в журнале безопасности о том, что журнал очищен
Просмотреть архиви-рованный журнал	Щелкните Новый вид журнала (New Log View); укажите вид выбранного журнала

Задания и методические указания о их выполнению

1. Планирование и настройка политики аудита ресурсов и событий

Планирование политики аудита

Для планирования политики аудита компьютера прежде всего нужно ответить на несколько вопросов.

– Какие типы событий регистрировать?

– Регистрировать успешные, неудачные попытки или оба вида событий?

– Принимая решение, руководствуйтесь правилами, описанными далее.

– Необходимо регистрировать неудачные попытки доступа к компьютеру.

– Необходимо регистрировать неавторизованный доступ к файлам, составляющим базу данных по клиентам.

– Необходимо отслеживать использование цветного принтера для подготовки счетов за его использование.

– Необходимо следить, не пытается ли кто-либо изменить аппаратную конфигурацию компьютера.

– Необходимо вести учет действий, выполняемых администратором, чтобы отследить неавторизованные изменения.

– Необходимо вести учет процедур резервного копирования для предотвращения хищения данных.

– Необходимо отслеживать неавторизованный доступ к критически важным объектам Active Directory.

Ваши решения по аудиту перечисленных действий, успешных или неудачных попыток или обоих видов событий запишите в таблице.

Регистрируемое действие	Успех	Отказ
События входа в систему		
Управление учетными записями		
Доступ к службе каталогов		
Вход в систему		
Доступ к объектам		
Изменение системной политики		
Использование привилегий		

Отслеживание процесса		
Системные события		

Настройка политики аудита

1. Войдите в систему под любой учетной записью, входящей в группу Администраторы (Administrators).

2. Щелкните Пуск (Start), щелкните Выполнить (Run), в поле Открыть (Open) наберите mmc и щелкните ОК.

3. В окне Консоль 1 (Console 1), в меню Консоль (File), щелкните Добавить или удалить оснастку (Add/Remove Snap-In).

4. В окне Добавить или удалить оснастку (Add/Remove Snap-In) щелкните кнопку Добавить (Add),

5. В диалоговом окне Добавить изолированную оснастку (Add Standalone Snap-In) выберите в списке оснастку Групповая политика (Group Policy) и щелкните кнопку Добавить (Add).

6. Убедитесь, что в поле Объект групповой политики (Group Policy Object) окна Выбор объекта групповой политики (Select Group Policy Object) значится Локальный компьютер (Local Computer), затем щелкните кнопку Готово (Finish).

7. В диалоговом окне Добавить изолированную оснастку (Add Standalone Snap-In) щелкните Закрыть (Close).

Заметьте, что в окне Добавить/удалить оснастку (Add/Remove Snap-In) отображается элемент Политика «Локальный компьютер» (Local Computer Policy) несмотря на то, что вы выбрали оснастку Групповая политика (Group Policy). Дело в том, что для локального компьютера Групповая политика (Group Policy) означает то же самое, что и Политика «Локальный компьютер» (Local Computer Policy).

8. В окне Добавить/удалить оснастку (Add/Remove Snap-In) щелкните кнопку Закрыть (Close).

9. В дереве консоли дважды щелкните элемент Политика «Локальный компьютер» (Local Computer Policy).

10. Дважды щелкните элемент Конфигурация компьютера (Computer Configuration), затем дважды щелкните элемент Конфигурация Windows (Windows Settings).

11. Дважды щелкните элемент Параметры безопасности (Security Settings), затем дважды щелкните элементе Локальные политики (Local Policies).

12. Щелкните элемент Политика аудита (Audit Policy). В правой панели окна Политика «Локальный компьютер» (Local

Computer Policy) отобразятся текущие параметры политики аудита как показано на рис. 4.1.

13. Чтобы настроить политику аудита, в списке укажите Аудит входа в систему (Audit Logon Events) и в меню Действие (Action) щелкните пункт Свойства (Pro-perties), появится окно Свойства: аудит входа в систему (Audit Account Logon Events Properties), как показано на рис. 4.2. Или в правой части окна дважды щелкните каждый тип события и установите флажок Успех (Audit Successful Attempts) или Отказ (Audit Failed Attempts) согласно следующей таблице.

Регистрируемое действие	Успех	Отказ
События входа в систему		
Управление учетными записями	X	
Доступ к службе каталогов		
Вход в систему		X
Доступ к объектам	X	X
Изменение системной политики	X	
Использование привилегий	X	
Отслеживание процесса	X	X
Системные события		

14. Закройте консоль MMC и сохраните локальную групповую политику.

15. Перезапустите компьютер, чтобы изменения немедленно вступили в силу.

Команда gpupdate позволяет обновлять параметры как локальной групповой политики, так и политики для объектов Active Directory, включая параметры безопасности. Чтобы обновить параметры на локальном компьютере, войдите в режим командной строки, наберите gpupdate и нажмите Enter. Для получения более полного описания команды gpupdate в меню Пуск (Start) щелкните Справка и поддержка (Help And Support) и используйте поиск для нахождения строки gpupdate.

2. Настройка аудита объектов Windows XP Professional

Настройка аудита файлов

1. Войдите в систему с использованием любой учетной записи, входящей в группу Администраторы (Administrators).

2. С помощью Проводника (Windows Explorer) создайте папку с именем Audit в корне системного диска (например, C:\Audit).

3. В папке Audit создайте текстовый файл с именем AUDIT (например, C:\Audit\Audit).

4. Щелкните правой клавишей мыши на файле AUDIT и выберите Свойства (Properties).

5. В диалоговом окне Свойства (Properties) выберите вкладку Безопасность (Security) и щелкните кнопку Дополнительно (Advanced).

Если в диалоговом окне Свойства (Properties) нет вкладки Безопасность (Security), выясните, находятся ли выбранные файлы и папки в разделе, отформатированном как NTFS? Если компьютер не входит в домен, выключен ли простой общий доступ к файлам (Simple File Sharing)? Для выключения простого общего доступа к файлам щелкните Пуск (Start), щелкните правой кнопкой мыши Мой компьютер (My Computer), затем щелкните пункт меню Проводник (Explore). В меню Сервис (Tools) выберите пункт Свойства папки (Folder Options). На вкладке Вид (View) снимите флажок Использовать простой общий доступ к файлам (Рекомендуется) [Simple File Sharing (Recommended)] и щелкните ОК.

6. В диалоговом окне Дополнительные параметры безопасности для AUDIT выберите вкладку Аудит (Auditing).

7. Щелкните кнопку Добавить (Add).

8. В диалоговом окне Выбор: пользователь или группа (Select User Or Group), в поле Имя (Name), укажите Все (Everyone) и щелкните ОК.

9. В диалоговом окне Элемент аудита для Audit.txt (Audit Entry For Audit.txt) установите флажки Успех (Successful) и Отказ (Failed) для каждого из следующих событий:

- Создание файлов/Запись данных (Create Files/Write Data);
- Удаление (Delete);
- Смена разрешений (Change Permissions);
- Смена владельца (Take Ownership).

10. Щелкните ОК. Windows XP Professional отобразит группу Все (Everyone) в диалоговом окне Дополнительные параметры безопасности для audit.txt (Advanced Security Settings For).

11. Для подтверждения изменений щелкните кнопку ОК.

Настройка аудита принтера

1. Щелкните Пуск (Start), затем –Панель управления (Control Panel), далее щелкните категорию Принтеры и другое оборудование (Printers And Other Hardware) и значок Принтеры и факсы (Printers And Faxes).

2. В окне Принтеры (Printers) щелкните правой кнопкой мыши значок принтера HPColorLaserJet 4500 PS, затем щелкните пункт меню Свойства (Properties).

3. На вкладке Безопасность (Security) щелкните кнопку Дополнительно (Advanced).

4. В диалоговом окне Дополнительные параметры безопасности для HPColorLaserJet 4500 PS , на вкладке Аудит (Auditing), щелкните кнопку Добавить.

5. В диалоговом окне Выбор: пользователь или группа (Select User Or Group), в поле Имя (Name), укажите Все (Everyone) и щелкните ОК.

6. В диалоговом окне Элемент аудита для HPColorLaserJet 4500 PS (Auditing Entry For HP Color LaserJet 4500 PS) установите флажок Успех (Successful) для всех типов событий.

7. Щелкните ОК. Windows XP Professional отобразит группу Все (Everyone) в диалоговом окне Управление доступом для HPColorLaserJet 4500 PS(Access Control Settings For HP Color LaserJet 4500 PS).

8. Для подтверждения изменений щелкните ОК.

9. Закройте окно Свойства HPColorLaserJet 4500 PS (HP Color LaserJet 4500 PS Properties), щелкнув ОК.

10. Закройте окно Принтеры и факсы (Printers And Faxes).

Проверка правильности параметров политики аудита для файла AUDIT

1. Щелкните Пуск (Start), Панель управления (Control Panel), затем –Учетные записи пользователей (User Accounts).

2. Убедитесь, что учетная запись User2 существует и является ограниченной (Limited).

3. Создайте пароль User2 для учетной записи User2.

4. Закройте все окна и выйдите из системы.

5. Зарегистрируйтесь в системе под именем User2, используя пароль.

6. Откройте Проводник (Windows Explorer), затем откройте файл C:\Audit\Audit. В открывшемся окне программы Блокнот (Notepad) появится пустой файл AUDIT.

7. Введите следующий текст: «Этот файл изменен пользо-

вателем User2».

8. Попытайтесь сохранить файл. Удалось ли вам сохранить файл? Почему?

9. Закройте файл, не сохраняя его, и завершите работу с системой.

3. Управление журналом безопасности

Просмотр журнала безопасности компьютера и отбора событий

1. Войдите в систему под любой учетной записью, входящей в группу Администраторы (Administrators).

2. Щелкните Пуск (Start), Панель управления (Control Panel), категорию Производительность и обслуживание (Performance And Maintenance) и Администрирование (Administrative Tools), затем дважды щелкните ярлык Просмотр событий (Event Viewer).

3. В дереве консоли щелкните приложение (Application Log) и просмотрите его содержимое. Просмотрите описание нескольких событий, дважды щелкнув соответствующие записи.

4. В дереве консоли щелкните система (System Log) и просмотрите его содержимое. Просмотрите описание нескольких событий, дважды щелкнув каждую их соответствующих записей.

Успешные попытки условно обозначены значком ключа, а неудачные –значком замка. Кроме того, указаны дата и время события, категория события и пользователь, действие которого вызвало данное событие. В колонке Категория (Category) отображается тип события, например доступ к объекту, управление учетными записями, доступ к службе каталогов или попытки регистрации в системе. Типы регистрируемых событий представлены в таблице 4.8.

Чтобы просмотреть дополнительную информацию о любом событии, щелкните название события и в меню Действие (Action) щелкните пункт Свойства (Properties).

5. В дереве консоли щелкните безопасность (Security Log) и просмотрите его содержимое. Просмотрите описания всех событий категории Отказ (Failure), дважды щелкая соответствующие записи, пока не найдете попытку доступа пользователя User2 к файлу C:\Audit\Audit.

6. В меню Вид (View) выберите пункт Фильтр (Filter).

7. В диалоговом окне Свойства: Безопасность (Security Properties), в поле Пользователь (User), введите User2 и щелкните ОК. Применение фильтра уменьшит число событий, которые

придется просмотреть, чтобы найти нужное.

8. Дважды щелкните каждое из событий. Обратите внимание, что все они относятся к пользователю User2.

Настройка размера и содержимого файла журнала

1. В дереве консоли выберите элемент Система (System).

2. В меню Действие (Action) щелкните пункт Свойства (Properties).

3. В диалоговом окне свойств журнала выберите Затирать старые события по необходимости (Overwrite Events As Needed).

4. В поле Максимальный размер журнала (Maximum Log Size) измените максимальный размер журнала на 2048 кбайт и щелкните ОК. Теперь Windows XP Professional будет заполнять журнал, пока его объем не достигнет 2048 кбайт, а затем начнет затирать старые события по мере необходимости.

5. Закройте окно Просмотр событий (Event Viewer) и окно Администрирование (Administrative Tools).

Таблица 4.8

Типы регистрируемых событий

Идентификатор	Категория	Описание
512	Системное событие	Перезагрузка операционной системы
513	Системное событие	Завершение работы операционной системы (shutdown)
514	Системное событие	Загрузка пакета аутентификации
515	Системное событие	Запуск процесса аутентификации (в стандартной конфигурации WinLogon.exe)
516	Системное событие	Сбой при ретистрации одного или нескольких событий аудита1
517	Системное событие	Очистка журнала аудита
518/528	Вход/выход пользователя системы	Загрузка пакета оповещения об изменениях в списке пользователей Пользователь успешно вошел в систему

529	Вход/выход пользователя из системы	Вход пользователя в систему запрещен -имя или пароль, введенные при входе в систему, некорректны
530	Вход/выход пользователя из системы	Вход пользователя в домен в данное время запрещен
531	Вход/выход пользователя из системы	Вход пользователя в систему запрещен - учетная запись пользователя заблокирована администратором
532	Вход/выход пользователя из системы	Вход пользователя в Домен запрещен - учетная запись пользователя автоматически заблокирована по достижении определенной даты
533	Вход/выход пользователя из системы	Вход пользователя в домен с данной рабочей станции запрещен
534	Вход/выход пользователя из системы	Данный тип (интерактивный, сетевой или сервисный) входа пользователя в систему запрещен
535	Вход/выход пользователя из системы	Вход пользователя в систему запрещен - пароль пользователя устарел
536	Вход/выход пользователя из системы	Пользователь не смог войти в домен из-за сбоев сетевых сервисов
537	Вход/выход пользователя из системы	Пользователь не смог войти в систему по какой-то другой причине
538	Вход/выход пользователя из системы	Пользователь успешно вышел из системы

539	Вход/выход пользователя из системы	Вход пользователя в систему запрещен - учетная запись пользователя автоматически заблокирована из-за превышения максимально допустимого количества попыток входа в систему с неверным паролем
560	Доступ к объекту	Пользователь попытался открыть объект
561	Доступ к объекту	Пользователь закрыл объект
576	Использование опасных привилегий	В маркере доступа пользователя присутствует опасная привилегия
577	Использование опасных привилегий	Предпринята попытка использования опасной привилегии при выполнении операции, не связанной с доступом к объектам
578	Использование опасных привилегий	Предпринята попытка использования опасной привилегии для получения доступа к объекту
592	Запуск/завершение процессов	Запуск нового процесса
593	Запуск/завершение процессов	Завершение процесса
594	Запуск/завершение процессов	Дублирование дескриптора (handle) объекта
595	Запуск/завершение процессов	Непрямой доступ к объекту
608	Изменения в политике безопасности	Субъекту предоставлена новая привилегия

609	Изменения в политике безопасности	У субъекта отнята привилегия
610	Изменения в политике безопасности	Установлены доверительные отношения с другим доменом
611	Изменения в политике безопасности	Доверительные отношения с другим доменом прекращены
612	Изменения в политике безопасности	Изменена политика аудита
624	Изменения в списке пользователей	Создана учетная запись нового пользователя
625	Изменения в списке пользователей	Изменен тип учетной записи
626	Изменения в списке пользователей	С учетной записи пользователя снята блокировка
627	Изменения в списке пользователей	Неудачная попытка изменить пароль пользователя
628	Изменения в списке пользователей	Удачная попытка изменить пароль пользователя
629	Изменения в списке пользователей	Учетная запись пользователя заблокирована
630	Изменения в списке пользователей	Учетная запись пользователя удалена
631	Изменения в списке пользователей	Создана новая глобальная группа
632	Изменения в списке пользователей	Пользователь добавлен в глобальную группу
633	Изменения в списке пользователей	Пользователь удален из глобальной группы

634	Изменения в списке пользователей	Глобальная группа удалена
635	Изменения в списке пользователей	Создана новая локальная группа
636	Изменения в списке пользователей	Пользователь добавлен в локальную группу
637	Изменения в списке пользователей	Пользователь удален из локальной группы
638	Изменения в списке пользователей	Локальная группа удалена
639	Изменения в списке пользователей	Произведены изменения в учетной записи локальной группы, не связанные с изменением членства пользователей в этой группе
640	Изменения в списке пользователей	Произведены изменения в списке пользователей, не связанные с редактированием учетных записей
641		Произведены изменения в учетной записи глобальной группы, не связанные с изменением членства пользователей в этой группе
642		Произведены изменения в учетной записи пользователя, не связанные с изменением типа учетной записи, пароля пользователя и членства пользователя в группах

Указания по выполнению отчета

Отчет должен содержать:

– название работы;
– цель работы;
– порядок действий по выполнению лабораторной работы;
– выводы по результатам проделанной работы.

Контрольные вопросы

1. Какие три журнала Windows XP Professional можно просматривать средствами утилиты просмотра событий? Для чего предназначен каждый из них?
2. Как просмотреть журнал безопасности удаленного компьютера?
3. Какие два способа поиска конкретных событий есть в утилите просмотра событий? Что позволяет делать каждая из команд?
4. Размер любого из журналов может изменяться от_____кбайт до_____Гбайт, а по умолчанию он равен_____кбайт. Что происходит при переполнении журнала, если для него выбран параметр Не затирать события (очистка журнала вручную) (Do Not Overwrite Events)?

ЛАБОРАТОРНАЯ РАБОТА № 5 ИСПОЛЬЗОВАНИЕ ПРОГРАММНЫХ СРЕДСТВ КОНТРОЛЯ И АНАЛИЗА ВЫПОЛНЕНИЯ ПОЛИТИКИ БЕЗОПАСНОСТИ НА ПРИМЕРЕ ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS XP

Цель работы: освоение системных программ Windows XP, программ из комплекта Windows NT Resource Kit и других программных средств, предназначенных для:

– просмотра и управления разрешениями на доступ к конфиденциальным объектам компьютерной системы;

– просмотра и анализа записей аудита;

– анализа соответствия реализуемой в компьютерной системе политики безопасности требованиям стандартов безопасности;

– дополнительной защиты базы учетных записей пользователей компьютерной системы и используемых ими рабочих станций.

Подготовка к выполнению работы:

Подготовить для включения в отчет о лабораторной работе определения понятий:

– матрица доступа;

– дискреционный список контроля доступа;

– домен безопасности;

– журнал (файл) аудита;

– запись журнала аудита;

– стандарт безопасности.

Подготовить для включения в отчет о лабораторной работе ответы на следующие вопросы:

1. Кто управляет дискреционным списком контроля доступа к объектам в операционной системе Windows XP?
2. Как должны использоваться записи журнала аудита событий безопасности?
3. Какие права доступа к файлу аудита имеет по умолчанию администратор системы?
4. Что такое консольное приложение Windows?

Порядок выполнения работы:

1. После собеседования с преподавателем и получения до-

пуска к работе войти в систему с указанным общим именем учетной записи (с правами администратора).

2. Освоить использование системной программы по управлению списками контроля доступа (CACLS):

– начать сеанс работы в режиме командной строки Windows XP (Пуск | Программы | Стандартные | Командная строка);

– в строке приглашения ввести название программы, ознакомиться с ее назначением и параметрами и сохранить данную информацию в отчете о лабораторной работе (через буфер обмена с помощью команд подменю «Изменить» системного меню окна командной строки);

– перейти (с помощью команды cd \Учебные материалы) в папку «Учебные материалы» и с помощью программы cacls получить и сохранить в файле в своей индивидуальной папке разрешения на доступ к папке «КЗИ2000», введя следующую команду

– cacls КЗИ2000 >*имя файла*

– (для переключения раскладок клавиатуры в режиме командной строки использовать комбинации клавиш Alt+правый Shift и Alt+левый Shift);

– просмотреть созданный файл с помощью Internet Explorer и включить его содержимое в отчет о лабораторной работе, снабдив необходимыми комментариями (с учетом сведений, приведенных в приложении);

– повторить два предыдущих пункта для своей индивидуальной папки;

– перейти в свою индивидуальную папку (с помощью команды командной строки cd) и с помощью одного вызова программы cacls запретить доступ группе «Пользователи» ко всем файлам и вложенным папкам своей индивидуальной папки;

– проверить результаты выполнения предыдущего пункта с помощью команды «Свойства» контекстного меню своей индивидуальной папки и включить в отчет о лабораторной работе текст вызова программы cacls и ответ на вопрос, почему доступ Вам к файлам своей папки теперь недоступен;

– разрешить доступ по чтению группе «Пользователи» к файлам и вложенным папкам своей индивидуальной папки с помощью одного вызова программы cacls, проверить результаты и включить в отчет о лабораторной работе текст вызова программы cacls;

– завершить (с помощью команды exit) сеанс работы в режиме командной строки и включить в отчет о лабораторной работе ответ на вопрос, в чем преимущество использования програм-

мы cacls перед назначением разрешений на доступ к объектам при помощи Проводника Windows.

3. Ознакомиться с возможностями программ управления и анализа разрешений на доступ к объектам компьютерных систем на основе Windows XP:

– начать работу с программой просмотра разрешений на доступ к объектам и параметров политики безопасности DumpACL, размещенной в папке TEMP \ DumpACL на диске c;

– ознакомиться с порядком настройки параметров отчета о результатах анализа разрешений (команда меню Report | Permissions Report Options) и включить эти сведения в отчет о лабораторной работе;

– с помощью команды меню Report | Dump Permissions for File System получить и включить в отчет сведения о результатах анализа разрешений на доступ к папке «КЗИ2000» и своей индивидуальной папке, а также ответ на вопрос, в чем разница между данными результатами и сведениями, полученными при помощи команды cacls;

– с помощью других команд меню Report получить и включить в отчет результаты анализа разрешений на доступ к реестру Windows (только раздел HKEY_CURRENT_USER) и принтеру;

– ознакомиться и включить в отчет о лабораторной работе сведения о порядке получения и содержании информации о зарегистрированных пользователях и группах (команды Dump… меню Report);

– включить в отчет о лабораторной работе сведения о назначении и результатах применения команд Dump Policies и Dump Rights меню Report;

– включить в отчет о лабораторной работе копии экранных форм, используемых программой DumpACL, и завершить работу с этой программой;

– начать работу с программой управления разрешениями на доступ к объектам FileAdmin из группы Administrator Assistant меню Пуск | Программы;

– получить с помощью данной программы разрешения на доступ к папке «КЗИ2000» и своей индивидуальной папке и включить их в отчет;

– с помощью программы FileAdmin оставить полный доступ к своей индивидуальной папке, вложенным в нее папкам и файлам только самому себе (своей индивидуальной учетной записи) и пользователю User (учесть при этом действие переключателей “Propagate Through Entire Tree?”), а всем остальным пользовате-

лям и группам – доступ только для чтения;

– с помощью программы FileAdmin (кнопка Clone) распространить виды доступа к своей индивидуальной папке, установленные для группы «Пользователи», на группу «Опытные пользователи»;

– изучить назначение кнопки Options программы FileAdmin (определение настроек и просмотр журнала изменений прав доступа к объектам);

– включить в отчет о лабораторной работе копии экранных форм, используемых программой FileAdmin, и завершить работу с этой программой;

– начать работу с программой управления разрешениями на доступ к реестру Windows RegAdmin из группы Administrator Assistant меню Пуск | Программы;

– с помощью программы RegAdmin получить и включить в отчет о лабораторной работе сведения о разрешениях на доступ к разделам реестра HKEY_LOCAL_MACHINE и HKEY_CURRENT_USER, а также ответ на вопрос, как изменить права доступа к разделам реестра Windows с помощью программы RegAdmin;

– включить в отчет о лабораторной работе копии экранных форм, используемых программой RegAdmin, и завершить работу с этой программой;

– начать работу с программой управления и анализа разрешений на доступ к объектам Security Explorer из группы Administrative Tools (Common) меню Пуск | Программы;

– с помощью программы Security Explorer (команда меню Tools | Show permissions) просмотреть и включить в отчет о лабораторной работе разрешения на доступ к папке «КЗИ2000» и к своей индивидуальной папке, а также ответ на вопрос, какая дополнительная информация о дискреционных списках контроля доступа выводится программой Security Explorer;

– изучить и включить в отчет сведения о назначении кнопок диалогового окна Directory Permissions программы Security Explorer (Modify, Grant Permissions и т.д.), а также ответ на вопрос, возможно ли «клонирование» прав доступа к объекту в программе Security Explorer;

– с помощью команды меню Tools | Search for Permissions программы Security Explorer получить, сохранить в файле в своей индивидуальной папке и включить в отчет о лабораторной работе сведения о папках диска с, к которым имеет доступ (в том числе полный) группы «Пользователи» и «Все»;

– изучить и отразить в отчете о лабораторной работе сред-

ства вызова функций программы Security Explorer с помощью контекстного меню Проводника Windows;

– включить в отчет о лабораторной работе копии экранных форм, используемых программой Security Explorer, и завершить работу с этой программой;

– начать работу с программой управления разрешениями на доступ к объектам Security Manager из группы Admin Tools меню Пуск | Программы;

– получить с помощью программы Security Manager и включить в отчет о лабораторной работе разрешения на доступ к папке «КЗИ2000» и своей индивидуальной папке (для сохранения отчета программы можно воспользоваться командой ее меню File | Save Report);

– выделить в левой части окна программы Security Manager имя своей индивидуальной папки и на ее примере изучить и включить в отчет о лабораторной работе команды контекстного меню и связанные с ними функции этой программы по управлению разрешениями на доступ к объектам (особо обратить внимание на команду Replace Owner и включить в отчет о лабораторной работе ответ на вопрос, в чем потенциальная опасность применения этой возможности);

– включить в отчет о лабораторной работе копии экранных форм, используемых программой Security Manager, и завершить работу с этой программой;

– начать работу с программой управления разрешениями на доступ к объектам компьютерной системы предприятия Virtuosity (с помощью меню Пуск | Программы);

– с помощью программы Virtuosity получить и отразить в отчете разрешения на доступ к папке «КЗИ2000» и своей индивидуальной папке;

– с помощью Справки программы Virtuosity изучить и включить в отчет о лабораторной работе сведения о назначении команд меню Actions | Save into Database и Actions | Apply from Database;

– включить в отчет о лабораторной работе копии экранных форм, используемых программой Virtuosity, и завершить работу с этой программой.

4. Ознакомиться с возможностями программ анализа выбранной для компьютерной системы политики безопасности и ее соответствия требованиям стандартов в области информационной безопасности:

– начать работу с программой проверки соответствия

настроек Windows XP требованиям класса C2 TCSEC (программа c2config из комплекта Windows NT Resource Kit) с помощью команды «Выполнить» меню «Пуск»;

– ознакомиться с результатами анализа политики безопасности, полученными с помощью программы c2config, сохранить их в отчете о лабораторной работе и снабдить необходимыми комментариями, раскрывающими сущность того или иного анализируемого параметра (наиболее подробно для тех параметров, значения которых не соответствуют требованиям класса безопасности C2);

– включить в отчет сведения о смысле изображений рядом с анализируемым параметром политики безопасности в окне программы c2config (при необходимости можно воспользоваться разделом List Box Display Справки данной программы;

– включить в отчет о лабораторной работе копии экранных форм, используемых программой c2config, и завершить работу с этой программой;

– начать работу с демонстрационной версией программы анализа безопасности компьютерных систем и сетей Kane Security Analyst из группы Kane Security Analyst for NT меню Пуск | Программы;

– с помощью кнопок главного окна программы Kane Security Analyst изучить и включить в отчет ее основные функции (анализ политики учетных записей, выбираемых пользователями паролей, политики аудита, прав доступа к файлам и папкам, прав доступа к реестру, соответствия требованиям класса C2, рисков при использовании данной политики безопасности и др.);

– включить в отчет о лабораторной работе копии экранных форм, используемых программой Kane Security Analyst, и завершить работу с этой программой.

5. Изучить средства эффективного анализа журнала аудита событий безопасности:

– начать работу с системной программой Просмотр событий (Панель управления | Администрирование) и открыть журнал аудита событий безопасности;

– с помощью команды «Фильтр» меню «Вид» изучить и отразить в отчете о лабораторной работе средства отбора необходимых для анализа записей (критерии отбора, переход от просмотра отобранных записей к просмотру всего журнала и наоборот, изменение порядка сортировки записей, поиск нужных записей, изменение вида отображения записей);

– с помощью команд меню «Действие» изучить и отразить в

отчете средства сохранения и восстановления журнала аудита (сохранить журнал аудита событий безопасности в виде текстового файла в своей индивидуальной папке);

– включить в отчет о лабораторной работе копии экранных форм, использованных при выполнении данного пункта, и завершить работу с системной программой Просмотр событий;

– запустить в режиме командной строки программу dumpel из комплекта Windows NT Resource Kit с параметром -?, включить в отчет сведения о параметрах этой программы работы с журналами аудита;

– с помощью программы dumpel сохранить в текстовом файле в своей индивидуальной папке выбранные записи системного журнала аудита, введя следующую строку: dumpel –l system –f *имя файла* –e 6005 –e 6006 –e 6009 –m EventLog.

Включить в отчет фрагмент созданного таким образом файла и ответ на вопрос, какая дополнительная по сравнению с системной программой Просмотр событий возможность существует у программы dumpel;

– завершить работу в режиме командной строки.

6. Ознакомиться с возможностями системной программы дополнительной защиты базы учетных записей с помощью ее шифрования:

– начать работу с программой syskey с помощью команды «Выполнить» меню «Пуск»;

– нажать кнопку «Обновить», ознакомиться и отразить в отчете варианты генерации системного ключа шифрования базы учетных записей, нажать кнопку «Отмена» (дважды);

– включить в отчет о лабораторной работе ответ на вопрос, какие достоинства и недостатки есть у каждого из предлагаемых программой syskey вариантов генерации криптографического ключа.

7. Ознакомиться с возможностями дополнительного хранителя экрана из комплекта Windows NT Resource Kit, осуществляющего принудительный выход из системы по истечении заданного периода времени:

– скопировать файл winexit.scr из папки C:\Disrtrib\Resource Kit 2\COMMON\COMMON в папку C:\WINDOWS\system32 (если это еще не сделано);

– с помощью команды «Свойства» контекстного меню Рабочего стола (закладка «Заставка») установить и настроить (кнопка «Параметры») хранитель экрана Logoff Screen Saver;

– закрыть окно свойств экрана и проверить работу установ-

ленного хранителя экрана;

– включить в отчет о лабораторной работе сведения о параметрах и порядке использования дополнительного хранителя экрана, а также копии экранных форм, использованных при выполнении данного пункта.

8. Включить в отчет о лабораторной работе ответы на контрольные вопросы:

– почему компьютерные системы на основе Windows XP не могут быть сертифицированы по классу безопасности TCSEC выше, чем C2?

– какой класс защищенности автоматизированных систем в соответствии с требованиями руководящих документов Гостехкомиссии РФ соответствует, на Ваш взгляд, классу C2 TCSEC?

– почему многие из рассмотренных в настоящей лабораторной работе программ работают в режиме командной строки?

– какая из рассмотренных в данной лабораторной работе программ управления разрешениями на доступ к объектам кажется Вам наиболее удобной и почему?

– составьте строку вызова системной программы cacls для того, чтобы обеспечить доступ по чтению ко всем файлам и папкам папки c:\students для всех членов группы «Преподаватели»;

– в чем преимущества, на Ваш взгляд, дополнительного хранителя экрана winexit.scr перед стандартными хранителями экрана?

– какие угрозы безопасности и каналы утечки конфиденциальной информации может устранить программа syskey?

– какая из рассмотренных в данной лабораторной работе программ управления разрешениями на доступ к объектам имеет небезопасную функцию и как могут быть нейтрализованы последствия ее несанкционированного применения?

9. Подготовить отчет о выполнение лабораторной работы, который должен включать в себя:

– титульный лист с названиями университета, факультета, кафедры, учебной дисциплины и лабораторной работы, фамилиями и инициалами студента (студентов) и преподавателя, города и года выполнения работы;

– содержание отчета с постраничной разметкой;

– ответы на вопросы, данные в ходе подготовки к выполнению работы;

– сведения о выполнении работы по пунктам с включением содержания задания, копий экранных форм и ответов на вопросы; ответы на контрольные вопросы.

Порядок защиты лабораторной работы:

1. К защите лабораторной работы допускаются студенты, выполнившие ее в компьютерном классе, предъявившие результаты своей работы преподавателю и подготовившие отчет о выполнении лабораторной работы, содержание которого соответствует п. 9 порядка выполнения работы;

2. На защите студенты предъявляют отчет о выполнении лабораторной работы, дают пояснения по деталям выполнения задания и отвечают на вопросы преподавателя.

3. По результатам защиты каждому студенту выставляется дифференцированная оценка, учитываемая в при определении его итогового рейтинга за семестр.

4. В случае неудовлетворительной оценки по результатам защиты лабораторной работы или пропуска соответствующего занятия студент должен защитить работу повторно в другой день.

Приложение

Стандартные типы доступа к объектам в операционной системе Windows XP

– SINCHRONIZE – использовать объект для синхронизации;

– WRITE_OWNER – изменить владельца объекта;

– WRITE_DAC – изменить дискреционный список контроля доступа к объекту;

– READ_CONTROL – прочитать данные из дискреционного списка контроля доступа;

– DELETE – удалить объект.

Специальные права доступа к объектам

– READ_DATA – прочитать данные из объекта;

– WRITE_DATA – записать данные в объект;

– APPEND_DATA – добавить данные в объект;

– READ_ATTRIBUTES – прочитать атрибуты объекта;

– WRITE_ATTRIBUTES – записать атрибуты объекта;

– READ_EA – прочитать расширенные атрибуты объекта;

– WRITE_EA – записать расширенные атрибуты объекта;

– EXECUTE – выполнить программный файл.

Родовые права доступа к объектам

• GENERIC_READ - READ_CONTROL, READ_DATA, READ_ATTRIBUTES, READ_EA, SINCHRONIZE;

• GENERIC_WRITE - READ_CONTROL, WRITE_DATA, WRITE_ATTRIBUTES, WRITE_EA, APPEND_DATA, SINCHRONIZE;

• GENERIC_EXECUTE - READ_CONTROL, READ_ATTRIBUTES, EXECUTE, SINCHRONIZE.

ЛАБОРАТОРНАЯ РАБОТА 6
УСТАНОВКА И НАСТРОЙКА ВИРТУАЛЬНОЙ МАШИНЫ VIRTUALBOX

Цель работы: научиться устанавливать и настраивать виртуальные машины.

Краткие теоретические сведения

Технология создания виртуальной машины не слишком сложна, но включает в себя несколько этапов. В первую очередь, на компьютер устанавливается непосредственно само приложение ВМ. Далее создается виртуальный компьютер (виртуальная машина), на который и устанавливается нужная операционная система. В общем случае, *алгоритм работы с виртуальной машиной на компьютере* можно обозначить следующим образом:

– выбрать тип устанавливаемой операционной системы;

– установить объем ОЗУ, отводимый для виртуальной машины;

– указать размер жесткого диска виртуальной машины;

– добавить или удалить периферийные устройства (например, USB порты, звук);

– запустить созданную виртуальную машину;

– установить требуемую ОС в запущенной виртуальной машине.

Приведем алгоритмы создания и настройки ВМ на примере приложения ВМ ***Qemu*** (примеры работы с другими приложениями ВМ будут приведены в заданиях лабораторной работы).

Создание ВМ:

1. Запустить **Мастер создания новых виртуальных машин** , щелкнув по кнопке ***Create new Virtual Machine (Создать новую Виртуальную Машину)*** .
2. Ввести *имя* создаваемой виртуальной машины в поле ***New Virtual Machine Name (Новая ВМ)***.
3. Установить *тип операционной системы* в раскрывающемся списке ***Operating System (Операционная система)***.
4. Указать *объем оперативной памяти*, используемой ВМ (в мегабайтах) в поле ***Virtual Machine RAM (ОЗУ виртуальной машины)***.
5. Создать жесткий диск ВМ ***Create New Virtual Drive (Создать новый виртуальный диск)*** и указать его *параметры*: *каталог* для размещения жесткого диска; *размер жесткого диска* -

Drive Size (Размер жесткого диска).

6. Завершить создание виртуальной машины ***Save Virtual Machine (Сохранить ВМ)***.

Настройка ВМ:

1. Выделить виртуальную машину в списке ВМ.
2. Открыть *диалоговое окно свойств ВМ* кнопкой ***Configure Selected Virtual Machine (Конфигурирование выбранной ВМ)***.
3. На вкладке **General (Главная)** расположены общие параметры ВМ: ***RAM Installed (Объем установленной оперативной памяти); Enable USB Support (Поддержка USB); Sound (Звук)***.
4. На вкладке **Disk Configuration (Конфигурация дисков)** расположены параметры, относящиеся к дискам: ***Hard Disk Drives (Жесткие диски); CD-ROM Drives (Приводы CD-ROM); Boot from CD-ROM (Загрузка с CD-ROM); Use system CD-ROM Drive (Использование системного оптического привода)***.
5. На вкладке **Network (Сеть)** расположены параметры, относящиеся к сетевым возможностям ВМ: ***Network (Сетевые адаптеры используемые в ВМ)***.

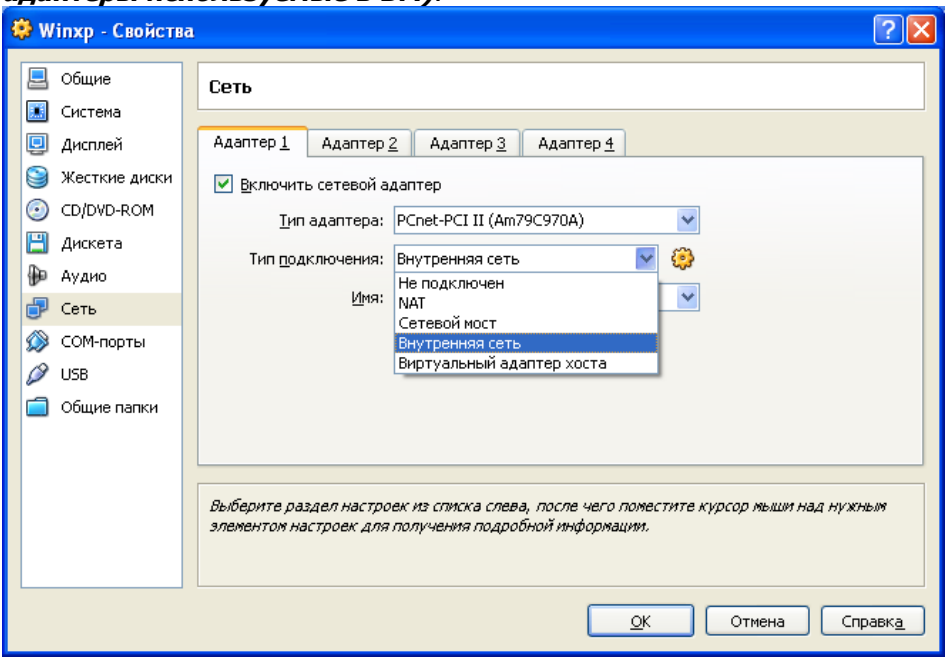

Рис.1.

Настройка сети

Для каждой виртуальной машины может быть настроено до четырех интерфейсов. Они могут работать в разных режимах. Режим выбирается из следующих вариантов:

1. Не подключен.
2. NAT.
3. Сетевой мост.
4. Внутренняя сеть.
5. Виртуальный адаптер хоста.

Режим NAT идеально подходит для того, чтобы дать гостевой ОС выход в Интернет. Однако отсутствие IP-адреса сводит на нет полезность этого режима.

В режиме Сетевой мост гостевой компьютер становится частью реальной сети и со стороны отличить, какой компьютер реальный, а какой виртуальный практически невозможно. DHCP-сервер реальной сети выдаст виртуальному компьютеру IP-адрес.

Режим Виртуальная сеть подходит для создания виртуальной сети в которую включены все виртуальные компьютеры, установленные на одном реальном компьютере, без включения его в эту сеть.

Режим Виртуальная сеть хоста позволит включить в эту сеть реальный компьютер.

6. На вкладке **Advanced (Дополнительно)** расположены дополнительные параметры ВМ: ***Machine Type (Тип аппаратной платформы)***.

В лабораторной работе будут использоваться установочные образы компакт дисков с различными операционными системами.

Образ диска – точная копия носителя информации, которая хранится в отдельном файле. Образы дисков позволяют хранить, например, содержимое оптических дисков на жестких дисках компьютера. Образ диска всегда можно записать на носитель информации или подключить к программе, которая умеет работать с образами дисков.

Порядок выполнения работы

Задание 1. Создайте виртуальную машину для операционной системы Windows 98.

1. Запустите приложение ***VirtualBox***.
2. Изучите *интерфейс приложения ВМ*: назначение кнопок и вкладок правой панели приложения.
3. Запустите **Мастер создания виртуальных машин** (кнопка ***Создать***).

4. Ознакомьтесь с информацией **Мастера** и перейдите к следующему шагу (***Далее***).

5. В окне **Имя машины и тип ОС** укажите:

- в поле **Имя**: *VM-1*
- в списке **тип ОС**: *Windows98*
- проверьте и перейдите в следующее окно кнопкой ***Далее***.

6. Укажите **объем основной памяти,** выделяемой ВМ – *64 Мбайта* и перейдите к следующему шагу с помощью кнопки ***Далее***.

7. В окне **Виртуальный жесткий диск** запустите **Мастер создания нового виртуального жесткого диска**, который будет системным для ВМ (кнопка ***Создать***). В окнах **Мастера**:

- ознакомьтесь с информацией **Мастера** и перейдите к следующему шагу с помощью кнопки ***Далее***;
- выберите **тип образа** создаваемого жесткого диска – *Динамически расширяющийся образ* и перейдите к следующему шагу (***Далее***);
- укажите **местоположение** и **размер** виртуального диска: в списке **Имя файла образа**: *c:|VirtualM| имя ВМ*; в группе **Размер образа**: *7 GB*; перейдите к следующему шагу (***Далее***);
- в окне **Итог** проверьте правильность установленных параметров создаваемого жесткого диска виртуальной машины и завершите его создание кнопкой ***Готово***. *Виртуальный жесткий диск ВМ будет храниться в файле с указанным вами именем и расширением имени* ***.vdi****. Автоматически произойдет возврат в окно* ***Виртуальный жесткий диск Мастера создания ВМ****, где в списке* ***Загрузочный жесткий диск (первичный мастер)*** *появится запись о созданном вами жестком диске и его местоположении. Продолжите создание ВМ нажав кнопку* ***Далее****.*

8. В окне **Итог Мастера создания новой ВМ**, проверив информацию о создаваемой ВМ, завершите создание виртуальной машины кнопкой ***Готово***. *После закрытия окна* ***Мастера****, произойдет автоматический возврат в приложение ВМ, на левой панели которого в списке виртуальных машин появится запись о созданной ВМ и отметкой о ее состоянии (выключена).*

Задание 2. Создайте виртуальную машину для ОС OpenSUSE Linux.

1. Запустите приложение ***BM VirtualBox***.

2. Запустите **Мастер создания виртуальных машин** (кнопка ***Создать***):

- ознакомьтесь с информацией **Мастера** и перейдите к сле-

дующему шагу с помощью кнопки ***Далее***.

3. Установите *имя виртуальной машины* и укажите *тип операционной системы*:

– введите в поле **Имя** – *VM-2*;

– введите в поле **Тип ОС** – *Linux 2.6*;

– подтвердите введенные параметры кнопкой ***Далее***.

4. Установите **объем оперативной памяти**, которая будет использоваться ВМ, – *256 Мбайт* и перейдите к следующему шагу с помощью кнопки ***Далее***.

5. Создайте **жесткий диск** для виртуальной машины:

– запустите **Мастер создания нового виртуального диска** кнопкой ***Создать***;

– ознакомьтесь с информацией **Мастера** и перейдите к следующему шагу с помощью кнопки ***Далее***.;

– укажите **Тип образа виртуального диска** – *Динамически расширяющийся образ* и и перейдите к следующему шагу с помощью кнопки ***Далее***.;

– укажите **размер** и **местоположение** виртуального диска:

– введите в поле **Имя файла образа** - *OpenSUSE*;

– установите **размер жесткого диска** - *3,50 Гбайт*;

– подтвердите введенные параметры кнопкой ***Далее***;

– закройте диалоговое окно **Мастера создания жестких дисков** кнопкой ***Готово***;

– завершите создание жесткого диска кнопкой ***Далее***.

6. Завершите создание виртуальной машины кнопкой ***Готово***.

7. Подключите к созданной виртуальной машине загрузочный образ операционной системы ***OpenSUSE***:

– откройте ***Менеджер виртуальных дисков (Файл/Менеджер виртуальных дисков)*** ;

– активизируйте вкладку **Образы CD/DVD**;

– откройте диалоговое окно добавления образов кнопкой ***Добавить***;

– перейдите в каталог с образами установочных дисков;

– выберите файл ***opensuse.iso*** (кнопка ***Открыть***);

– закройте диалоговое окно **Менеджера виртуальных дисков** кнопкой ***ОК***;

– активизируйте виртуальную ***OpenSUSe*** машину в списке виртуальных машин;

– откройте окно *свойств виртуальной машины* ***(Ма-***

шина/Свойства).

– активизируйте пункт CD/DVD-ROM;

– установите флажок *Подключить CD/DVD*;

– установите радиокнопку *Файл ISO-образа* и выделите в раскрывающемся списке ***OpenSUSE.iso***;

– завершите подключение виртуального диска кнопкой ***ОК***.

8. Сделайте снимок созданной ВМ и сохраните его в личном каталоге.

Задание 3. Измените конфигурацию созданной ранее виртуальной машины Windows 98.

1. Запустите приложение ***ВМ VirtualBox***.
2. Активизируйте в списке виртуальных машин ***VM-1***.
3. Откройте окно **Свойства** (кнопка ***Свойства***) и познакомьтесь со списком устройств, которые могут быть подключены к ВМ.
4. Подключите к ВМ образ установочного диска:

– в списке устройств левой части окна **Свойства** выберите *CD/DVD-ROM*;

– в правой части окна:

– установите флажок *Подключить CD/DVD*

– включите радиокнопку *Файл ISO-образа*

– укажите месторасположение файла образа установочного диска ОС.

5. Подключите к виртуальной машине сетевой адаптер:

– в списке устройств левой части окна **Свойства** выберите *Сеть*;

– в правой части окна: установите флажок *Включить сетевой адаптер*; добавьте сетевой адптер кнопкой ***Добавить***  в разделе *Хост-интерфейсы*; введите имя добавляемого интерфейса, например *VirtualBox 1*; *Следует дождаться окончания установки оборудования;* выберите в списке **Подключен к** - *Хост-интерфейс*.

6. Закройте окно **Свойства** кнопкой **ОК**.

Контрольные вопросы

1. Виртуализация – это:

– общий термин, охватывающий абстракцию всех ресурсов;

– общий термин, охватывающий абстракцию аппаратных ресурсов;

– общий термин, охватывающий абстракцию программных

ресурсов.

2. Вычислительная среда, набор ресурсов и правил работы, которой формируется в некой другой вычислительной среде – это:

- виртуальная машина;
- консоль виртуальных машин;
- эмулятор;
- монитор виртуальных машин;

3. Тип виртуальной машины (ВМ), размещаемый между операционной системой и аппаратным обеспечением?

4. Метод или процесс, заключающийся в имитации функционирования одной системы или ее части средствами другой системы без потери функциональных возможностей?

5. Соответствие комбинаций клавиш, действиям в приложении ВМ VirtualBox:

- RCTRL – осуществить сброс;
- RCTRL+DEL – переслать ВМ сигнал нажатия клавиш CTRL+ALT+DEL;
- RCTRL+R – перейти в хостовый компьютер?

6. В состав приложения ВМ входят:

- консоль ВМ;
- монитор ВМ;
- хостовая ОС;
- гостевая ОС?
-

7. Операционная система, запускаемая в среде виртуальной машины:

- консольная ОС;
- хостовая ОС;
- гостевая ОС;
- виртуальная ОС?

8. Типовое имя сетевого адаптера в среде приложения виртуальных машин VirtualBox:

- REALTEK;
- AMD PCNET;
- NVIDIA.

9. Образ диска это:

- содержимое компакт диска, хранимое на жестком диске;
- точная копия носителя информации, хранимая в файле;
- слепок системного диска, хранимый в файле?

10. Инструмент для создания виртуальных машин на компьютере это:

- хостовая ВМ;
- приложение ВМ;
- консоль ВМ?