Министерство науки и высшего образования РФ

ФГАОУ ВО «Томский государственный университет систем управления и радиоэлектроники»

Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)

А.Ю. Якимук

ПРИКЛАДНАЯ КРИПТОГРАФИЯ

методические рекомендации для лабораторных, практических и самостоятельных работ для студентов направления подготовки 25.05.03 Техническая эксплуатация транспортного радиооборудования

Томск, 2025

УДК 004.056
ББК 32.973.26-018.2
Я 64

Якимук, А.Ю. Прикладная криптография: методические рекомендации для лабораторных, практических и самостоятельных работ [Электронный ресурс] / – Томск: ТУСУР, 2025. – 359 с.

Практикум содержит описания лабораторных и практических работ по дисциплине «Прикладная криптография» для специальности 25.05.03 Техническая эксплуатация транспортного радиооборудования. В практикуме даны задания, методические указания по выполнению, требования по представлению отчётности, вопросы для самоконтроля.

Одобрено на заседании кафедры КИБЭВС протокол №1 от 28.01.2025 года

УДК 004.056
ББК 32.973.26-018.2

© Якимук А.Ю. 2025
© Томск. гос. ун-т систем упр. и радиоэлектроники, 2025

ВВЕДЕНИЕ

В данном методическом пособии представлены лабораторные и практические работы, которые направлены на закрепление полученных знаний в области прикладной криптографии.

Целью является развитие у студентов представлений о практическом использовании криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности. В рамках практических и лабораторных задач рассматриваются математические основы современной криптографии, основные криптографические алгоритмы.

ПРАКТИЧЕСКАЯ РАБОТА №1.
Множества, операции и алгебраические структуры

1. Краткие теоретические сведения

Понятие множества является фундаментальным в математике и поясняется через близкие понятия: совокупность, семейство, класс и др. Множество – совокупность объединенных по некоторым признакам различных объектов, называемых элементами множества. В множестве не может быть двух одинаковых элементов.

Мы будем понимать под множеством любую совокупность объектов, называемых элементами множества. Множества с конечным числом различных элементов могут быть описаны путем явного перечисления всех элементов. Обычно эти элементы заключаются в фигурные скобки. Например, {16,32,64} – множество степеней двойки, заключенных между 10 и 100.

Если x – элемент множества X, то говорят, что x принадлежит X, и записывают x∈X. В противном случае записывают x∈X. Множество обозначается прописной буквой какого-либо алфавита, а его элементы – строчными буквами того же или другого алфавита. Для некоторых особо важных множеств приняты стандартные обозначения, которых следует придерживаться.

Так, буквами N, Z, Q, R обозначают соответственно множество натуральных чисел, множество целых чисел, множество рациональных чисел и множество вещественных чисел. Два множества X и Y равны, если каждый элемент множества X содержится в Y и наоборот.

Пусть A, B, C— тройка непустых множеств.
Бинарной операцией, или бинарной функцией, на паре A, B со значениями в C называется отображение

$$P: A * B \to C$$

Пусть A — непустое множество. Бинарной операцией на множестве A, или внутренней бинарной операцией, называют отображение

$$P: A * A \to A$$

Комбинация множеств и операций, которые могут быть применены к элементам множества, называются алгебраической структурой.

2. Задание на практическую работу

1. Ознакомьтесь с теорией по теме множеств, бинарных операций и алгебраических структур.

2. Опишите множество чисел от 1 до 100 кратных числу 14.

3. Приведите пример бинарных отношений, обладающих свойствами рефлексивности, симметричности, транзитивности.

4. Опишите множество элементов, входящих в множества N, Z, Q, R. Какие алгебраические структуры могут быть созданы на базе этих множеств?

5. Приведите пример нейтральных элементов для данных алгебраических структур.

ПРАКТИЧЕСКАЯ РАБОТА №2.
Наименьшее общее кратное. Наибольший общий делитель.

1. Краткие теоретические сведения

Целое число s называется делителем (или множителем) целого числа n, если n=st для некоторого t∈Z. В свою очередь n называется кратным s. Делимость n на s обозначается символом |.

Делимость – транзитивное свойство на Z. Целое число p, делители которого исчерпываются числами ±p, ±1 (несобственные делители), называется простым. Обычно в качестве простых берутся положительные простые числа > 1.

Наибольший общий делитель (НОД) двух данных чисел «a» и «b» — это наибольшее число, на которое оба числа «a» и «b» делятся без остатка. Кратко наибольший общий делитель чисел «a» и «b» записывают так: НОД (a; b). Пример: НОД (12; 36) = 12.

Алгоритм Евклида - предназначен для нахождения НОД. Заключается в последовательном нахождении остатка от деления большего числа на меньшее с отбрасыванием большего.

Наименьшее общее кратное (НОК) двух данных чисел «a» и «b» — это наименьшее число, которое делится без остатка на оба числа «a» и «b». Кратко наименьшее общее кратное чисел «a» и «b» записывают так: НОК (a; b). Пример: НОК (12; 36) = 36.

$$\text{НОК}\,(a,b) = {}^{a*b}/_{\text{НОД}\,(a,b)}$$

2. Задание на практическую работу

1. Ознакомьтесь с теорией по теме вычисления наибольшего общего делителя и наименьшего общего кратного.

2. Найдите значения НОК и НОД для следующих пар чисел:

а) 17 и 38;
б) 14 и 42;
в) 3 и 93;
г) 4 и 18;
д) 43 и 66.

ПРАКТИЧЕСКАЯ РАБОТА №3.
Китайская теорема об остатках.

1. Краткие теоретические сведения

Существует легенда, что в Китае военачальники делали так: давали несколько последовательных команд типа «В колонну по 7 становись!», «В колонну по 11 становись!», … , и в каждом случае выясняли, сколько солдат получилось в последнем ряду. После этого — только по найденным остаткам — вычислялось общее количество солдат с помощью китайской теоремы об остатках.

Пусть m_1, m_2, ..., m_n — попарно взаимно простые натуральные числа (то есть НОД(m_i , m_j) = 1 при i!=j) и M = $m_1 m_2$ ... m_n.

Тогда, каковы бы ни были целые числа a_1, a_2, ... , a_n, система сравнений

$$x \equiv a_1 \bmod m_1$$
$$x \equiv a_2 \bmod m_2$$
$$\dots$$
$$x \equiv a_n \bmod m_n$$

имеет единственное решение

$$x \equiv a \pmod{M},$$

где $a=\sum a_i * M_i * \mu_i$

$M_i=M/m_i$

$\mu_i=M_{i\,-1} \bmod m_i$

2. Задание на практическую работу

1. Ознакомьтесь с теорией по теме.

2. Выполните вычисление «численности армии» для которой будут верны следующие остатки:

а) 4 при делении на 5, 6 при делении на 7 и 1 при делении на 13;

б) 3 при делении на 5, 2 при делении на 17 и 4 при делении на 23

в) 2 при делении на 5, 8 при делении на 17 и 1 при делении на 13

г) 1 при делении на 5, 6 при делении на 17 и 21 при делении на 23

д) 5 при делении на 13, 1 при делении на 7 и 31 при делении на 43.

ПРАКТИЧЕСКАЯ РАБОТА №4.
Длинная арифметика. Возведение в степень.

1. Краткие теоретические сведения

Представим, что оператора возведения в степень нет в нашем распоряжении, так что остаётся лишь умножать. Определение степени с целым неотрицательным показателем x^n позволяет сделать вычисление с использованием $n-1$ умножения. Но умножение — достаточно затратная операция (вспомним умножение в столбик). Поэтому постараемся свести к минимуму число выполняемых умножений.

К примеру, если показатель степени сам является степенью двойки, $n=2^m$, то потребуется всего лишь m умножений, точнее, возведений в квадрат: $(\ldots((x^2)^2)\ldots)^2$

2. Задание на практическую работу

1. Ознакомиться с теорией.
2. Вычислить следующие значения:
   а) $23^{731} \bmod 71$;
   б) $43^{128} \bmod 67$;
   в) $13^{932} \bmod 83$;
   г) $64^{731} \bmod 67$;
   д) $27^{614} \bmod 31$;
   е) $29^{499} \bmod 53$;
   ж) $42^{991} \bmod 89$.

ПРАКТИЧЕСКАЯ РАБОТА №5.
Исторические криптографические системы. Шифр Цезаря.

1. Краткие теоретические сведения

Согласно описаниям историка Светония в книге «Жизнь двенадцати цезарей» данный шифр использовался Гаем Юлием Цезарем для секретной переписки со своими генералами (I век до н.э.). Применительно к русскому языку суть его состоит в следующем. Выписывается исходный алфавит (А, Б, ..., Я), затем под ним выписывается тот же алфавит, но с циклическим сдвигом на 3 буквы влево.

А	Б	В	Г	…	Ю	Я
Г	Д	Е	Ё	…	Б	В

При зашифровке буква А заменяется буквой Г, Б - на Д и т. д. Так, например, исходное сообщение «РАМА» после шифрования будет выглядеть «УГПГ». Получатель сообщения «УГПГ» ищет эти буквы в нижней строке и по буквам над ними восстанавливает исходное сообщение «РАМА».

Ключом в шифре Цезаря является величина сдвига нижней строки алфавита. Количество ключей для всех модификаций данного шифра применительно к алфавиту русского языка равно 33.

2. Задание на практическую работу

1. Изучите краткую теорию по шифу Цезаря.
2. Зашифруйте следующие сообщения с помощью шифра Цезаря:
   а) Слово «апельсин» с помощью сдвига на 18;
   б) Слово «барокко» с помощью сдвига на 4;
   в) Слово «мультиметр» с помощью сдвига на 5;
   г) Слово «восстание» с помощью сдвига на 14;
   д) Слово «пингвин» с помощью сдвига на 23;
   е) Слово «равнодушие» с помощью сдвига на 13;
   ж) Слово «выходной» с помощью сдвига на 19;
   з) Слово «технология» с помощью сдвига на 32;
   и) Слово «крокодил» с помощью сдвига на 31.

ПРАКТИЧЕСКАЯ РАБОТА №6.
Частотный криптоанализ.

1. Краткие теоретические сведения

Таблица замен имеет вид случайной перестановки. Одним из существенных недостатков шифров однозначной замены является их легкая вскрываемость. При вскрытии шифрограмм используются различные приемы, которые даже при отсутствии мощных вычислительных средств позволяют добиться положительного результата.

Один из таких приемов базируется на том, что в шифрограммах остается информация о частоте встречаемости букв исходного текста. Если в открытом сообщении часто встречается какая-либо буква, то в шифрованном сообщении также часто будет встречаться соответствующий ей символ.

2. Задание на практическую работу

1. Изучите краткую теорию по теме частотного анализа шифртекста.

2. Расшифруйте следующие криптограммы с применением частотного анализа:

а) ЧЕЛВНГ ТГШАФГЫАР УЮГХЛГ ФЩГПА Й ЧАШВЗГ ФЩГПА. ЬГ ЧАДНГЩВ ЩШЙЗЫАР АНМПАНЙНВ ЩГЧМ ПЕРЯЬЬАЩНВЦ.

б) ФИЮЭОЕ Щ ФИКСН – ЖАЭ П БХАЕ АБ ЩЛЦФЕС, ЗЫ ЩЭАЭЛЦЬ РБФЭОБЩ ЙЭКЗПНЫБАХС ОЦДБ ОХБУЭ.

в) ЯНЦШХ ВИ НОЬХШХИЙП ГБШЖНЕСПЭ, НЕСХИСЕЗ ЬЭОДСП ГБШЖНЕСП, С.И. ОТСП ЧДЬНЕНЧНГ.

ЛАБОРАТОРНАЯ РАБОТА №1.
Шифрованная файловая система Windows

1. Цель работы

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

2. Краткие теоретические сведения

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

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

Симметричный алгоритм шифрования, используемый EFS, зависит от версии операционной системы и выбранных настроек. Возможные варианты: 3DES, DESX, AES. Для шифрования каждого файла должен быть сгенерирован случайный ключ, называемый File Encryption Key (FEK). Секретность данного ключа, в свою очередь, обеспечивается с помощью асимметричного шифрования по алгоритму RSA, для чего используется открытый ключ пользователя, содержащийся в цифровом сертификате (рис. 1).

Когда пользователю необходимо получить доступ к содержимому зашифрованного файла, драйвер шифрованной файловой системы прозрачно для него расшифровывает FEK, используя закрытый ключ пользователя, а затем с помощью соответствующего симметричного алгоритма на расшифрованном ключе — сам файл (рис. 2).

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

в раздел NTFS. Остальные пользователи не могут получить доступ к содержимому файлов.

При шифровании каталога шифруются все находящиеся в нем файлы.

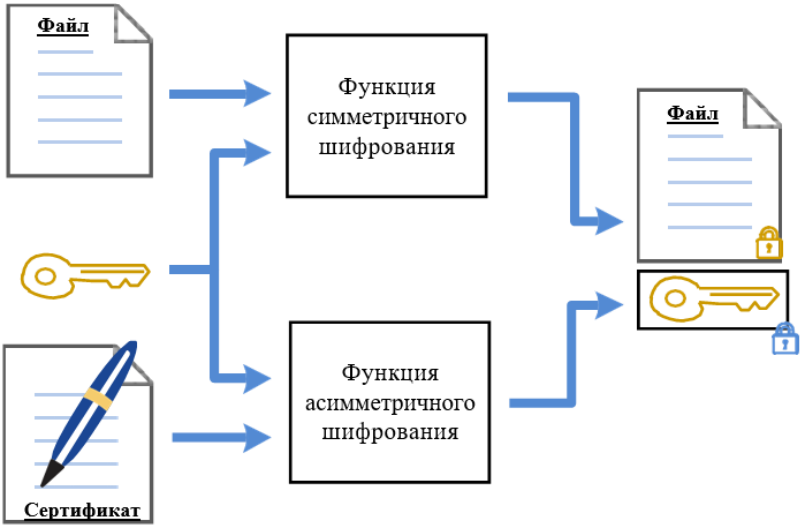

Рис. 1. Схема зашифрования файла

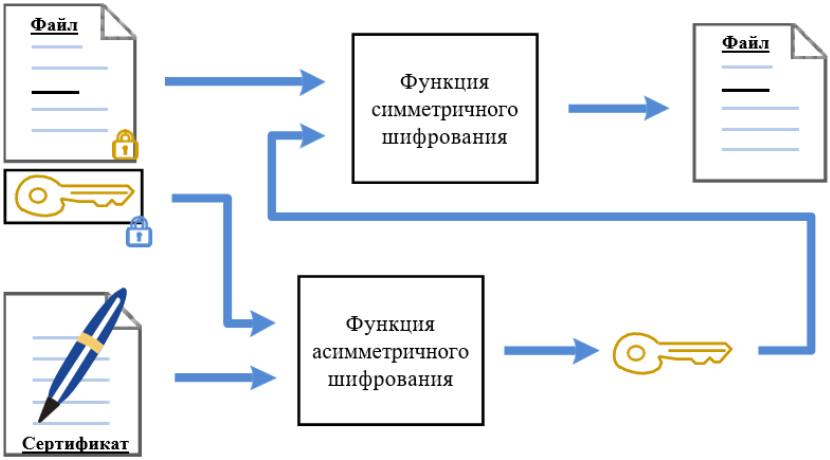

Рис. 2. Схема расшифрования файла

3. Ход работы

3.1 Шифрованная файловая система

Данная практическая работа может быть выполнена на любой виртуальной машине, удовлетворяющей требованиям к шифрованной файловой системе, указанным в предыдущем разделе. В качестве примера будет рассмотрена Windows 10.

Прежде чем приступить к изучению шифрованной файловой системы Windows, необходимо создать двух пользователей, от имени которых будут выполняться операции по шифрованию файлов (рис. 3). Как вариант, можно использовать при создании пользователей номер группы (NNNN) и инициалы студента на английском языке (FIO), выполняющего данную работу.

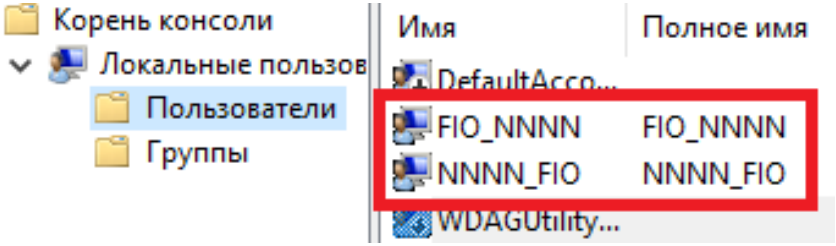

Рис. 3. Созданные пользователи для практической работы

Далее потребуется выбрать файлы, с которыми будет вестись дальнейшая работа. Для этого на локальном диске виртуальной машины создайте два произвольных файла, например, два текстовых файла NNNN.txt и FIO.txt (рис. 4) с указанием номера группы и фамилии исполнителя. Обязательно добавьте текст в содержание файла. Каждому из них затем будут назначены свои параметры шифрования.

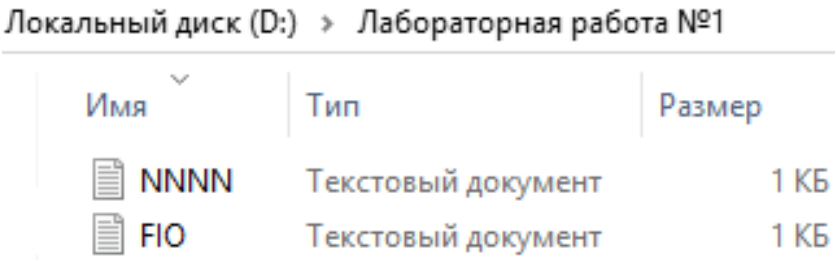

Рис. 4. Схема расшифрования файла

Зайдите под первым созданным пользователем (NNNN_FIO в текущем примере) и перейдите к шифрованию первого файла. Для этого необходимо выполнить следующие действия:

- вызвать контекстное меню нужного объекта (файла или папки) и выбрать пункт «Свойства»;
- перейти на вкладку «Общие» и нажать кнопку «Другие», что приведет к открытию окна «Дополнительные атрибуты»;
- активировать параметр «Шифровать содержимое для защиты данных» (рис. 5);
- закрыть оба окна при помощи кнопки «ОК».

Если шифрование было применено к отдельному файлу, который расположен не в корне локального диска, а в какой-либо папке, то система выдаст дополнительный запрос на запуск шифрования только данного файла или всей папки, в которой этот файл расположен (рис. 6).

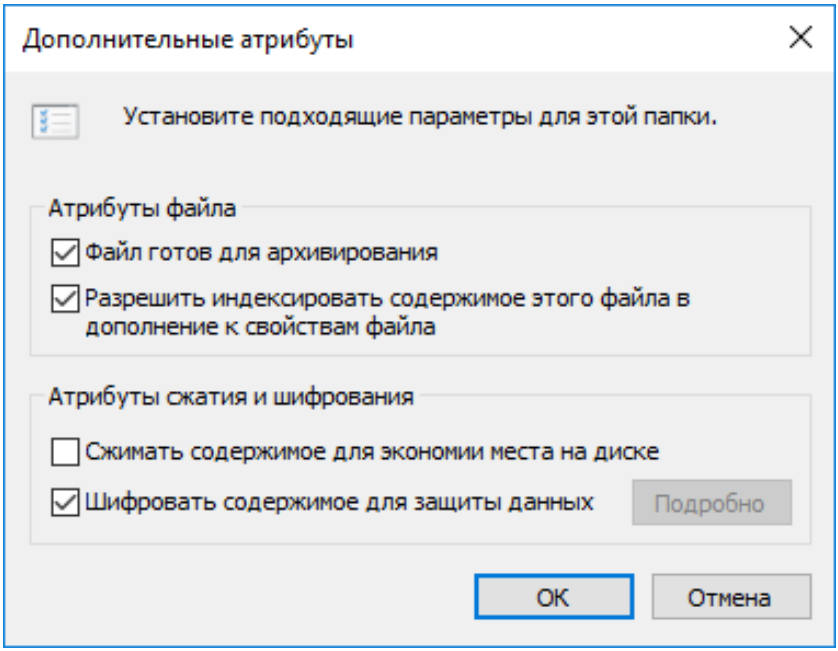

Рис. 5. Настройка атрибутов для шифрования файла

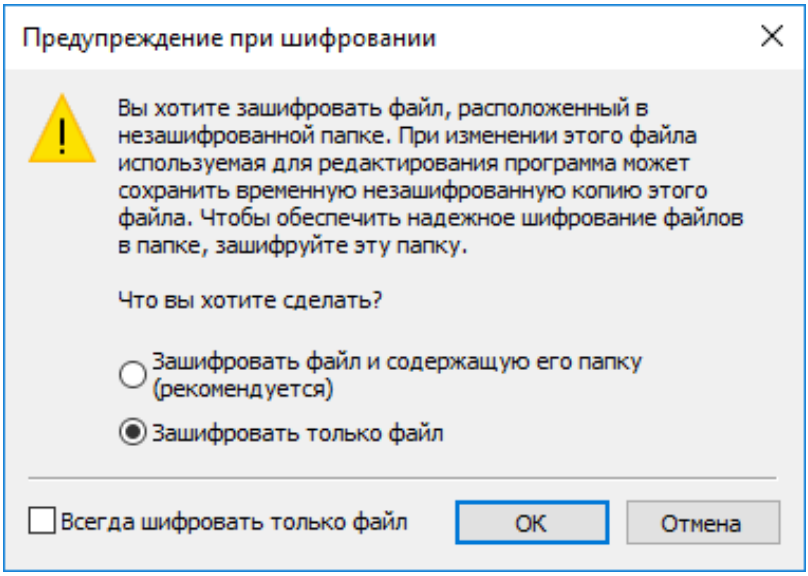

Рис. 6. Дополнительный запрос при шифровании файла

Если шифрование было применено к папке, то система выдаст дополнительный запрос на запуск шифрования всего каталога (рис. 7).

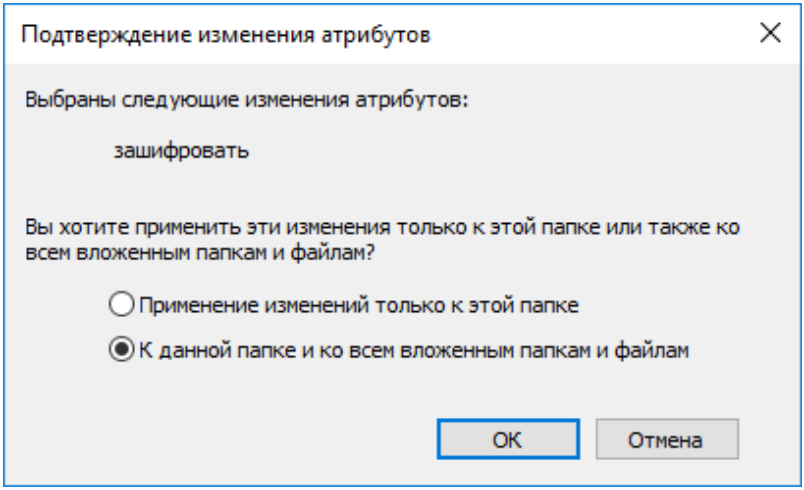

Рис. 7. Дополнительный запрос при шифровании папки

После этого файл (папка с файлами) будет зашифрован, а система сообщит о том, что в папке имеется зашифрованный файл (рис. 8) – значок файла изменится на аналогичный изначальному, но с обозначением замка в верхнем правом углу (на Windows 7 название зашифрованного файла отображалось зелёным цветом). Если нужно отключить шифрование, то необходимо снова открыть панель «Дополнительные атрибуты» и отключить параметр «Шифровать содержимое для защиты данных».

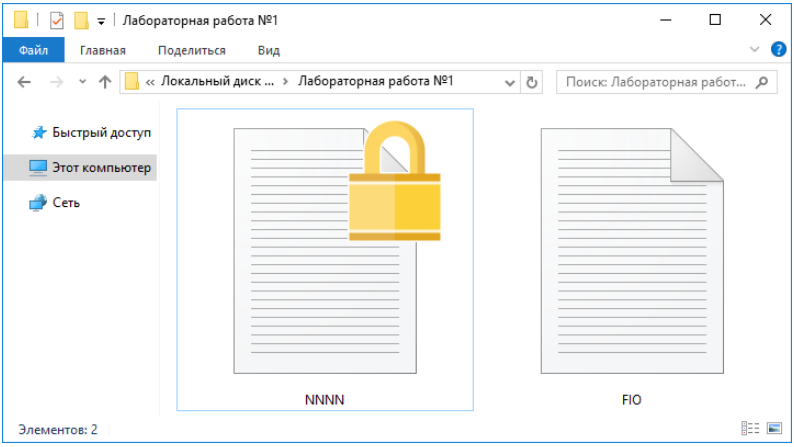

Рис.8. Вид файла с включенным шифрованием

При первой настройке функции шифрования отобразится предложение о создании архивной копии сертификата и ключа шифрования (рис. 9). Данную процедуру обязательно необходимо произвести, поскольку есть шанс потерять зашифрованные файлы, например, после переустановки системы или удаления учетной записи.

В случае, если по какой-то причине данное окно не появилось, можно запустить процесс архивации ключей следующим образом. Зайдите в свойства зашифрованного файла и откройте окно с дополнительными атрибутами. Нажмите на кнопку «Подробно» для отображения информации о доступе к данному файлу (рис. 10).

Выберите пользователя, чей сертификат необходимо архивировать и нажмите на кнопку «Архивация ключей». В результате будет запущен мастер экспорта сертификатов (рис. 11). Ознакомьтесь с информацией, указанной на приветственном окне мастера и нажмите кнопку «Далее».

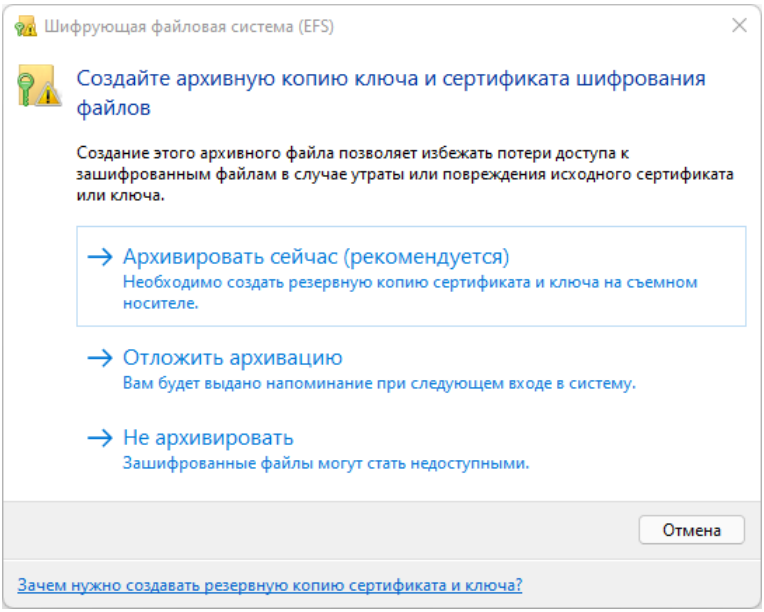

Рис.9. Вид файла с включенным шифрованием

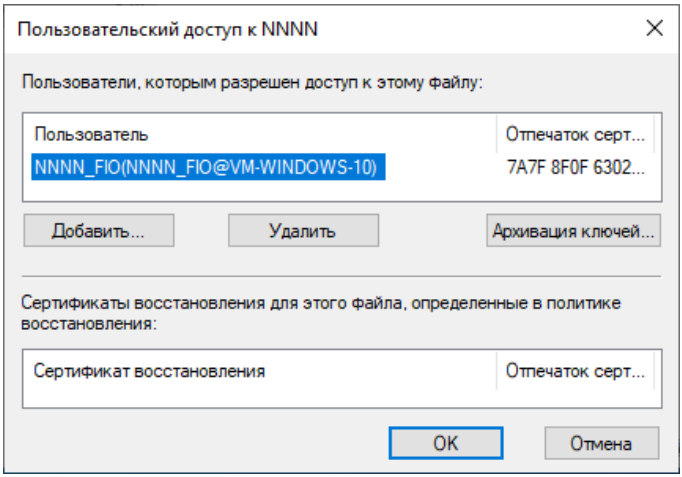

Рис.10. Информация о предоставленном доступе к зашифрованному файлу

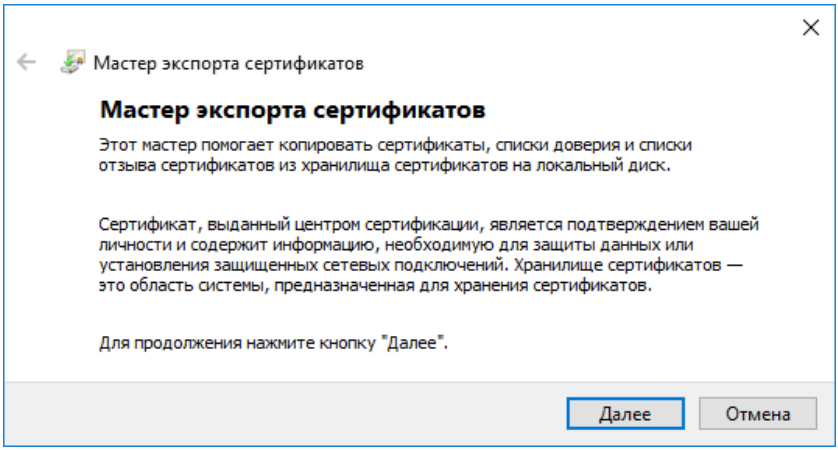

Рис.11. Мастер экспорта сертификатов

В следующем окне потребуется выбрать в каком формате будет осуществлен экспорт файла сертификата. Доступным для данного вида сертификатов является только формат файла обмена личной информацией (рис. 12).

Данный файл будет сформирован в соответствии с 12-м стандартом семейства Public Key Cryptography Standards (PKCS). Данные стандарты криптографии с открытым ключом являются спецификациями, разработанными RSA Security для ускорения разработки ассиметричных криптографических методов. Первый стандарт в данной группе как раз относится к алгоритму шифрования RSA.

PKCS#12 определяет формат файла, используемый для хранения и/или транспортировки закрытого ключа, цепочки доверия от сертификата пользователя до корневого сертификата удостоверяющего центра и списка отзыва сертификатов. Формат распознаётся и используется многими браузерами и почтовыми агентами. В файлах PKCS#12 хранятся одновременно и сертификат, и закрытый ключ.

Защита файла осуществляется одним из двух способов: безопасным, с использованием доверенной ключевой пары (открытый/закрытый ключи, подходящие для цифровой подписи и шифрования) или менее безопасным, с использованием симметричного ключа, основанного на пароле. Второй подходит для случаев, когда использование доверенных пар открытый/закрытый ключей недоступны.

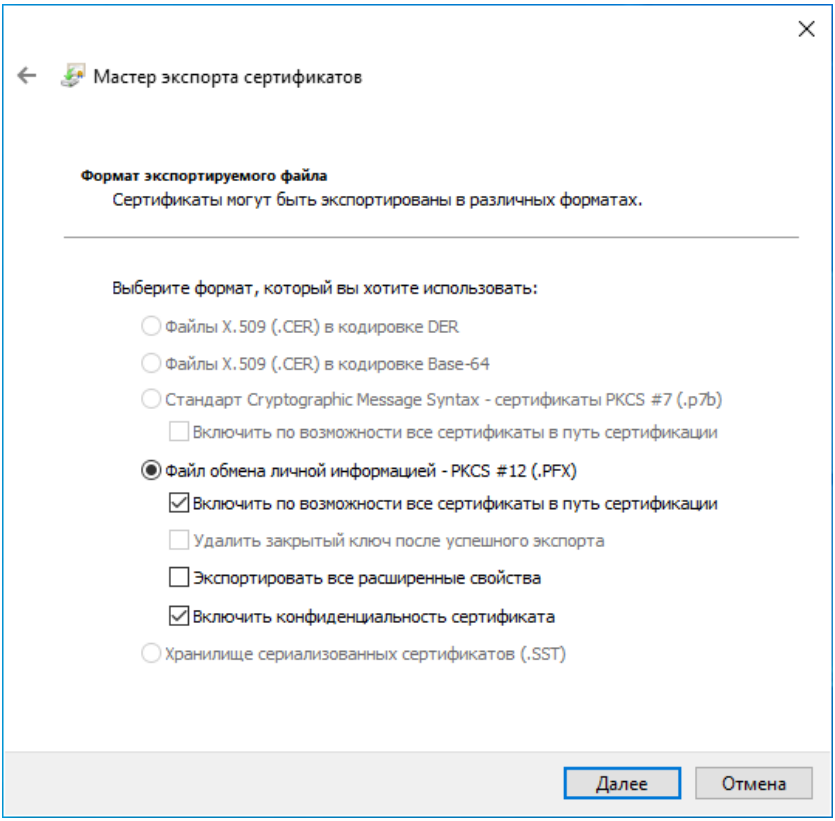

Рис.12. Формат файла экспортируемого сертификата

В текущем окне можете оставить все параметры по умолчанию и нажать на кнопку «Далее». Откроется раздел, относящийся к организации безопасности закрытого ключа (рис. 13). Раздел, относящийся к выбору групп или пользователей, доступен на компьютерах, включенных в состав домена. Поэтому в данном случае раздел игнорируем.

Поставьте галочку напротив пункта «Пароль». Задайте пароль и его подтверждение. В качестве алгоритма шифрования выберите AES. Альтернативой к нему идет вариант с тройным шифрованием по алгоритму DES (Triple DES или 3DES).

Нажмите на кнопку «Далее». В результате откроется следующая вкладка, в которой необходимо задать информацию по создаваемому файлу.

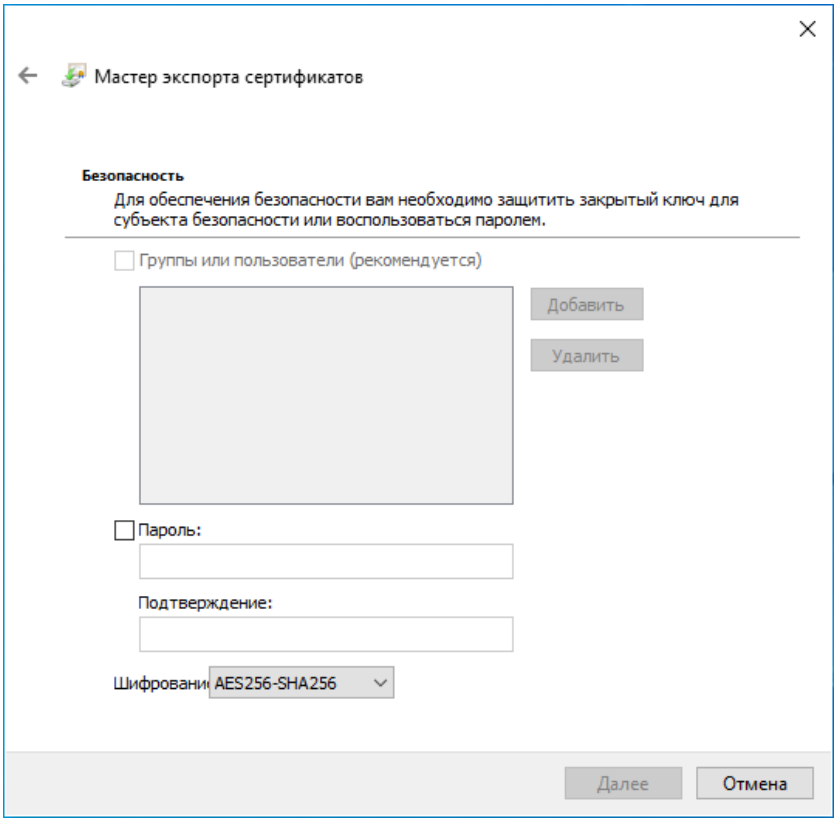

Рис.13. Защита закрытого ключа для субъекта безопасности

Нажмите на кнопку «Обзор» и выберите расположение, куда хотите сохранить экспортируемый сертификат с ключом (рис. 14). После внесения всей необходимой информации нажмите на кнопку «Далее».

На следующем шаге будет выведена обобщенная информация по процедуре экспорта сертификата. Ознакомьтесь с ней и нажмите кнопку «Готово». В результате будет выведено сообщение об успешном экспорте сертификата (рис. 15).

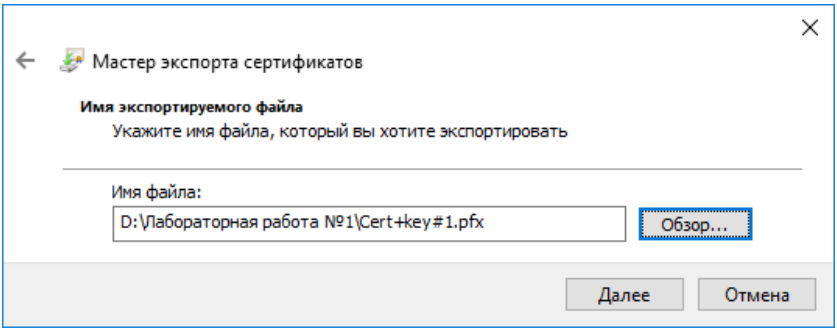

Рис.14. Защита закрытого ключа паролем

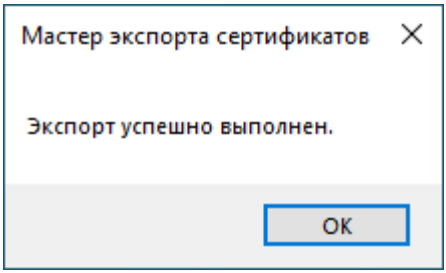

Рис.15. Уведомление об успешном экспорте сертификата

Чтобы проверить, что данный файл зашифрован, зайдите под учетной записью второго созданного пользователя. Попробуйте открыть файл первого пользователя (зашифрованный им) под учетной записью второго пользователя. Будет выведено сообщение об отказе доступа к файлу (рис. 16).

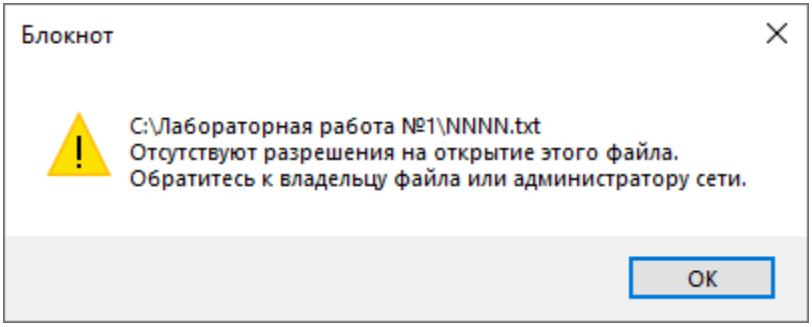

Рис.16. Уведомление об отказе в доступе

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

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

Удалим данный сертификат вручную у первого пользователя. Откройте меню «Пуск», в поле поиска введите название утилиты «certmgr.msc» и нажмите Enter (рис. 17).

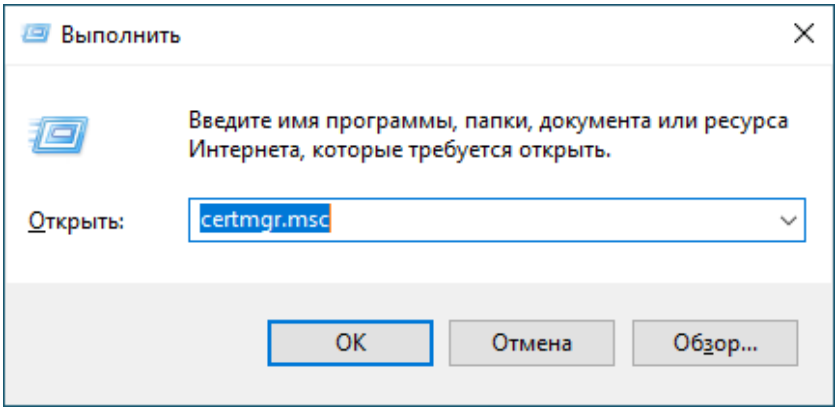

Рис.17. Вызов оснастки управления хранилищем сертификатов

В открывшемся окне управления хранилищем сертификатов откройте сертификаты раздела «Личное» (рис. 18).

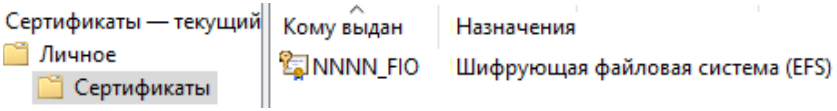

Рис.18. Сертификат первого пользователя в хранилище

Удалите сертификат первого пользователя. Система предупредит о том, что данная операция может привести к невозможности просмотреть и расшифровать файлы, зашифрованные с помощью данного ключа (рис. 19).

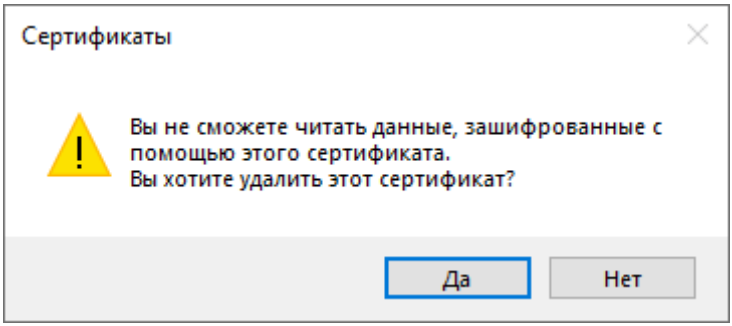

Рис.19. Предупреждение о последствиях удаления сертификата

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

Чтобы вернуть доступ, необходимо восстановить сертификат и закрытый ключ пользователя. Для этого снова откройте хранилище сертификатов, перейдите в сертификаты раздела «Личное» и, вызвав правой кнопкой контекстное меню, выберите «Все задачи/Импорт…». Запустится мастер импорта сертификатов, нажмите «Далее» (рис. 20).

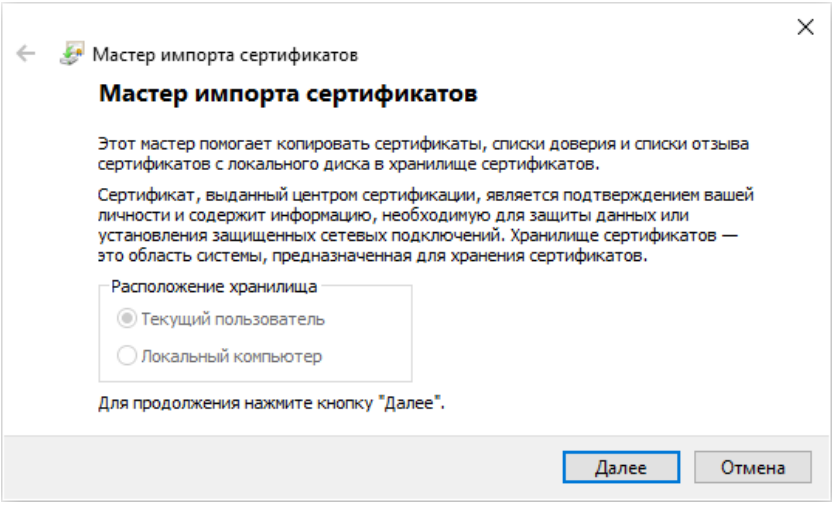

Рис.20. Мастер импорта сертификатов

Укажите нужный сертификат, при этом нужно сменить указанный тип файлов с .cer и .crt на .pfx, так как по умолчанию в программе задаются сертификаты без закрытого ключа, нажмите «Далее» (рис. 21).

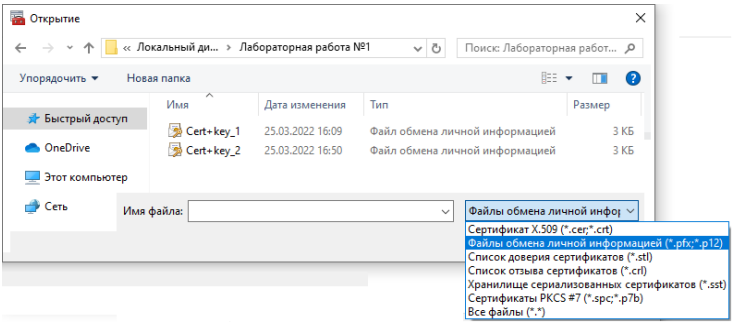

Рис.21. Выбор восстанавливаемого сертификата

В следующем окне необходимо ввести пароль, указанный при архивировании сертификата первого пользователя. Введите пароль и нажмите «Далее» (рис. 22).

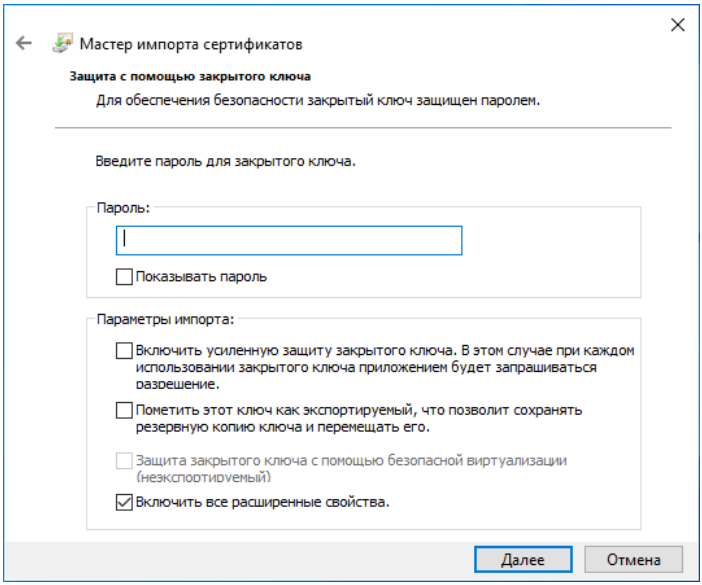

Рис.22. Ввод пароля для восстановления сертификата

Поместите сертификат в хранилище сертификатов «Личное», нажмите «Далее» (рис. 23).

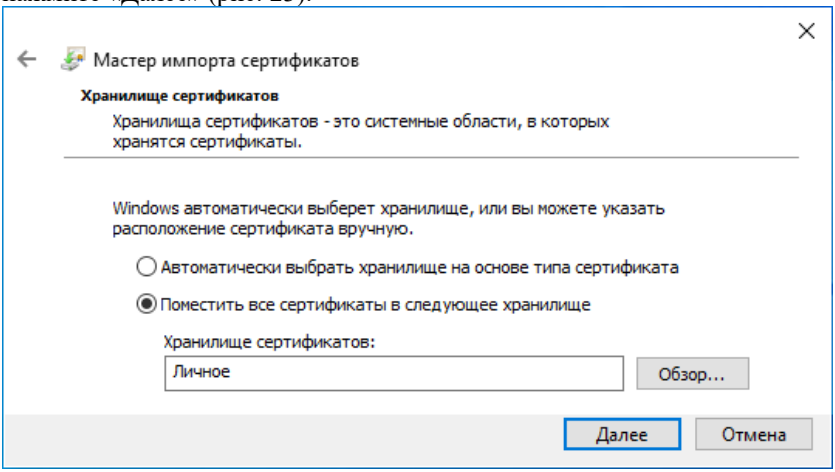

Рис.23. Выбор хранилища для импорта сертификата

Восстановление сертификата с закрытым ключом завершено (рис. 24). Теперь доступ к файлам должен быть восстановлен. Проверьте от лица первого пользователя возможность просмотра содержимого файла.

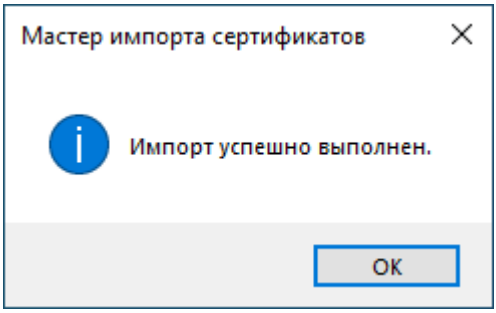

Рис.24. Уведомление об успешном импорте сертификата

3.2 Совместное использование файлов

Использовать шифрование файлов можно и при совместном использовании одного файла несколькими пользователями. Общий доступ для папок не устанавливается. Сделайте доступным второй файл первому пользователю. Для этого войдите под вторым пользователем и

откройте его личное хранилище сертификатов пользователя. Выделите сертификат, вызовите контекстное меню и выполните команду «Все задачи/Экспорт…» (рис. 25).

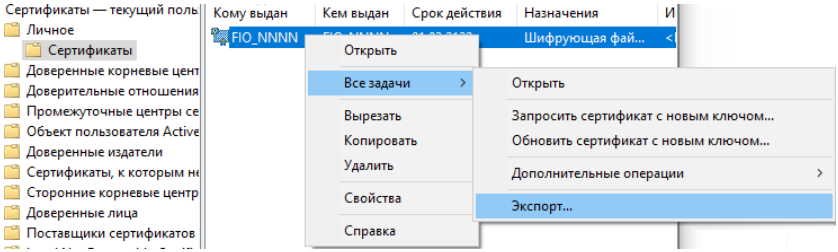

Рис.25. Экспорт сертификата второго пользователя

При этом необходимо выполнить экспорт сертификата без закрытого ключа (рис. 26).

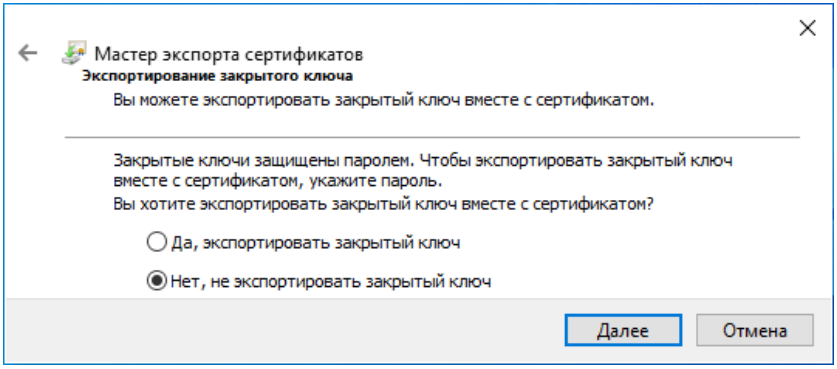

Рис.26. Экспорт сертификата без закрытого ключа

Представим, что данный сертификат был передан первому пользователю. Снова перейдите на учетную запись первого пользователя и откройте хранилище сертификатов пользователя. Перейдите в раздел сертификатов «Личное», вызовите контекстное меню и выполните команду «Все задачи/Импорт…». Импортируйте сертификат второго пользователя без закрытого ключа в раздел «Доверенные лица».

Откройте свойства первого созданного файла, перейдите на вкладку «Общие» и нажмите кнопку «Другие». В окне «Дополнительные атрибуты» нажмите кнопку «Подробно», откроется окно доступа к файлу (рис. 27).

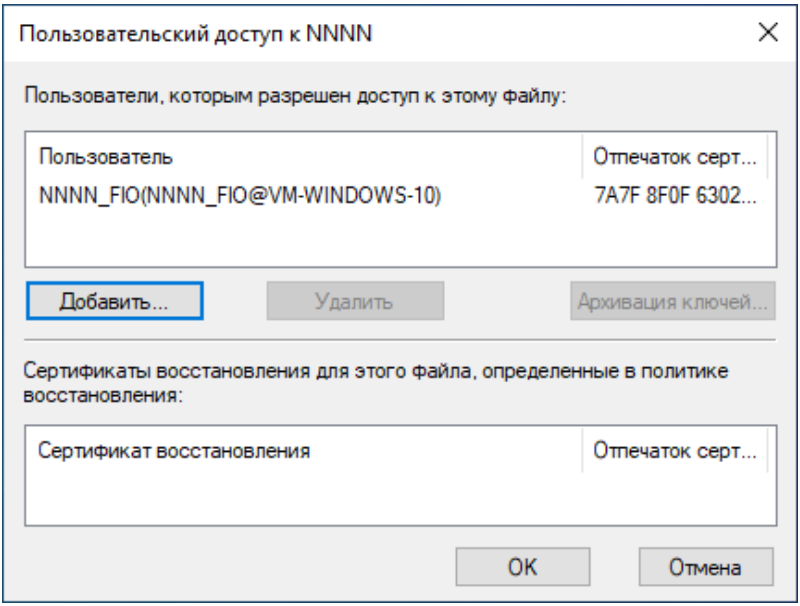

Рис.27. Настройка доступа к первому файлу

Нажмите кнопку «Добавить…» и выберите сертификат первого пользователя (рис. 28).

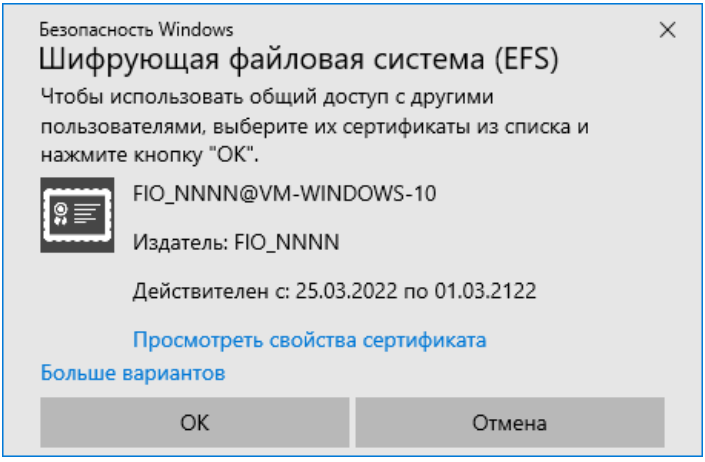

Рис.28. Добавление сертификата второго пользователя

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

4. Задание на лабораторную работу

1. Создайте учетные записи двух пользователей и файлы для каждого из них для выполнения практической работы.
2. Зашифруйте по одному файлу каждому из пользователей.
3. Архивируйте сертификаты с закрытым ключом для каждого из пользователей.
4. Сделайте совместный доступ к одному зашифрованному файлу для обоих пользователей.
5. Создайте третьего пользователя и проверьте доступ к файлу от него.
6. Составить по проделанной работе отчет.

5. Контрольные вопросы

1. В каких выпусках операционных систем Windows присутствует шифрованная файловая система?
2. Для каких файловых систем применима шифрованная файловая система?
3. Для чего в шифрованной файловой системе используются симметричное и асимметричное шифрование?
4. Для чего нужно архивировать закрытый ключ и сертификат пользователя?
5. Каким образом можно предоставить доступ к зашифрованному файлу другому пользователю?

ЛАБОРАТОРНАЯ РАБОТА №2.
Шифрование диска BitLocker

1. Цель работы

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

2. Краткие теоретические сведения

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

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

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

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

Технология BitLocker предназначена для работы с носителями информации, на которых используются файловые системы exFAT,

FAT16, FAT32 или NTFS. Для шифрования диска с операционной системой на нем должна использоваться файловая система NTFS.

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

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

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

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

Когда защита выполняется исключительно с помощью доверенного платформенного модуля, в процессе включения компьютера на аппаратном уровне происходит сбор данных, которые позволят

установить подлинность аппаратного обеспечения. Данная проверка является «прозрачной» и не требует от пользователя никаких действий, в случае успешного прохождения, выполняется загрузка операционной системы в штатном режиме. При обнаружении угрозы BitLocker заблокирует диск с операционной системой. Чтобы разблокировать его, потребуется специальный ключ восстановления BitLocker, который необходимо создать при первом запуске BitLocker. В противном случае доступ к файлам может быть потерян.

3. Ход работы

3.1 Предварительная подготовка

Данная практическая работа может быть выполнена на любой виртуальной машине, удовлетворяющей требованиям, указанным в предыдущем разделе. В качестве примера будет рассмотрена ОС Windows 10.

Для выполнения данной практической работы будет необходимо наличие на виртуальной машине не менее двух локальных дисков. Перейдите в настройки виртуальной машины, в разделе «Носители» выберите контроллер SATA и добавьте второй жесткий диск (рис. 1).

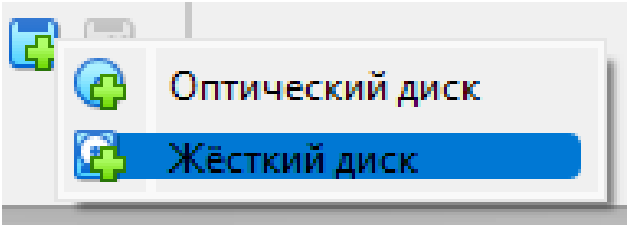

Рис. 2. Добавление второго жесткого диска

Чтобы добавленный жесткий диск стал доступным для работы после загрузки виртуальной машины запустите консоль управления MMC и в оснастке «Управление дисками» создайте простой том на добавленном диске.

Альтернативный вариант по созданию второго логического раздела на виртуальной машине заключается в сжатии имеющегося раздела для выделения места под второй том (рис. 2). Для вызова данной функции запустите оснастку «Управление дисками» и выберите имеющийся логический раздел. В контекстном меню выберите пункт «Сжать том».

Будет проведена оценка возможности сжать том и выведено окно, в котором можно определить величину высвобождаемого места (рис. 3). После выполнения сжатия на основе освободившегося дискового пространства создайте дополнительный раздел.

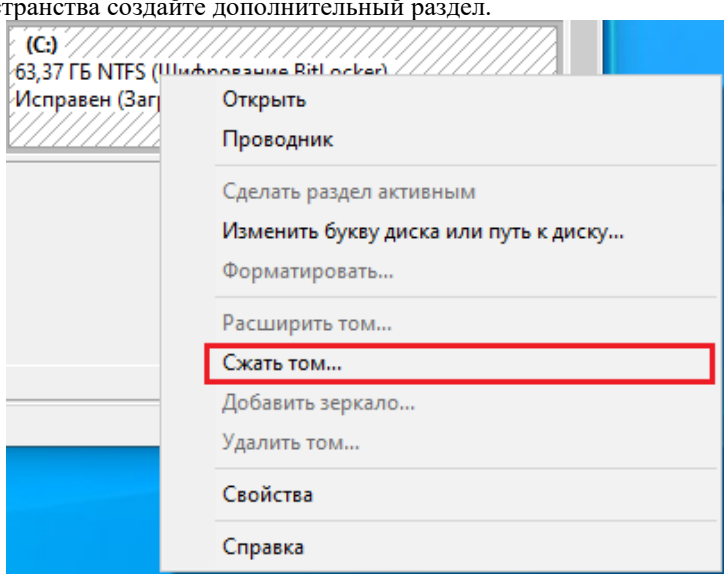

Рис. 2. Вызов функции сжатия тома

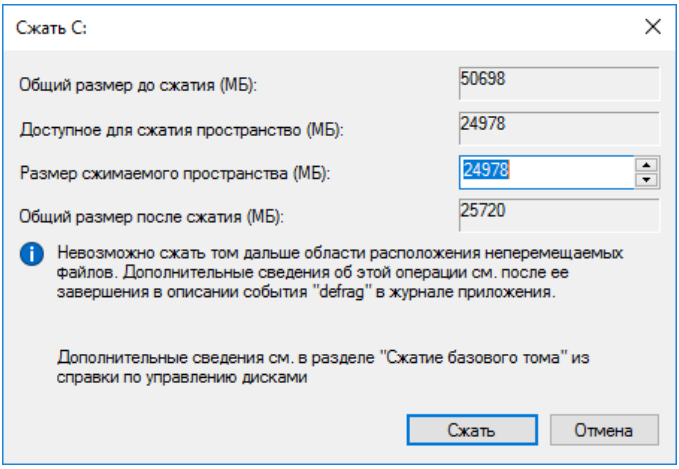

Рис. 3. Определение степени сжатия тома и объем освобожденного места

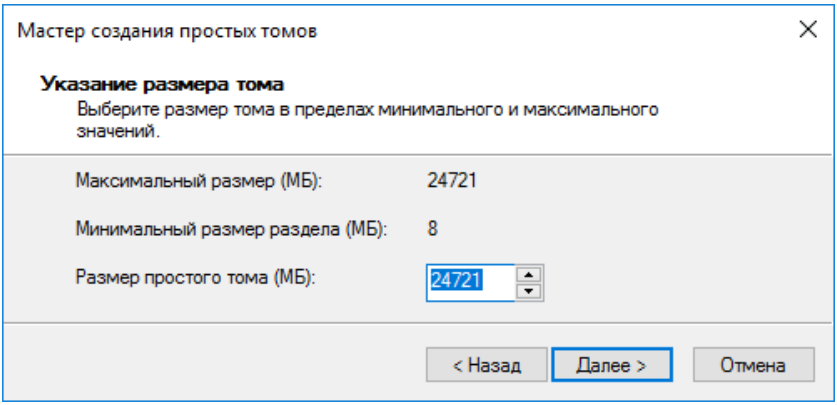

Рис. 4. Создание тома из освобожденного места

3.2 BitLocker To Go

Для шифрования локальных дисков, не являющихся системными, а также съемных дисков, предназначена функция BitLocker To Go. Чтобы воспользоваться данной функцией, необходимо открыть инструмент «Шифрование диска BitLocker» на «Панели управления» (рис. 5).

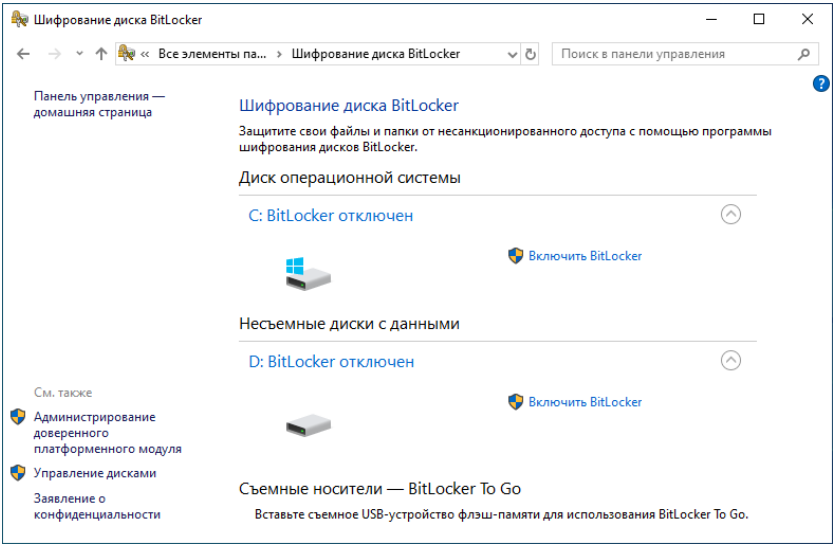

Рис. 5. Инструмент Windows «Шифрование диска BitLocker»

Чтобы запустить процедуру шифрования диска D, выполните команду «Включить BitLocker». Выберите способ шифрования с использованием пароля, введите произвольный пароль, содержащий не менее 8-ми символов, и нажмите «Далее» (рис. 6).

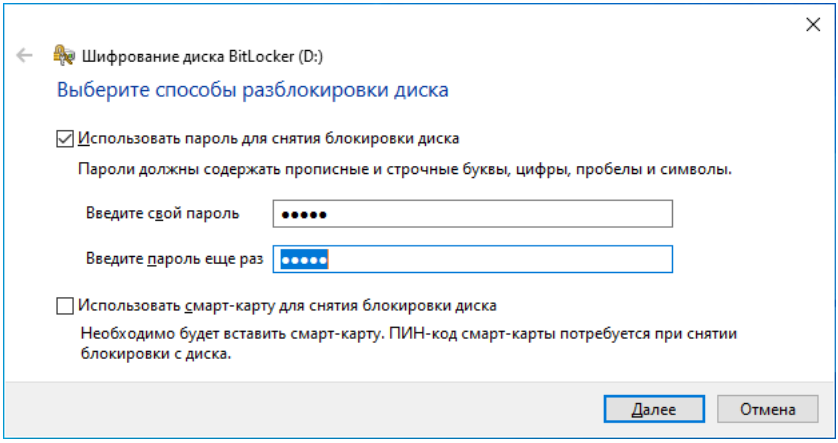

Рис. 6. Ввод пароля для блокировки диска

В следующем окне выберите пункт «Сохранить в файл» (рис. 7) и указав место сохранения файла, нажмите «Далее».

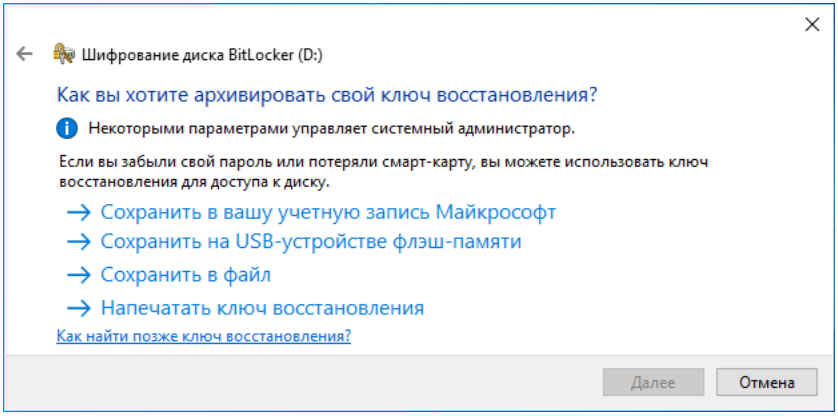

Рис. 7. Выбор варианта архивации ключа восстановления

Откроется меню выбора варианта шифрования диска (рис. 8). В качестве примера рассмотрим шифрование только занятого места на диске.

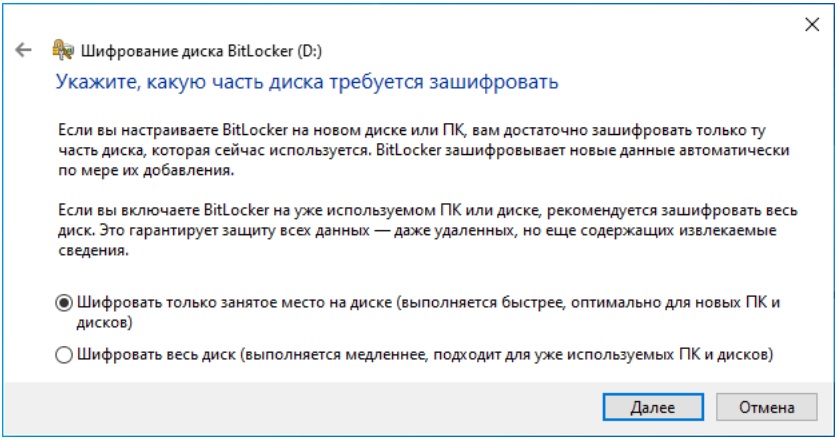

Рис. 8. Выбор варианта шифрования диска

На следующем шаге потребуется определиться с режимом шифрования диска (рис. 9). Этот режим был добавлен начиная с Windows 10 и является оптимальным для несъемных дисков. Выберите его и нажмите кнопку «Далее».

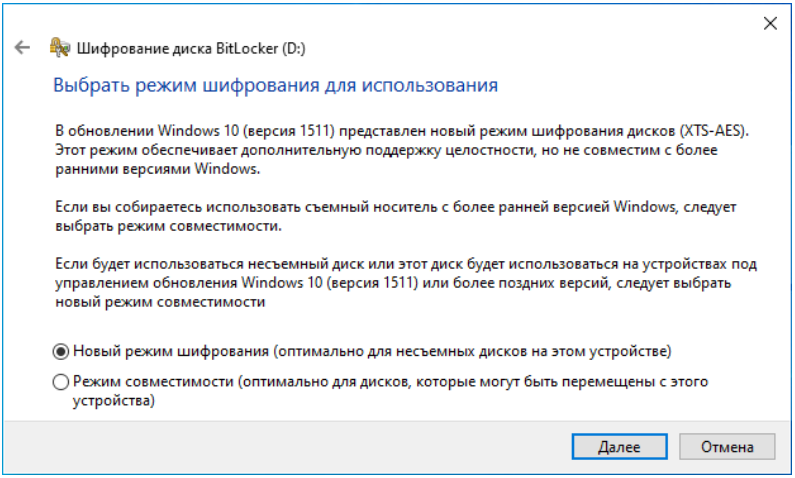

Рис. 9. Выбор режима шифрования диска

Затем запустите процедуру шифрования диска нажатием кнопки «Начать шифрование» (рис. 10) и дождитесь, когда диск будет полностью зашифрован (рис. 11).

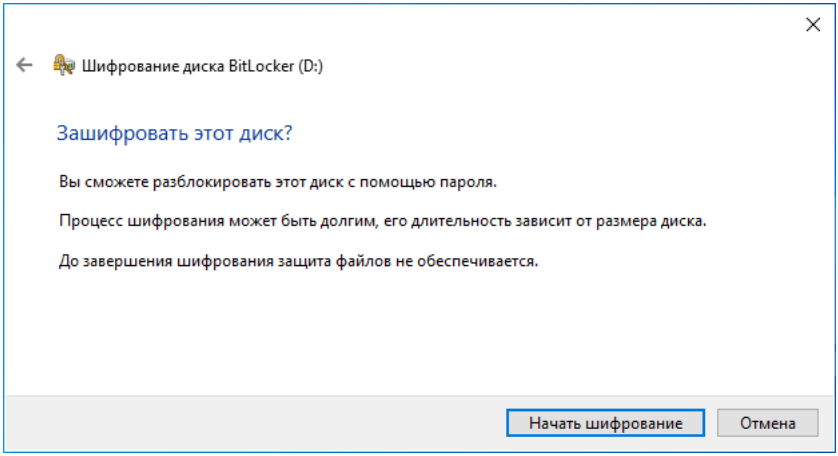

Рис. 10. Инструмент Windows «Шифрование диска BitLocker»

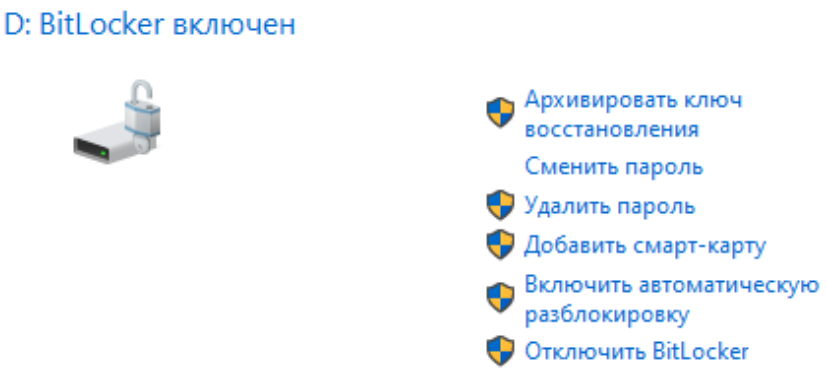

Рис. 31. Информация о включении BitLocker для диска D

Чтобы заблокировать диск, выполните перезагрузку. Теперь значок локального диска D в зашифрованном состоянии отображается с закрытым замком (рис. 12).

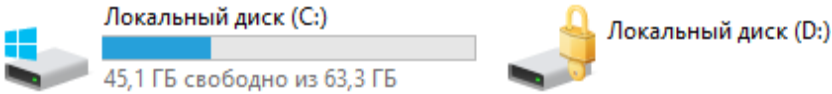

Рис. 42. Значок заблокированного диска D

При попытке открыть данный диск, появится окно с запросом пароля для разблокировки диска (рис. 13).

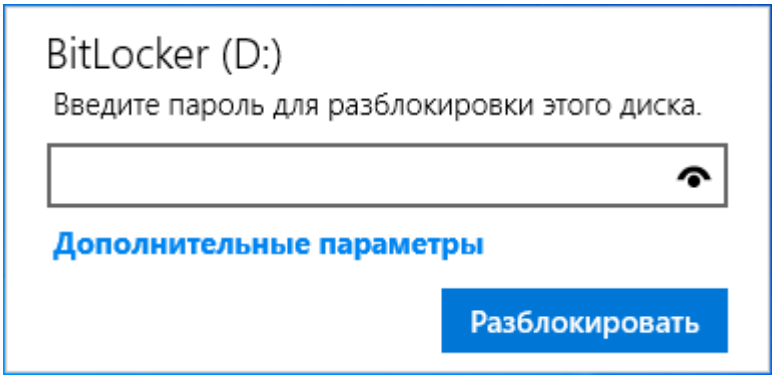

Рис. 53. Запрос на ввод пароля для снятия блокировки диска

После ввода верного пароля диск становится доступным, а значок диска изменяется на открытый замок (рис. 14).

Рис. 64. Значок разблокированного диска D

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

3.3 Использование BitLocker на компьютере без TPM

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

Откройте меню «Пуск», введите в поле поиска «gpedit.msc» и нажмите Enter (рис. 15).

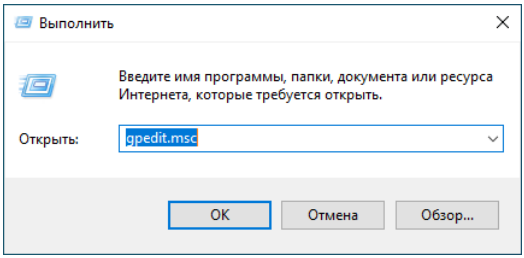

Рис. 75. Вызов оснастки редактора локальной групповой политики

В появившемся окне «Редактор локальной групповой политики» зайдите в раздел «Конфигурация компьютера», затем в «Административные шаблоны» и в «Компоненты Windows» найдите «Шифрование диска BitLocker» (рис. 16).

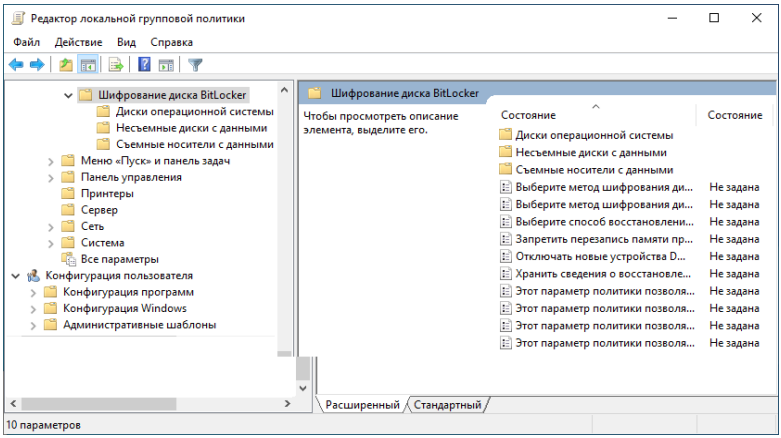

Рис. 86. Меню «Шифрование диска BitLocker» в групповых политиках

В данном компоненте зайдите в «Диски операционной системы» и откройте настройку «Этот параметр политики позволяет настроить требование дополнительной проверки подлинности при запуске» (рис. 17).

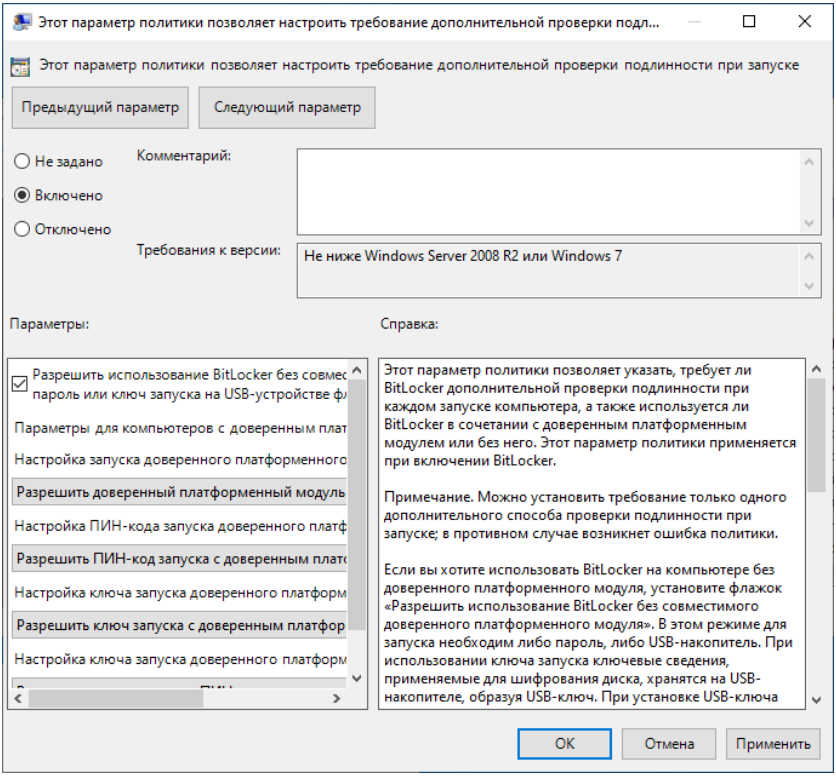

Рис. 97. Включение использования BitLocker без совместимого TPM

В появившемся окне выберите вариант «Включено», установите флажок «Разрешить использование BitLocker без совместимого TPM» и нажмите кнопку «ОК». Теперь вместо TPM можно использовать ключ запуска.

Закройте редактор локальной групповой политики. Чтобы новые настройки групповых политик вступили в силу немедленно, нажмите кнопку «Пуск», введите «gpupdate.exe /force» в поле поиска и нажмите Enter. Дождитесь завершения процесса (рис. 18).

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

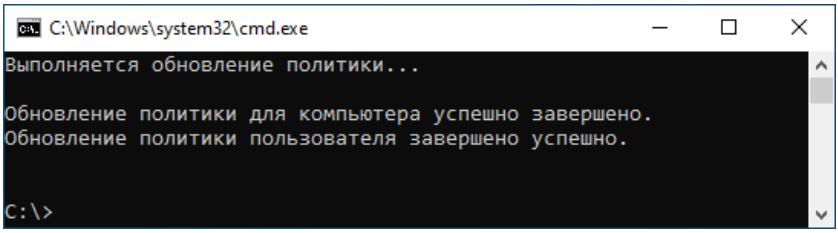

Рис. 108. Применение новых настроек групповых политик

3.4 Подготовка системного диска для BitLocker

Способ шифрования системного диска с использованием USB-флеш-накопителя в качестве носителя ключа запуска можно использовать только на компьютере, BIOS которого поддерживает чтение USB-устройств в загрузочной среде. Также необходимо, чтобы BIOS был настроен на загрузку сначала с жесткого диска, а затем с USB-устройства.

Для того, чтобы на виртуальной машине с Windows 10 было возможно использовать USB-флеш-накопитель для хранения ключевой информации необходимо установить пакет расширений от разработчика (рис. 19). Данное расширение позволит использовать в виртуальной машине устройства USB 2.0 и USB 3.0. Набор расширений можно установить по ссылке: www.virtualbox.org/wiki/Downloads. После установки расширений проверьте, чтобы в настройках виртуальной машины был включен соответствующий контроллер.

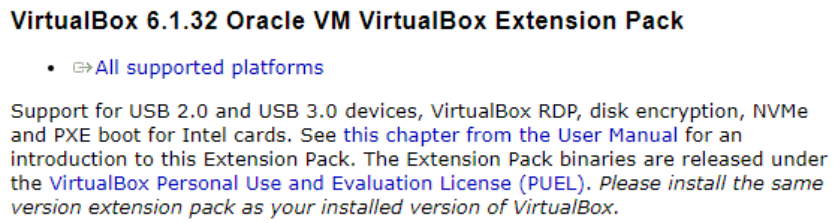

Рис. 119. Информация о расширении разрешений на сайте

Откройте инструмент «Шифрование диска BitLocker» и выполните команду «Включить BitLocker» для системного диска C.

Запустится проверка конфигурации компьютера, время выполнения которой может занимать несколько минут (рис. 20).

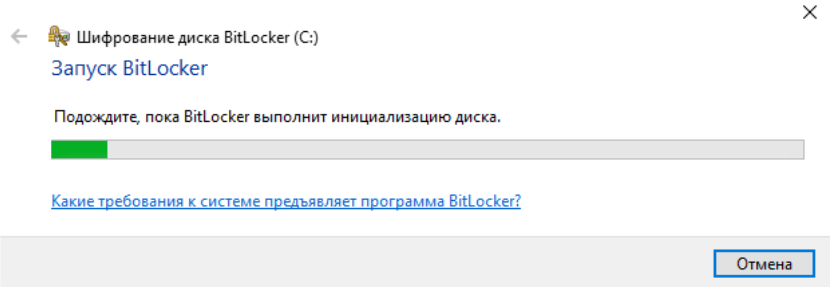

Рис. 20. Проверка конфигурации компьютера

После выполненной проверки конфигурации компьютера отобразится окно с перечнем вариантов способов разблокировки диска при запуске (рис. 21). Выберите пункт «Вставлять USB-устройство флэш-памяти».

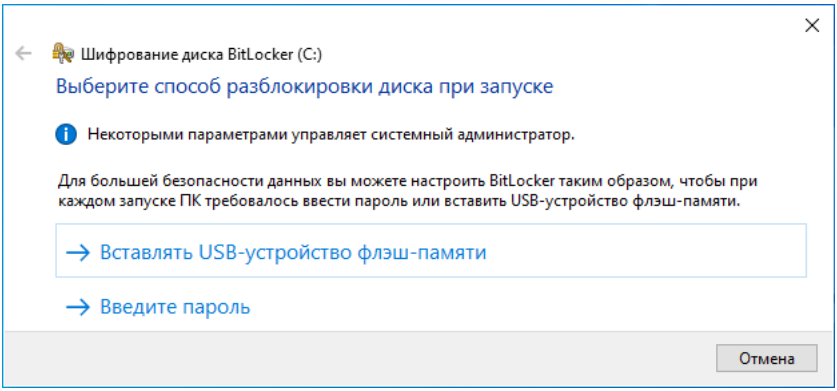

Рис. 21. Выбор способа разблокировки диска при запуске

Откроется окно выбора USB-устройств (рис. 22). Подключите USB-флэш-устройство и выберите его в данном списке.

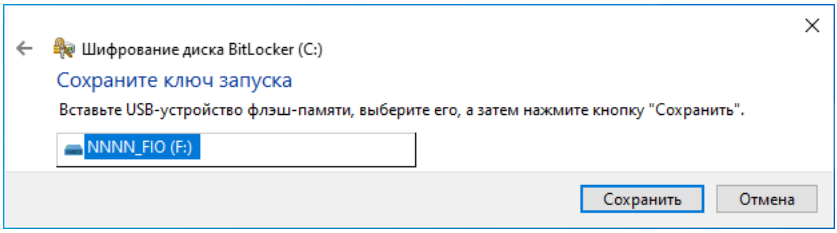

Рис. 22. Выбор флэш-устройства для сохранения ключа запуска

Затем будет предложен выбор способа сохранения ключа восстановления, необходимого для получения доступа к системному диску в случае утери USB-флеш-накопителя с ключом запуска (рис. 23).

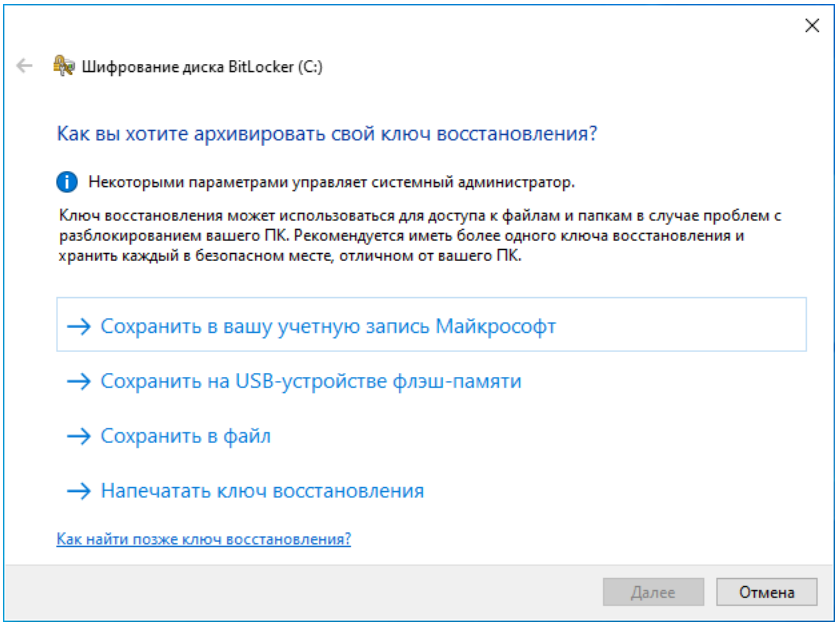

Рис. 23. Выбор места для архивации ключа восстановления

В качестве примера выберем то же устройство, на котором сохранили ключ для входа (рис. 24).

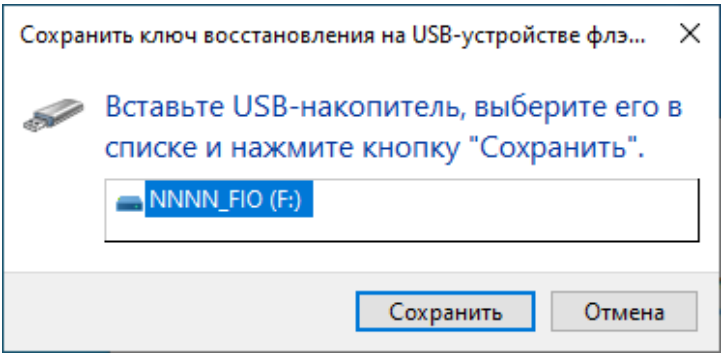

Рис. 23. Выбор USB-накопителя для архивации ключа восстановления

Откройте файл текстовый файл в корне выбранного USB-носителя. В нем можно ознакомиться с содержанием (рис. 24). Главный интерес для нас в данном случае представляет ключ восстановления. Он нам понадобится в случае, если не будет возможна загрузка с применением USB-носителя. Поэтому лучше его лучше сохранить на другом устройстве.

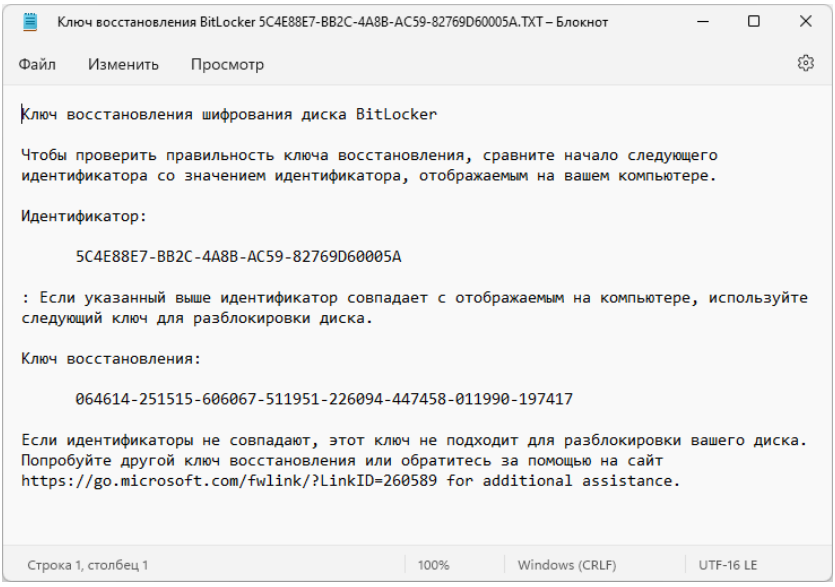

Рис. 24. Содержание файла с ключом восстановления

После этого будет необходимо выбрать то, какая часть диска будет зашифрована и какой для этого будет применяться режим шифрования. Аналогичные действия совершались ранее (рис. 9-10). Поскольку в данном случае мы работаем не с новым диском, то на данном этапе выберите «Шифровать весь диск». Выбор режима остается таким же, как и в предыдущем этапе – оптимальный для несъемных дисков.

Следующим этапом пользователю будет предложено запустить проверку системы BitLocker (рис. 25), для этого система выполнит перезагрузку. Данную проверку желательно произвести, чтобы потом не возникли ошибки после зашифрования системного диска.

Если BIOS компьютера поддерживает чтение USB-устройств в загрузочной среде, то запустится процедура шифрования системного диска. В противном случае (например, если выполнять данные действия на виртуальной машине) отобразится ошибка, и процедура шифрования будет отменена. По окончании проверки необходимо провести перезагрузку операционной системы (рис. 26).

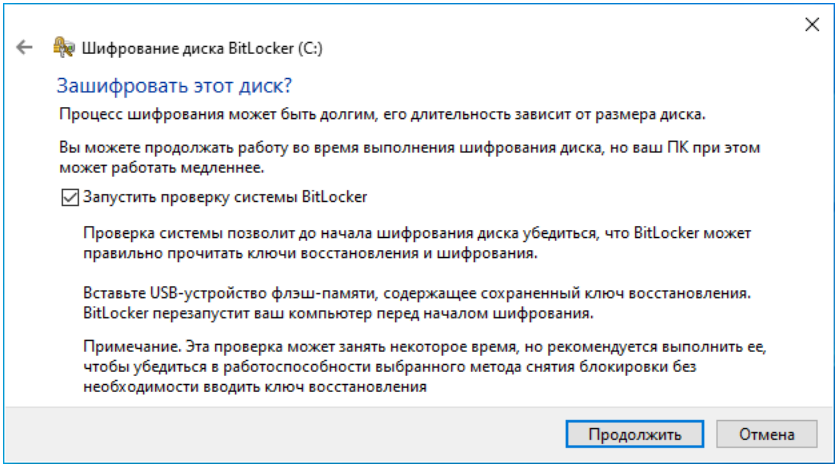

Рис. 25. Запрос необходимости проверки BitLocker

После зашифрования системного диска операционная система будет загружаться только при наличии вставленного USB-флеш-накопителя с ключом запуска во время загрузки системы. В качестве проверки не отключайте USB-флэш-накопитель при первой загрузке. В таком случае система загрузится без дополнительных уведомлений. В

меню BitLocker будет показано, что зашифрованы оба локальных диска (рис. 27).

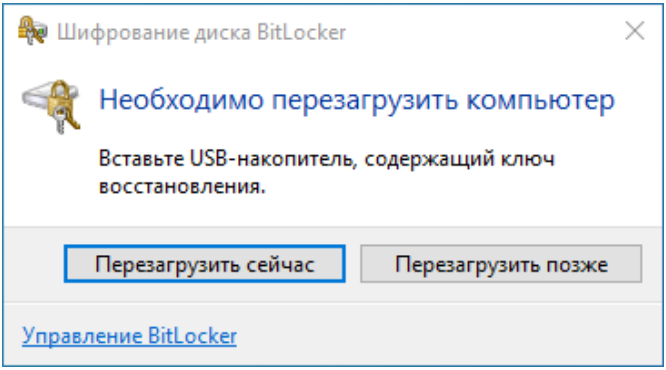

Рис. 26. Сообщение о необходимости перезагрузки

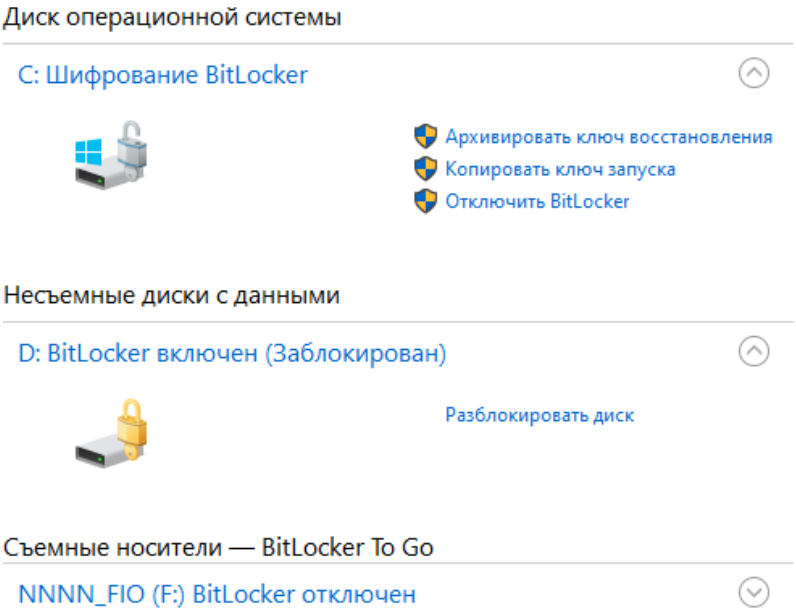

Рис. 27. Информация о шифровании дисков в BitLocker

Смоделируем ситуацию, при которой ключ запуска был по какой-либо причине утерян. В таком случае для загрузки системы можно воспользоваться ручным вводом 48-значного ключа восстановления. Отключите от виртуальной машины USB-флэш-накопитель с ключом запуска и перезагрузите виртуальную машину. В результате появится сообщение о необходимости подключения ключа (рис. 28).

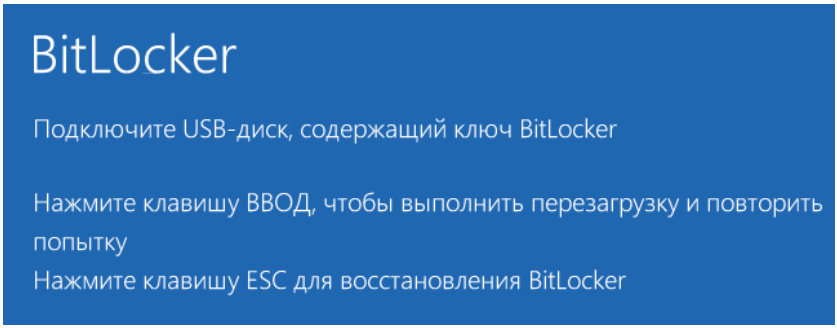

Рис. 28. Запрос ключа BitLocker

На этом этапе нам понадобится использовать полученный 48-значный ключ восстановления (recovery password). Обычно рекомендуется хранить его в любом месте, кроме жесткого диска той машины, системный диск которой был зашифрован. Поскольку в данном случае мы сохранили его на съемном носителе, то можем прочитать содержимое на другом устройстве (в случае с виртуальной машиной на гостевой ОС).

В случае, если подключить USB-диск с ключом, то потребуется нажать клавишу «Enter» для перезагрузки системы. Операционная система запустится.

Если же по какой-либо причине был утерян ключ запуска или сам носитель с ключом запуска, то можно воспользоваться ключом восстановления. Для этого снова отсоедините USB-диск с ключом и перезагрузите систему.

В окне запроса носителя с ключом запуска нажмите Esc. Откроется окно с вводом ключа восстановления. Введите 48-значный ключ восстановления, указанный системой до выполнения шифрования системного диска (рис. 29). После ввода правильного ключа восстановления выполнится запуск операционной системы.

Рис. 29. Вход по 48-значному ключу восстановления

4. Задание на лабораторную работу

1. Создайте второй локальный диск на виртуальной машине и зашифруйте его с помощью BitLocker.
2. Зашифруйте системный диск с применением usb-носителя для хранения ключа запуска.
3. Проверьте возможность запуска операционной системы с подключенным и отсутствующим носителем ключа запуска.
4. Составьте по проделанной работе отчет.

5. Контрольные вопросы

1. В каких выпусках операционных систем Windows присутствует технология шифрования дисков BitLocker?
2. В чем отличие BitLocker от шифрованной файловой системы?
3. Какие режимы работы системы шифрования возможны для шифрования системных дисков?
4. Что такое TPM?
5. Какие носители можно использовать для сохранения ключа запуска?

Указания для организации самостоятельной работы

Целями самостоятельной работы являются систематизация, расширение и закрепление теоретических знаний. Самостоятельная работа студента по дисциплине «Прикладная криптография» включает следующие виды активности:

1. Изучение тем теоретической части дисциплины, вынесенных для самостоятельной проработки.
2. Подготовка к лабораторным и практическим работам.
3. Подготовка реферата.
4. Выполнение индивидуальных заданий.

Изучение тем теоретической части дисциплины осуществляется на основе материала лекционных занятий. В рамках выполнения подготовки к лабораторным работам рекомендуется детально познакомиться с теоретическим материалом по темам лабораторных работ, а также с последовательностью действий выполнения лабораторных работ, указанных в методических указаниях.