Министерство науки и высшего образования РФ

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

А.Ю. Якимук

ПРИКЛАДНАЯ КРИПТОГРАФИЯ

Лабораторный практикум
для студентов специальностей и направлений
10.03.01 – «Информационная безопасность»,
10.05.02 – «Информационная безопасность
телекоммуникационных систем»,
10.05.03 – «Информационная безопасность
автоматизированных систем»,
10.05.04 – «Информационно-аналитические системы безопасности»

В-Спектр
Томск, 2022

УДК 004.056
ББК 32.973.26-018.2
К 64

К 64 **Якимук А.Ю.** Прикладная криптография: лабораторный практикум. – Томск: В-Спектр, 2022. – 195 с.
ISBN 978-5-91191-322-9

Практикум содержит описания лабораторных работ по дисциплине «Прикладная криптография» для специальностей 10.05.02 – «Информационная безопасность телекоммуникационных систем», 10.05.03 – «Информационная безопасность автоматизированных систем», 10.05.04 – «Информационно-аналитические системы безопасности» и направления 10.03.01 – «Информационная безопасность», задания, методические указания по выполнению, требования по представлению отчётности, вопросы для самоконтроля.

УДК 004.056
ББК 32.973.26-018.2

ISBN 978-5-91191-322-9

СОДЕРЖАНИЕ

ЛАБОРАТОРНАЯ РАБОТА №1
Шифрованная файловая система Windows

1. Цель работы

Целью лабораторной 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.

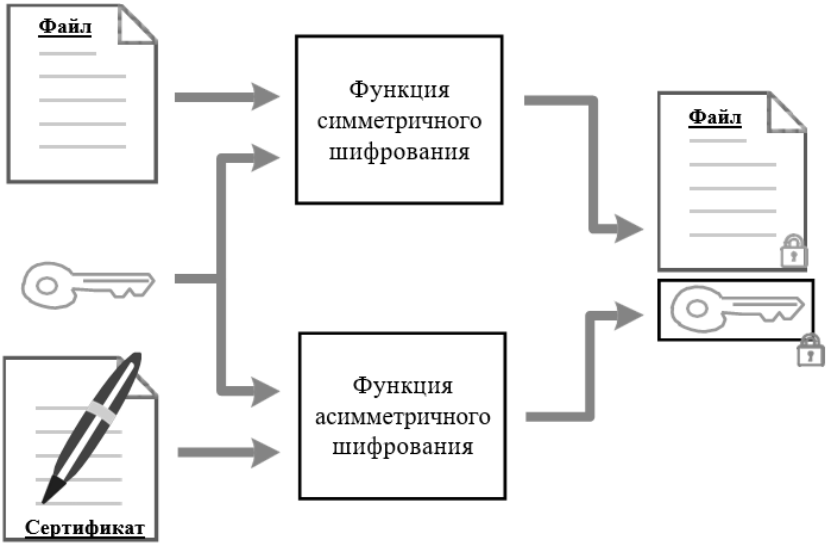

Рис. 1. Схема зашифрования файла

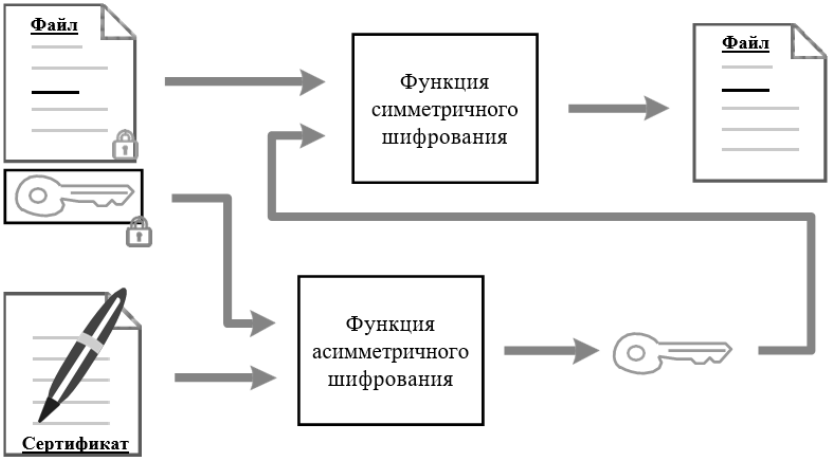

Рис. 2. Схема расшифрования файла

3. Ход работы

3.1 Шифрованная файловая система

Данная лабораторная 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.

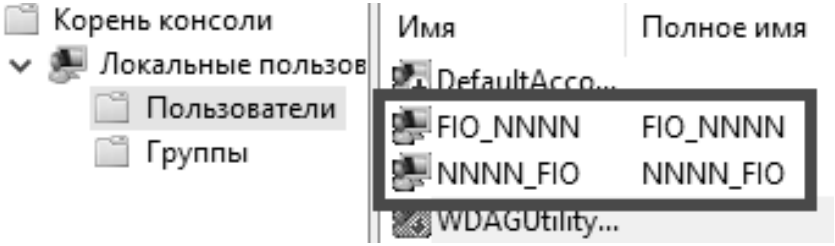

Рис. 3. Созданные пользователи для лабораторной работы

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.

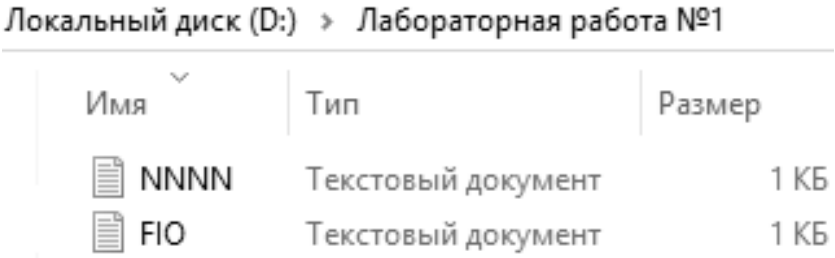

Рис. 4. Схема расшифрования файла

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).

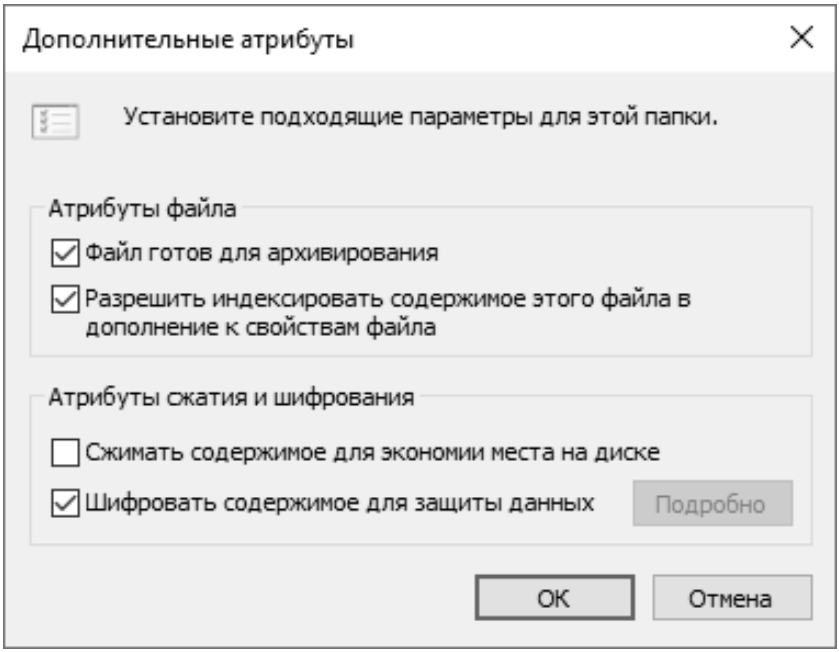

Рис. 5. Настройка атрибутов для шифрования файла

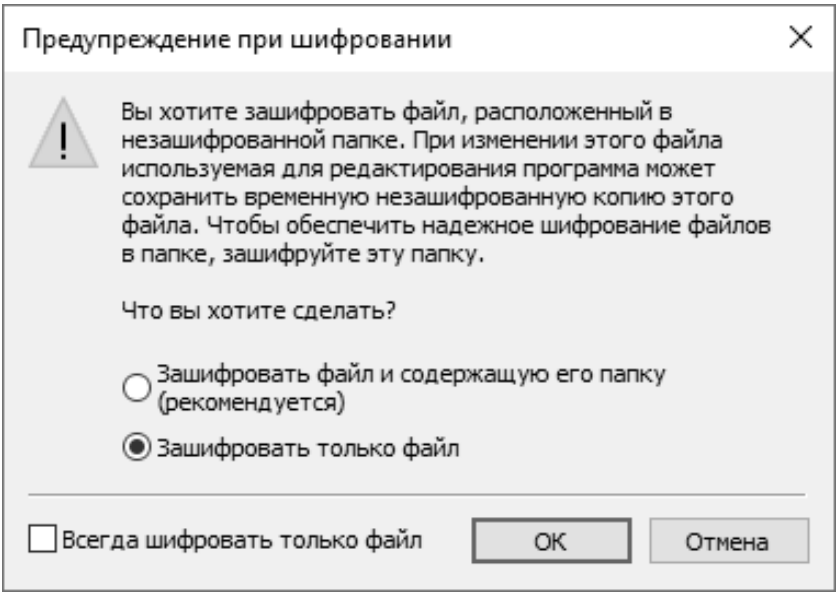

Рис. 6. Дополнительный запрос при шифровании файла

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

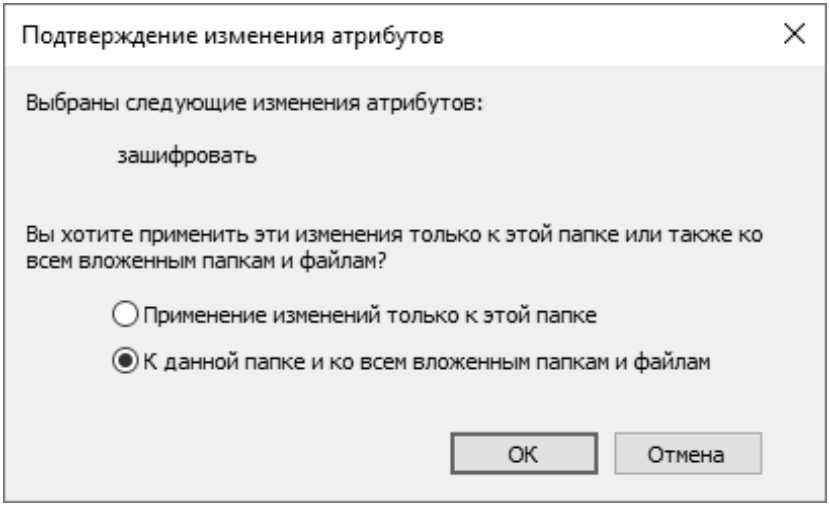

Рис. 7. Дополнительный запрос при шифровании папки

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».

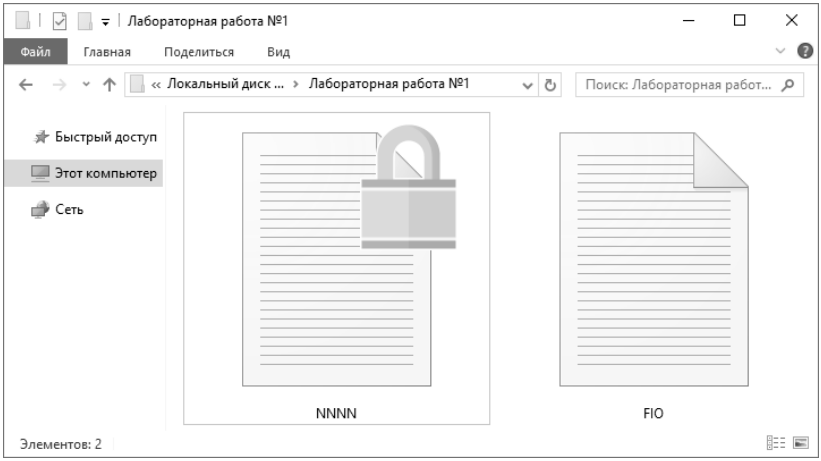

Рис.8. Вид файла с включенным шифрованием

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».

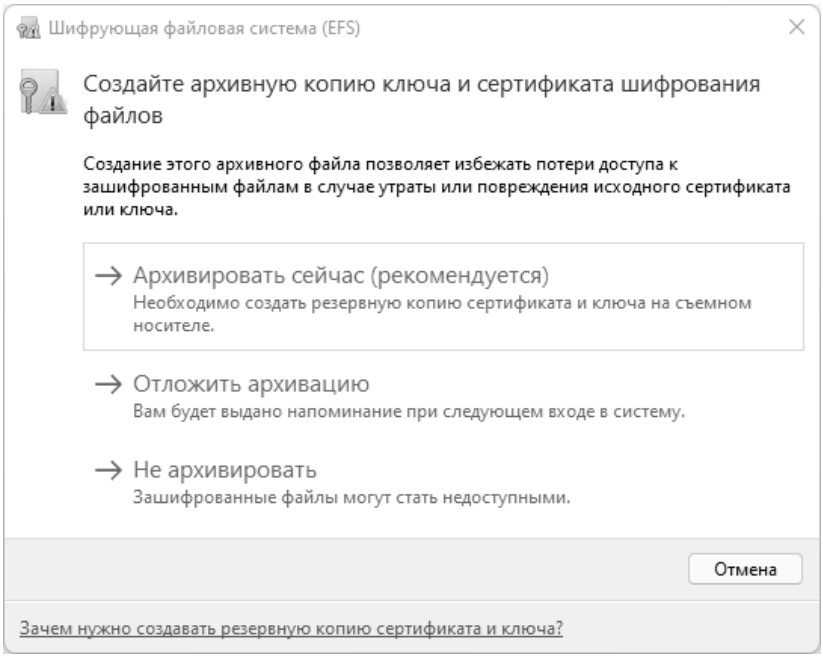

Рис.9. Вид файла с включенным шифрованием

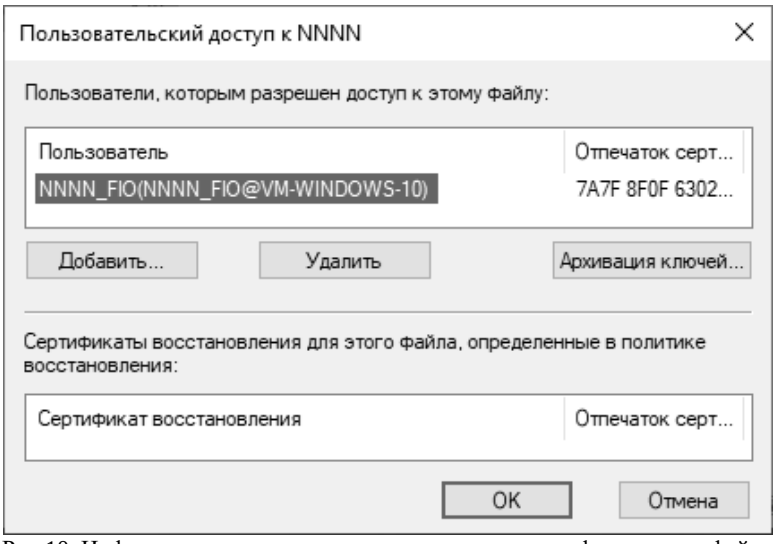

Рис.10. Информация о предоставленном доступе к зашифрованному файлу

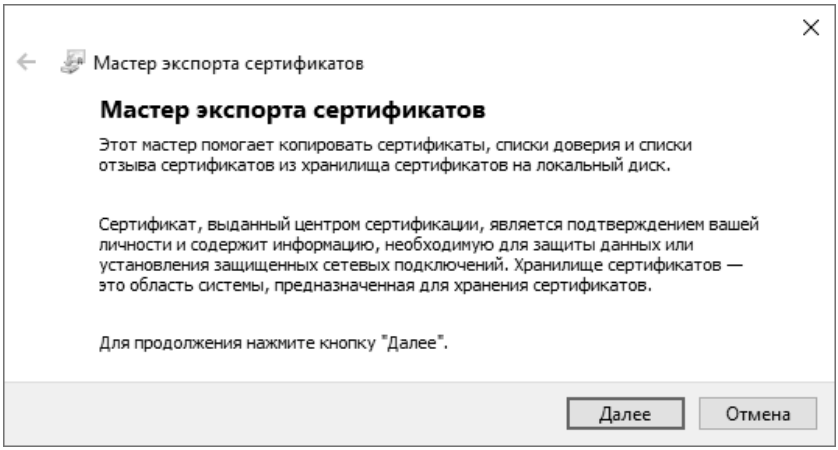

Рис.11. Мастер экспорта сертификатов

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.

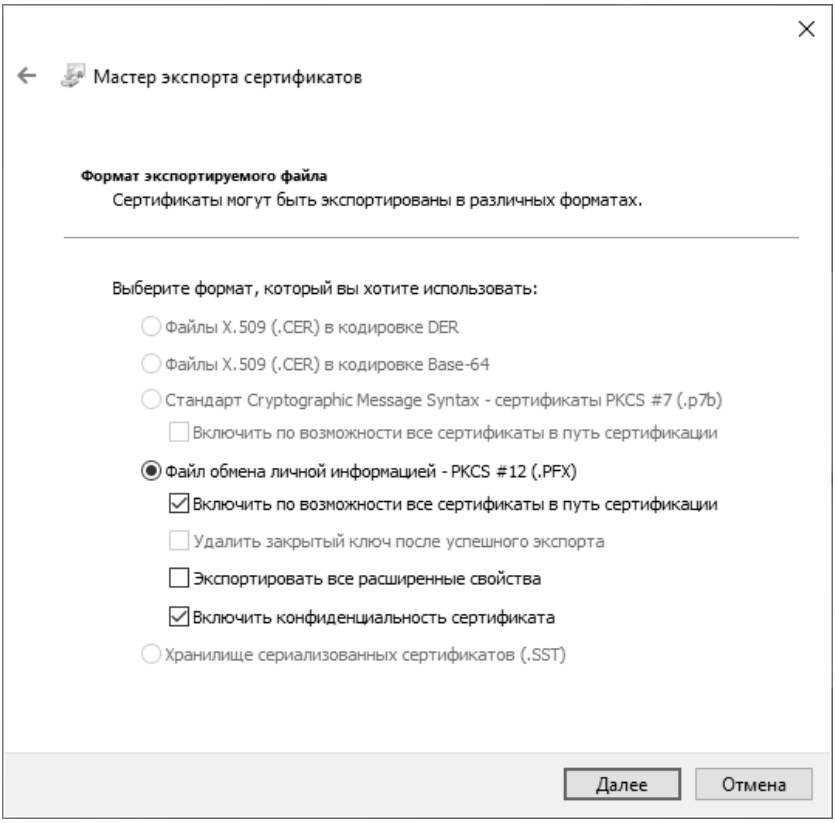

Рис.12. Формат файла экспортируемого сертификата

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.

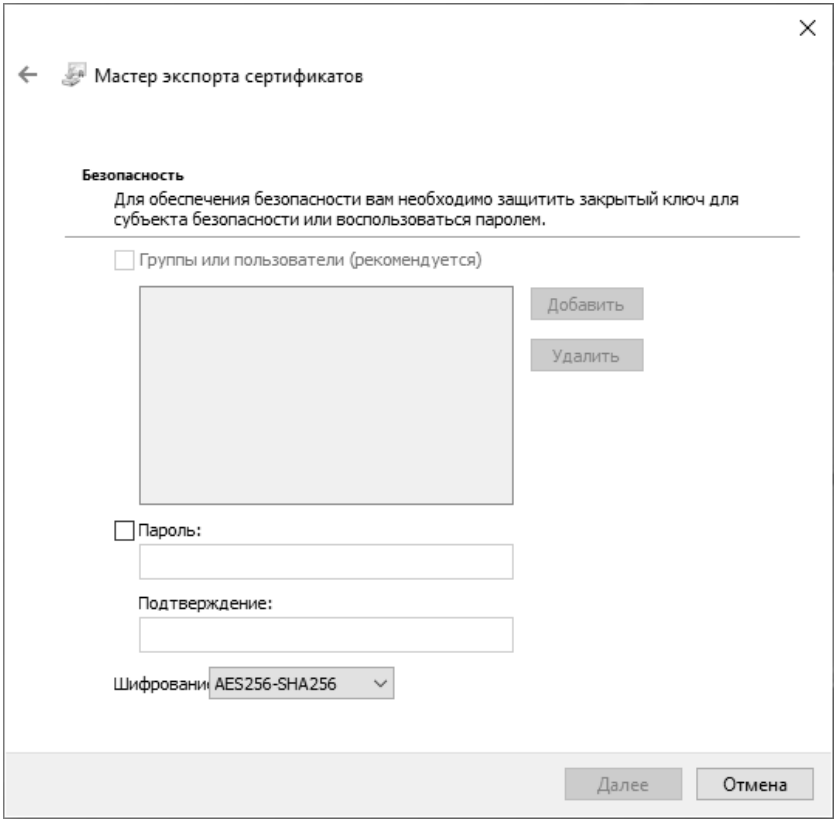

Рис.13. Защита закрытого ключа для субъекта безопасности

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).

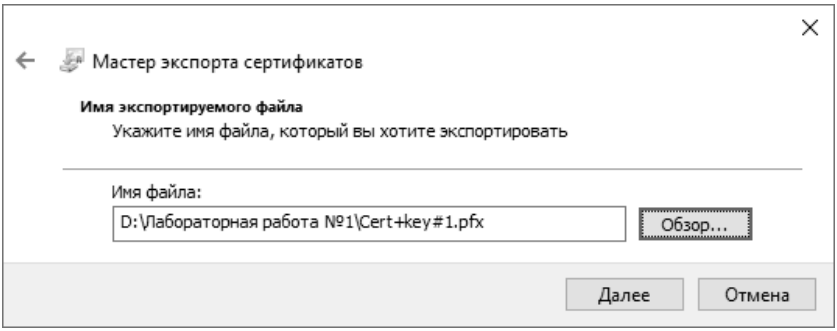

Рис.14. Защита закрытого ключа паролем

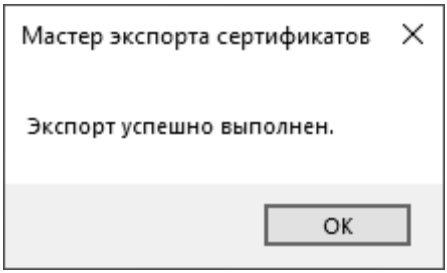

Рис.15. Уведомление об успешном экспорте сертификата

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).

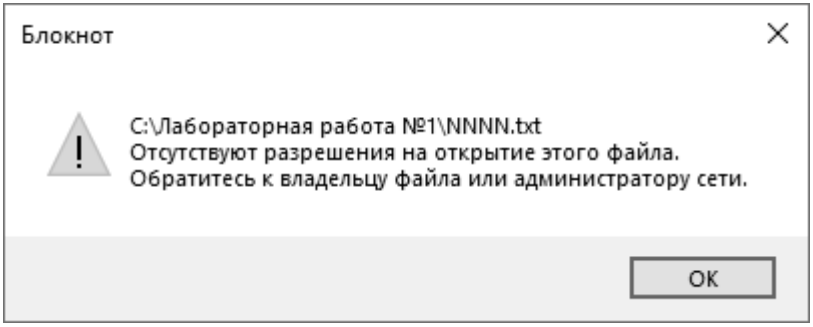

Рис.16. Уведомление об отказе в доступе

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).

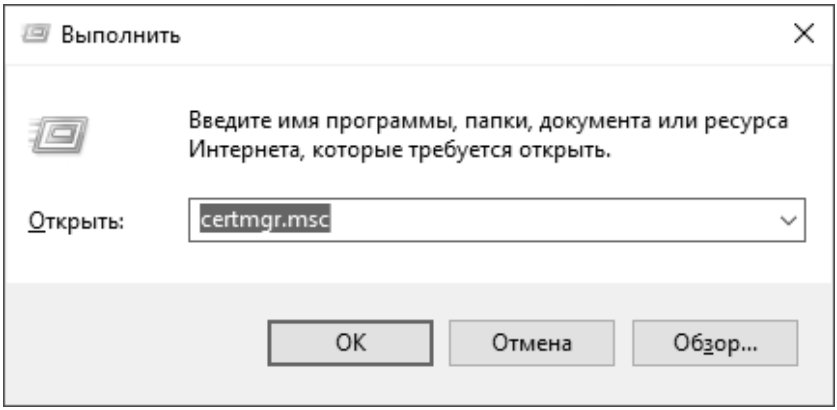

Рис.17. Вызов оснастки управления хранилищем сертификатов

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

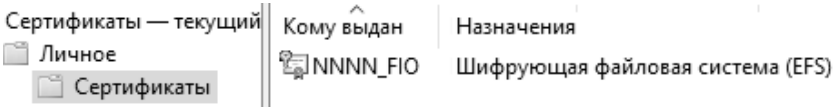

Рис.18. Сертификат первого пользователя в хранилище

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).

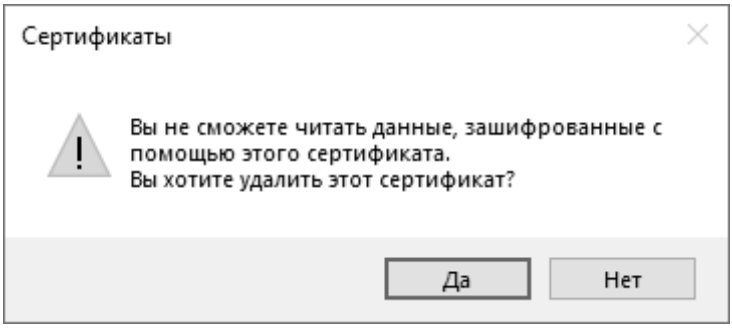

Рис.19. Предупреждение о последствиях удаления сертификата

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).

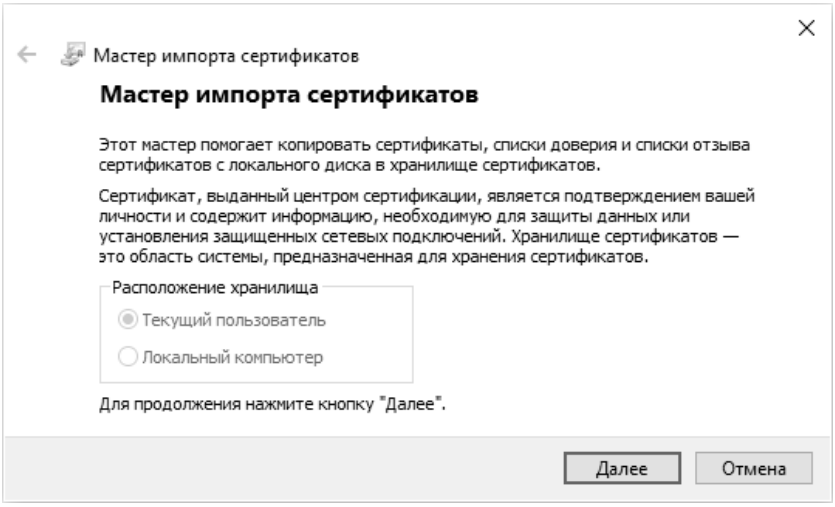

Рис.20. Мастер импорта сертификатов

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).

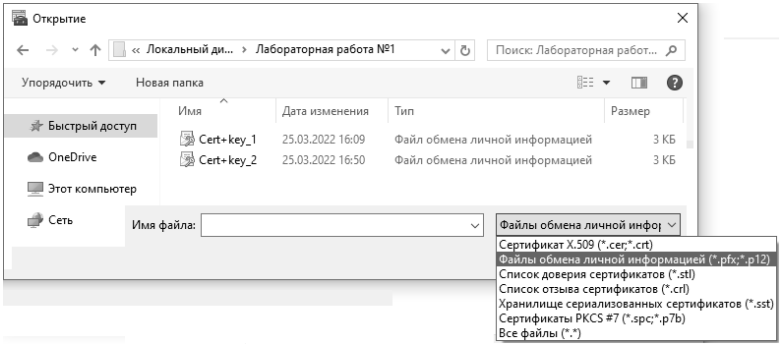

Рис.21. Выбор восстанавливаемого сертификата

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

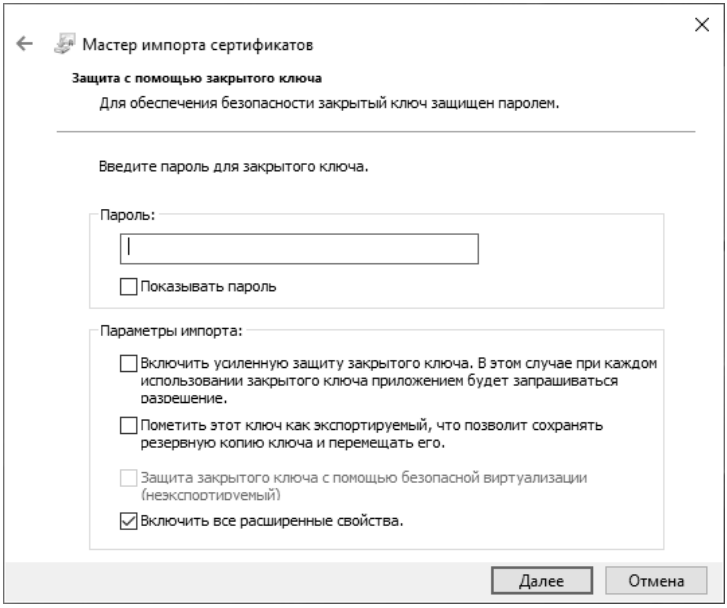

Рис.22. Ввод пароля для восстановления сертификата

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

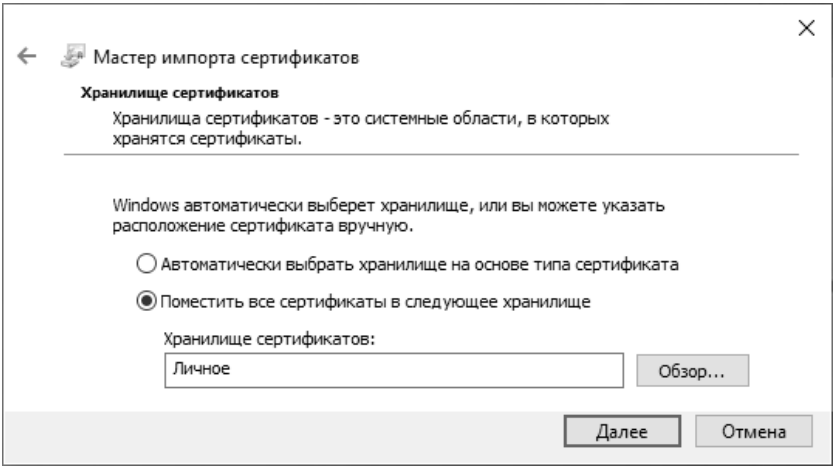

Рис.23. Выбор хранилища для импорта сертификата

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

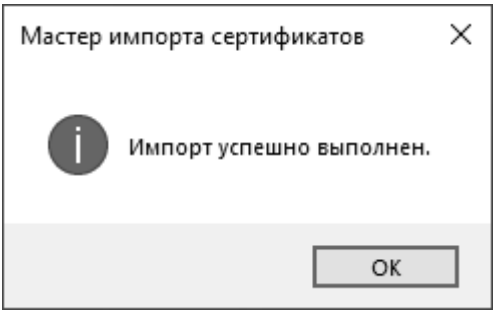

Рис.24. Уведомление об успешном импорте сертификата

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).

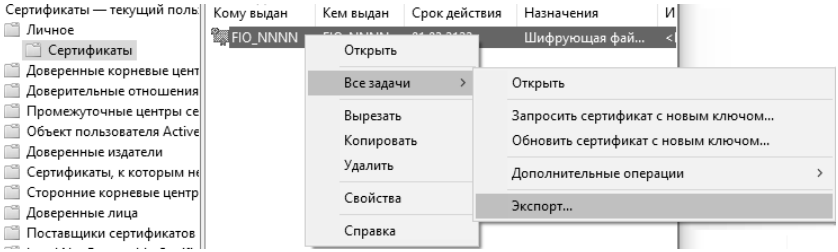

Рис.25. Экспорт сертификата второго пользователя

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

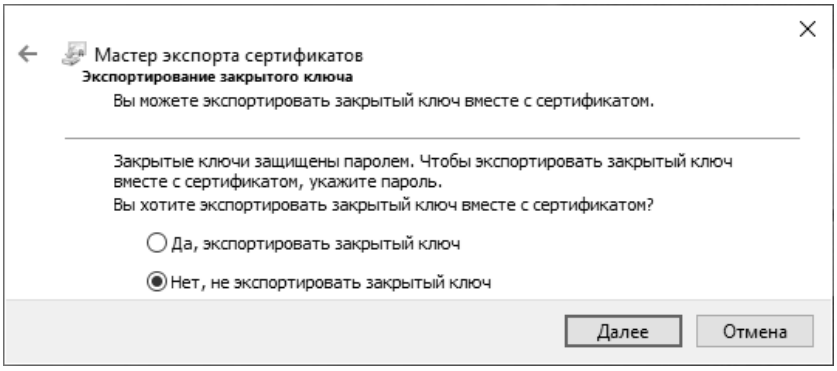

Рис.26. Экспорт сертификата без закрытого ключа

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).

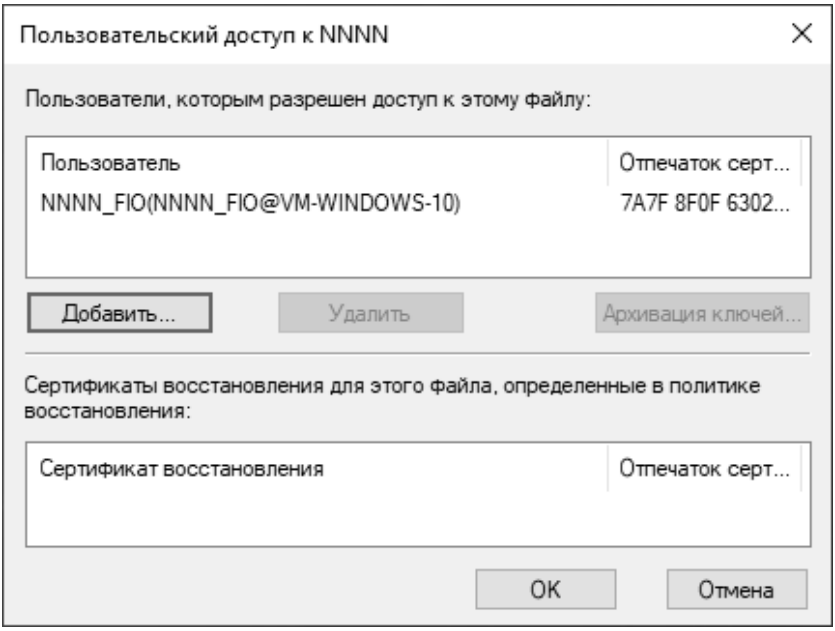

Рис.27. Настройка доступа к первому файлу

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

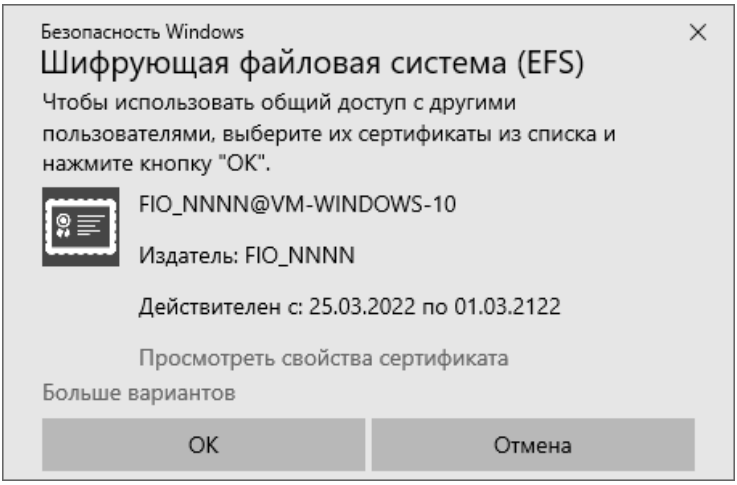

Рис.28. Добавление сертификата второго пользователя

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 лабораторной 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 используется симметричное шифрование?
4. Для чего в шифрованной файловой системе используется асимметричное шифрование?
5. Опишите алгоритм работы шифрованной файловой системы Windows.
6. Для чего нужно архивировать закрытый ключ и сертификат пользователя?
7. Что такое PKCS?
8. Для чего используется PKCS#12?
9. Каким образом можно предоставить доступ к зашифрованному файлу другому пользователю?
10. В каких форматах можно экспортировать сертификат из локального хранилища без экспорта закрытого ключа?

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 лабораторная 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 лабораторной 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).

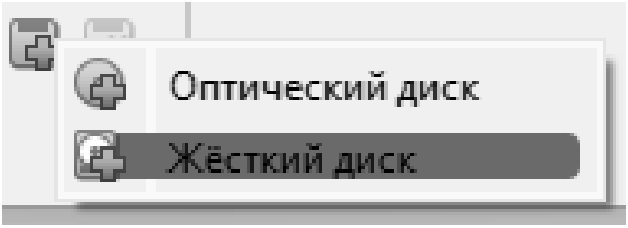

Рис. 2. Добавление второго жесткого диска

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.

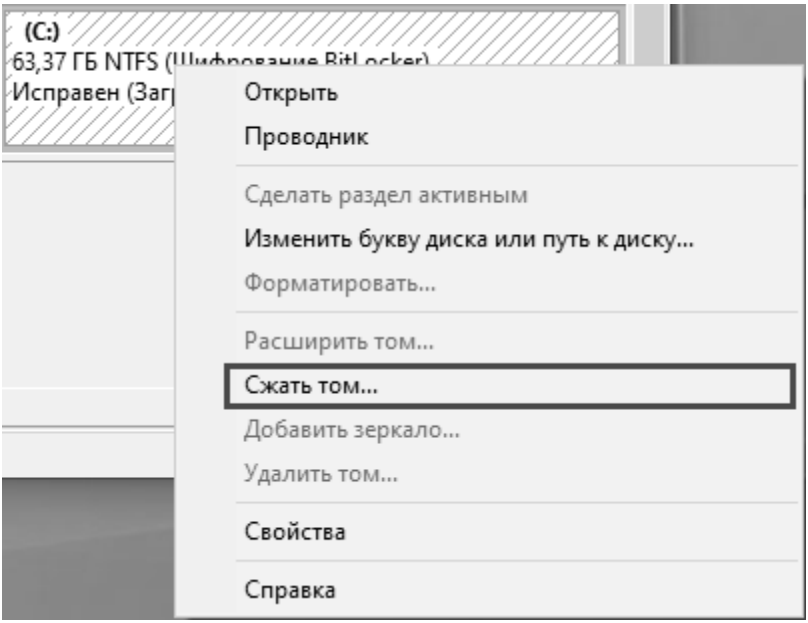

Рис. 2. Вызов функции сжатия тома

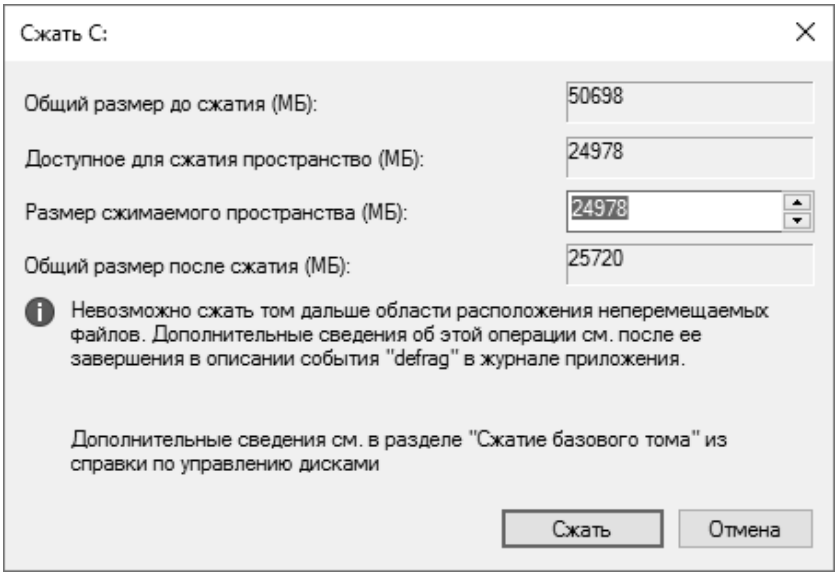

Рис. 3. Определение степени сжатия тома и объем освобожденного места

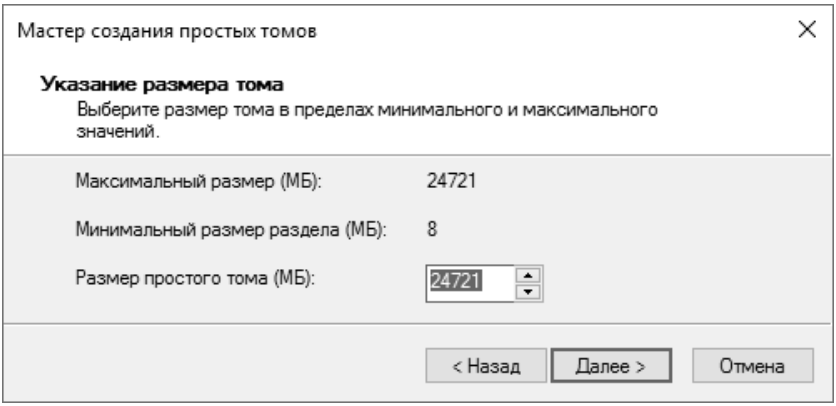

Рис. 4. Создание тома из освобожденного места

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).

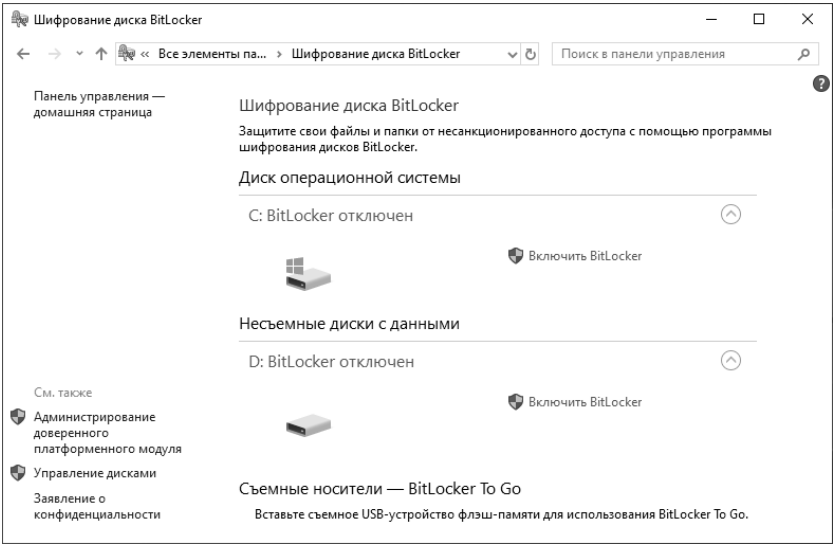

Рис. 5. Инструмент Windows «Шифрование диска BitLocker»

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).

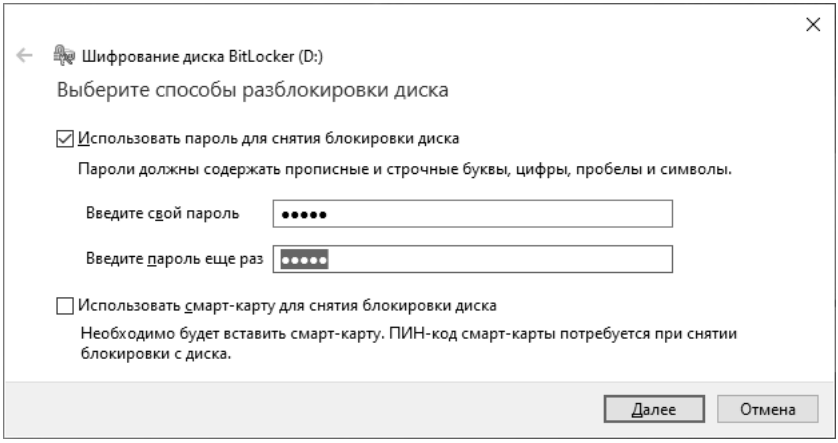

Рис. 6. Ввод пароля для блокировки диска

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

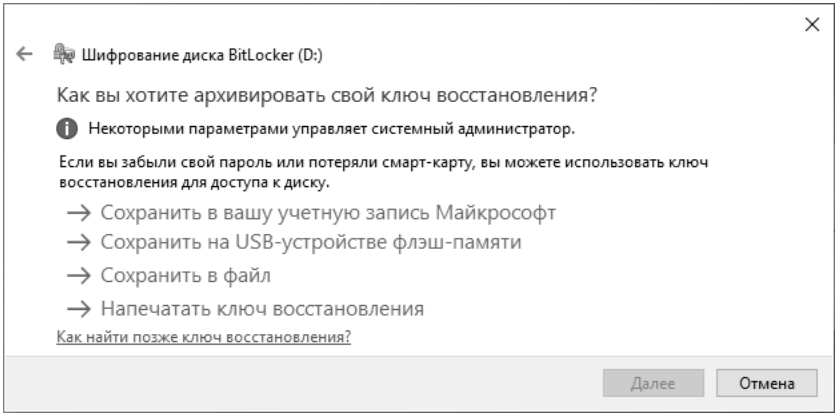

Рис. 7. Выбор варианта архивации ключа восстановления

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

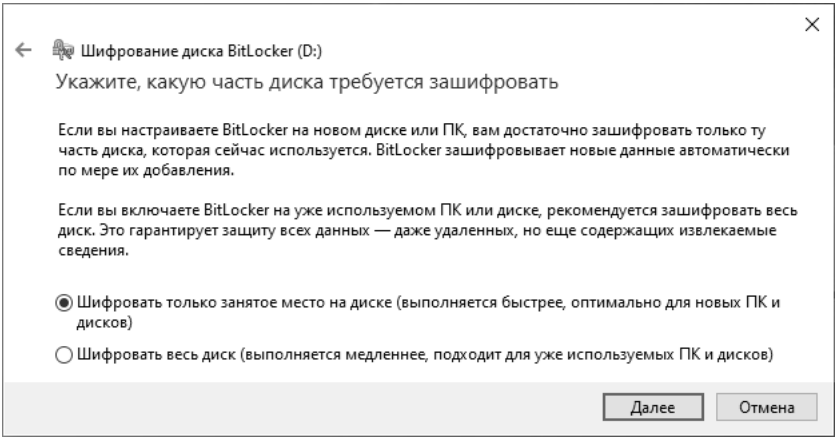

Рис. 8. Выбор варианта шифрования диска

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».

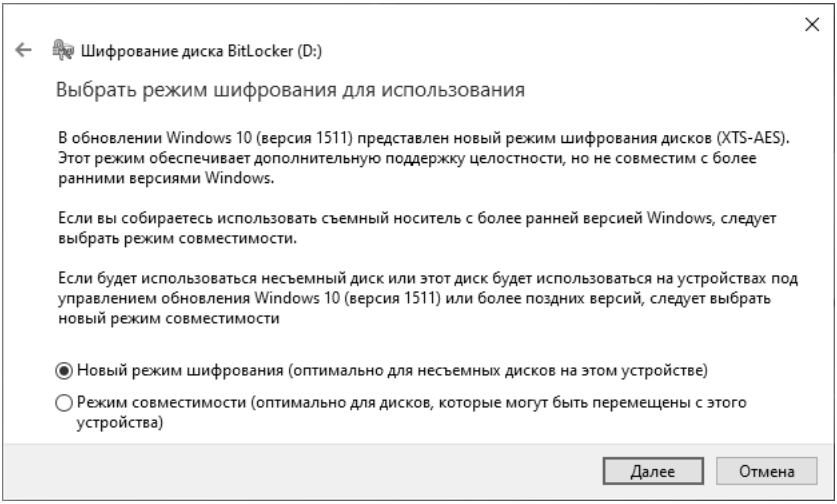

Рис. 9. Выбор режима шифрования диска

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

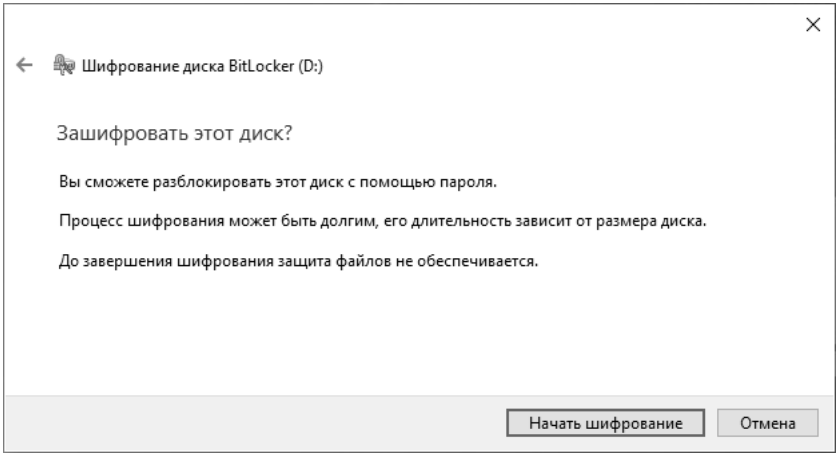

Рис. 10. Инструмент Windows «Шифрование диска BitLocker»

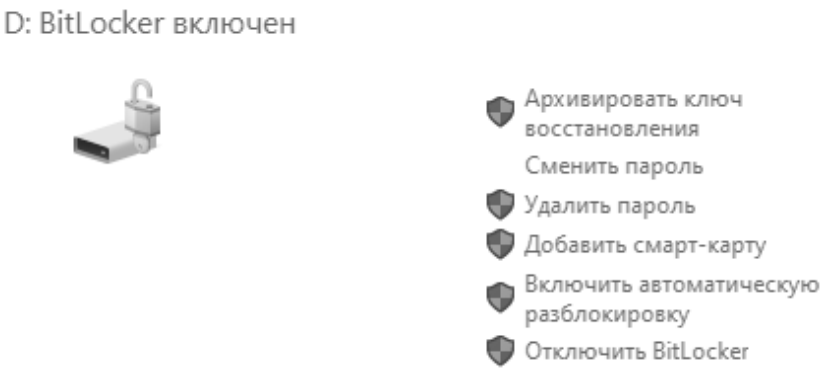

Рис. 31. Информация о включении BitLocker для диска D

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).

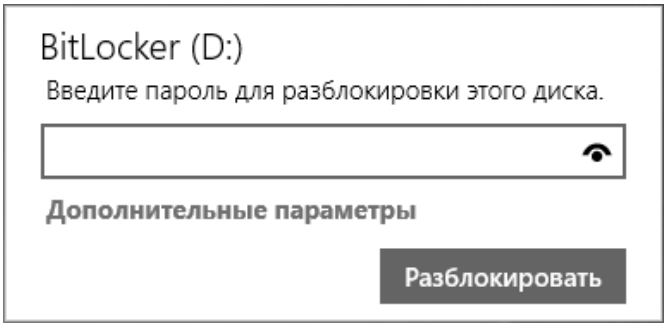

Рис. 53. Запрос на ввод пароля для снятия блокировки диска

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).

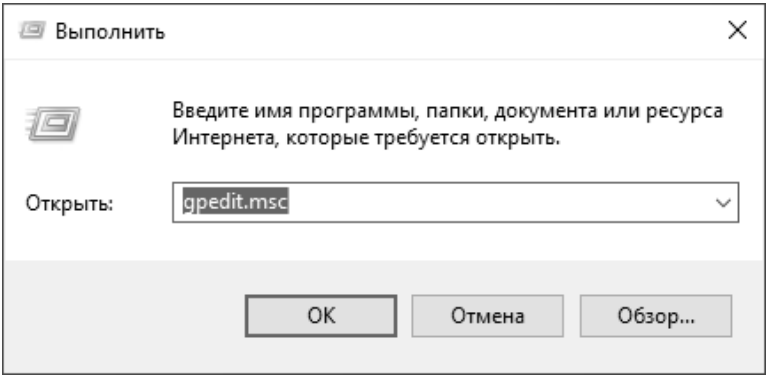

Рис. 75. Вызов оснастки редактора локальной групповой политики

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).

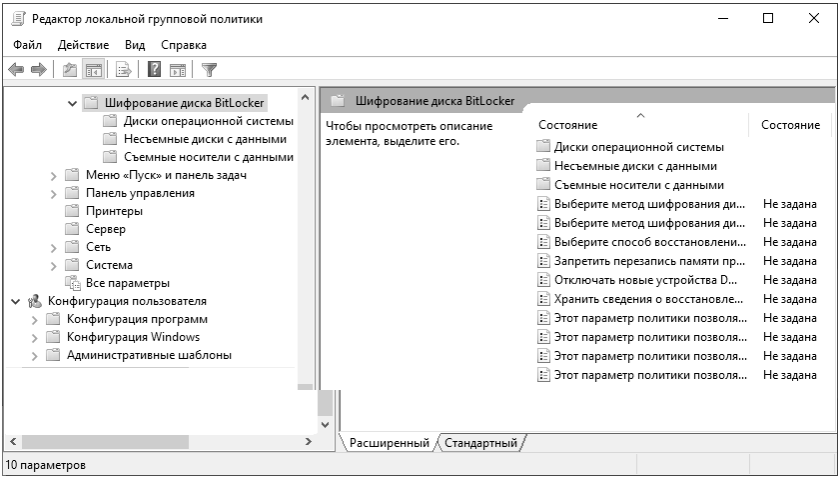

Рис. 86. Меню «Шифрование диска BitLocker» в групповых политиках

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

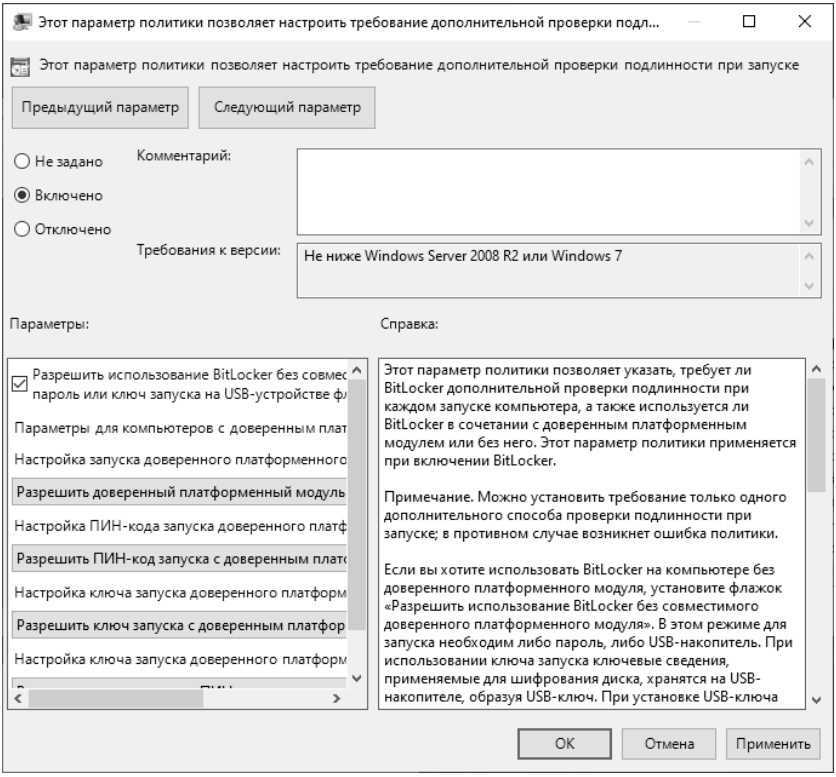

Рис. 97. Включение использования BitLocker без совместимого TPM

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.

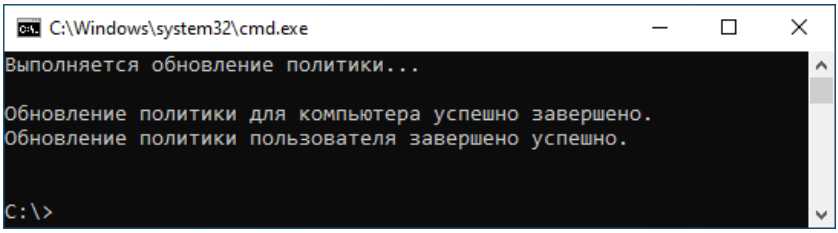

Рис. 108. Применение новых настроек групповых политик

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.

VirtualBox 6.1.32 Oracle VM VirtualBox Extension Pack

- ⇨All supported platforms

Support for USB 2.0 and USB 3.0 devices, VirtualBox RDP, disk encryption, NVMe and PXE boot for Intel cards. See this chapter from the User Manual for an introduction to this Extension Pack. The Extension Pack binaries are released under the VirtualBox Personal Use and Evaluation License (PUEL). *Please install the same version extension pack as your installed version of VirtualBox.*

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).

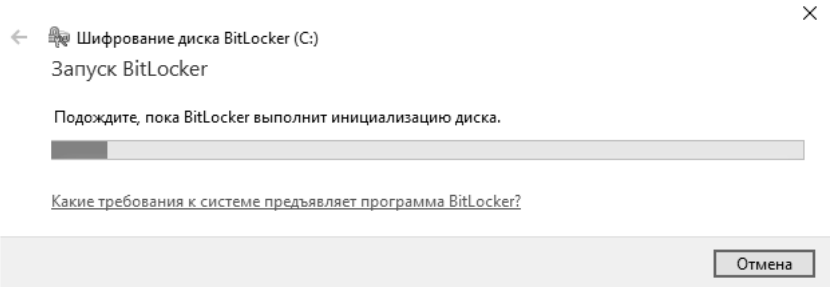

Рис. 20. Проверка конфигурации компьютера

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

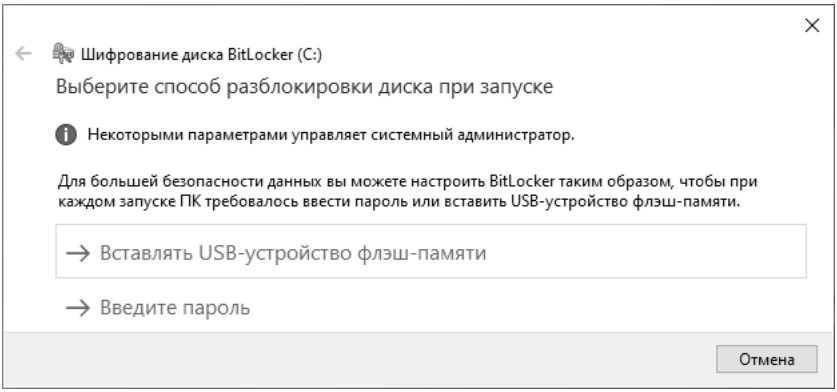

Рис. 21. Выбор способа разблокировки диска при запуске

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

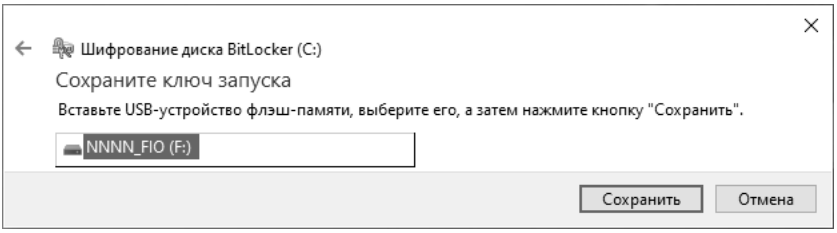

Рис. 22. Выбор флэш-устройства для сохранения ключа запуска

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).

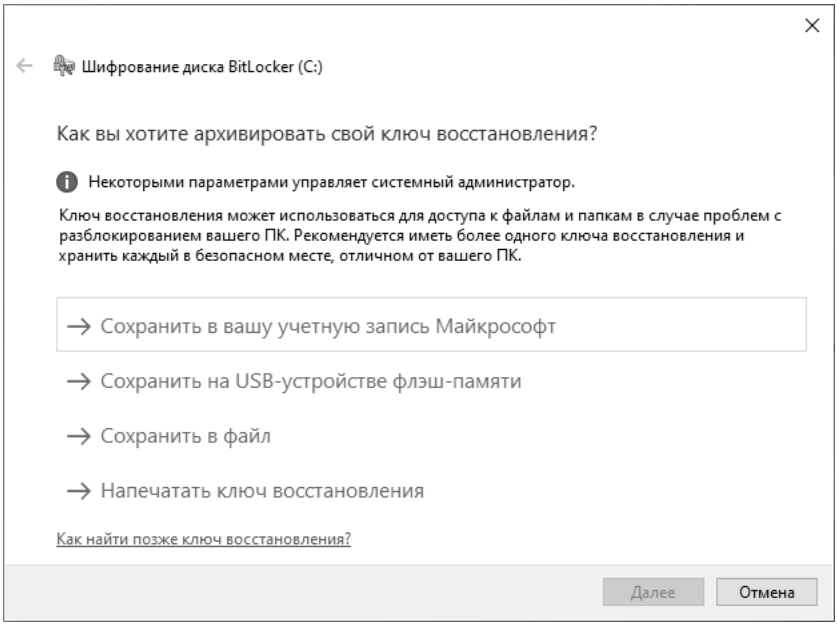

Рис. 23. Выбор места для архивации ключа восстановления

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

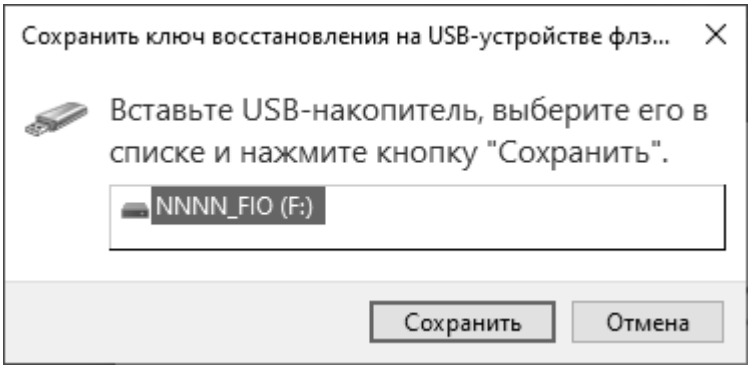

Рис. 23. Выбор USB-накопителя для архивации ключа восстановления

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.

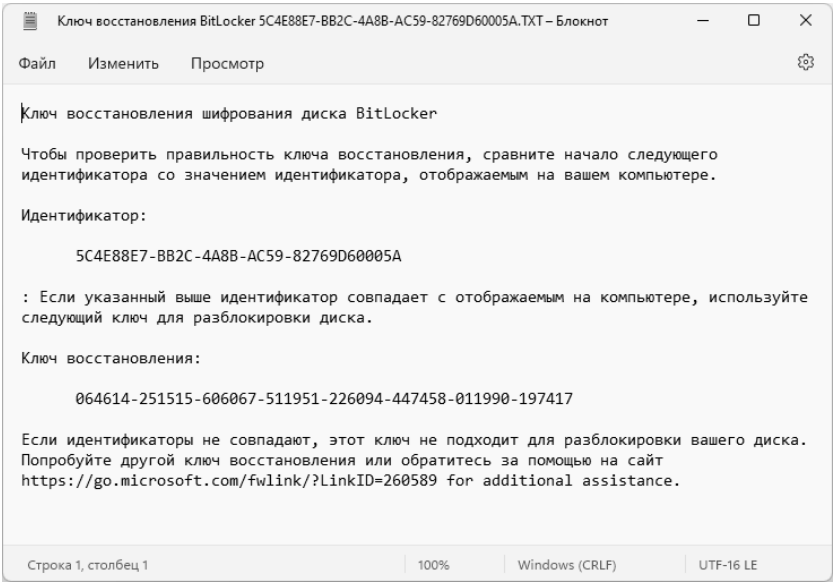

Рис. 24. Содержание файла с ключом восстановления

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).

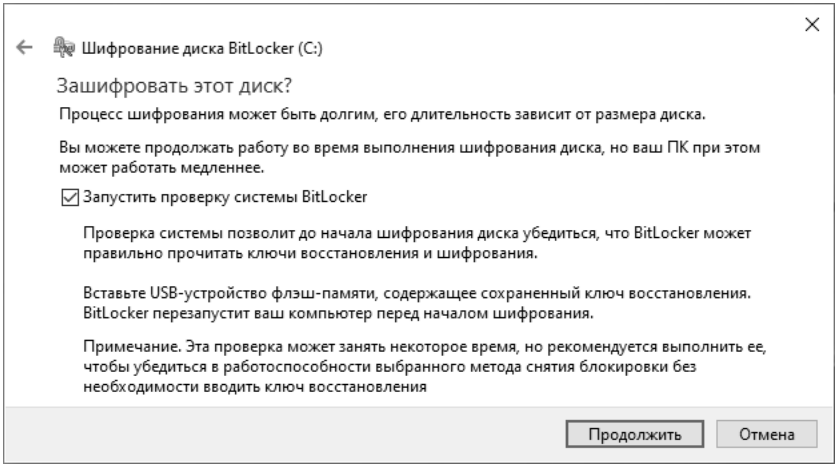

Рис. 25. Запрос необходимости проверки BitLocker

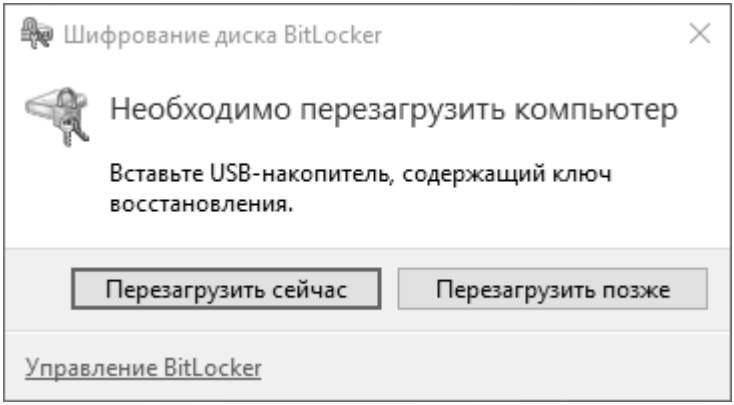

Рис. 26. Сообщение о необходимости перезагрузки

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).

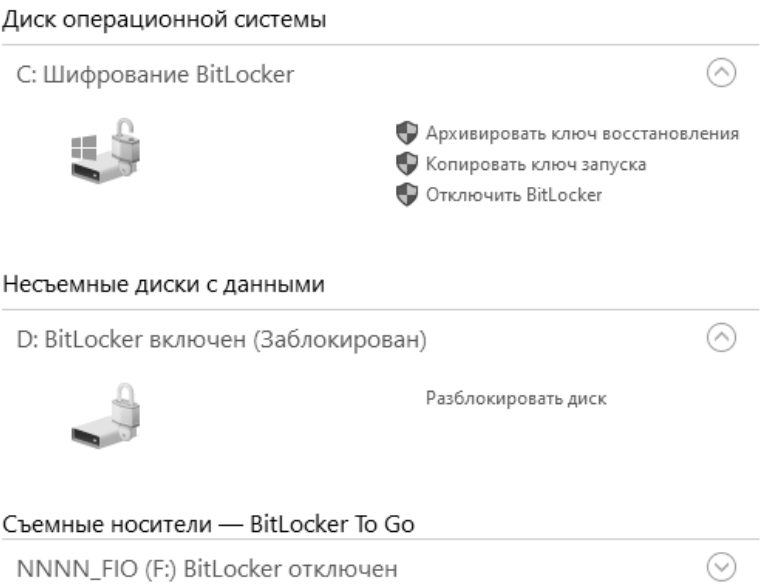

Рис. 27. Информация о шифровании дисков в BitLocker

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).

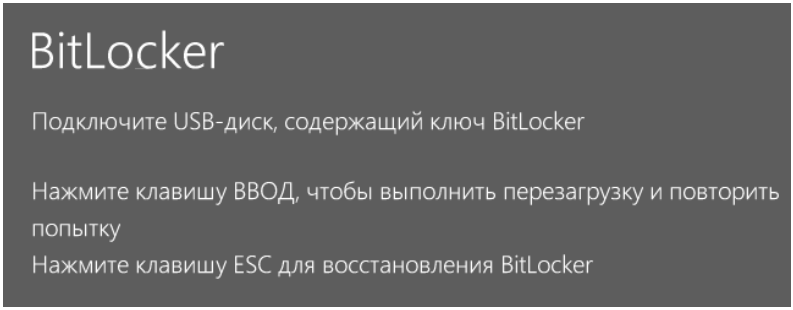

Рис. 28. Запрос ключа BitLocker

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. Какие файловые системы могут использоваться на внешних устройствах, чтобы их можно было применить с технологией BitLocker?

3. В чем отличие BitLocker от шифрованной файловой системы?

4. Какой алгоритм шифрования применяется в BitLocker?

5. Для чего используется функция BitLocker To Go?

6. Какие режимы работы системы шифрования возможны для шифрования системных дисков?

7. Что такое TPM?

8. Какие носители можно использовать для сохранения ключа запуска?

9. Объясните отличие между ключом запуска и ключом восстановления.

10. Каким образом можно восстановить доступ к операционной системе, установленной на зашифрованном с помощью BitLocker локальном диске, в случае утери носителя с ключом запуска?

ЛАБОРАТОРНАЯ РАБОТА №3
Шифрование диска VeraCrypt

1. Цель работы

Целью лабораторной работы является изучение средства шифрования информации «на лету» с применением стороннего программного обеспечения.

2. Краткие теоретические сведения

VeraCrypt – бесплатное программное обеспечение с открытым исходным кодом для шифрования файлов и дисков, использующая шифрование «на лету». Программа была создана на основе исходного кода программы TrueCrypt, которая когда-то была популярна, но проект был закрыт. На рис. 1 показан общий вид интерфейса программы.

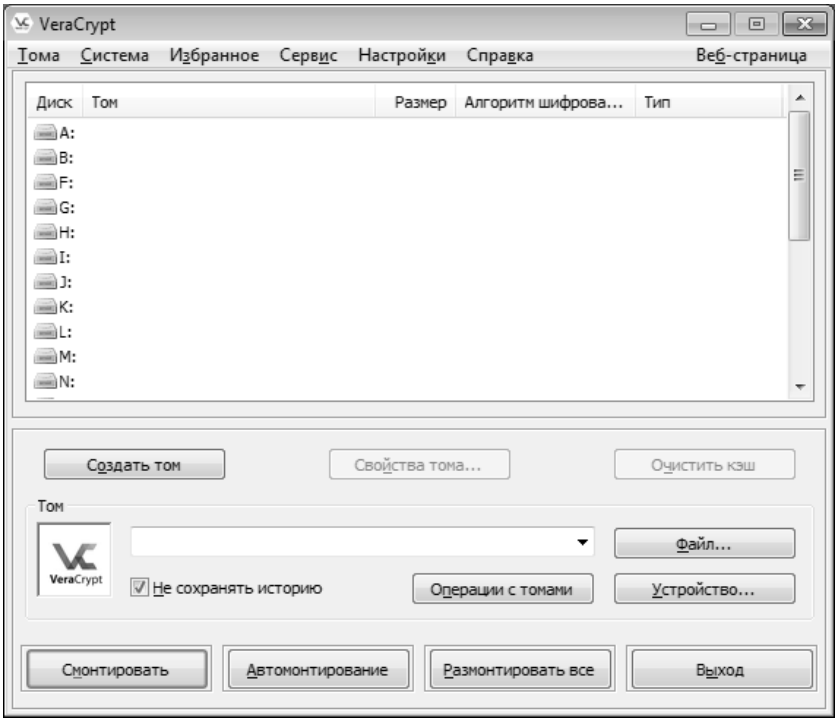

Рис. 12. Общий вид программы при первом запуске

Программа работает под операционными системами семейства Windows, Linux, MacOS X, FreeBSD 11. Выпускаются версии для установки и портативные, что не только упрощает работу с программой за счет кроссплатформенности и быстроты установки на новой системе, но и позволяет сразу избавиться от нее после завершения работы, что усложняет установку факта шифрования ею.

VeraCrypt использует следующие алгоритмы шифрования: AES, Serpent, Twofish, Camellia, Кузнечик, а также комбинации этих алгоритмов. Используемые криптографические хеш-функции: RIPEMD-160, SHA-256, SHA- 512, Стрибог и Whirlpool. Ключ заголовка и вторичный ключ заголовка для режима XTS генерируются при помощи алгоритма PBKDF2 с использованием 512-битной криптографической соли, число итераций составляет от 327 661 до 655 331, в зависимости от используемой хеш-функции. Это позволяет выбрать пользователю предпочитаемый алгоритм шифрования и балансировать между производительностью и сложностью криптографических преобразований.

Программа может создавать файловые контейнеры и шифровать диски целиком, при этом имеется возможность создать дополнительно скрытые контейнеры и тома, которые будут находиться внутри других зашифрованных контейнерах и томах. Это позволяет выдать ключ для расшифрования файлов злоумышленнику, но при этом важные файлы будут все еще находиться в безопасности.

Также возможно зашифровать системный диск и создать скрытую операционную систему. В случаи вынужденной выдачи пароля можно будет выдать пароль от операционной системы, которая не представляет ценности, в то время как ваши файлы останутся в безопасности.

Для расшифровывания может использоваться пароль или ключевой файл.

3. Ход работы

3.1 Создание зашифрованного файлового контейнера

Для создания зашифрованного файлового контейнера перейдите в меню «Программы» и в разделе «Тома» выберите операцию «Создать новый том» (рис. 2). В программе файловые контейнеры называются томами.

После этого высветится окно создания томов. Выберите пункт «Создать зашифрованный файловый контейнер» и нажмите кнопку «Далее» (рис. 3).

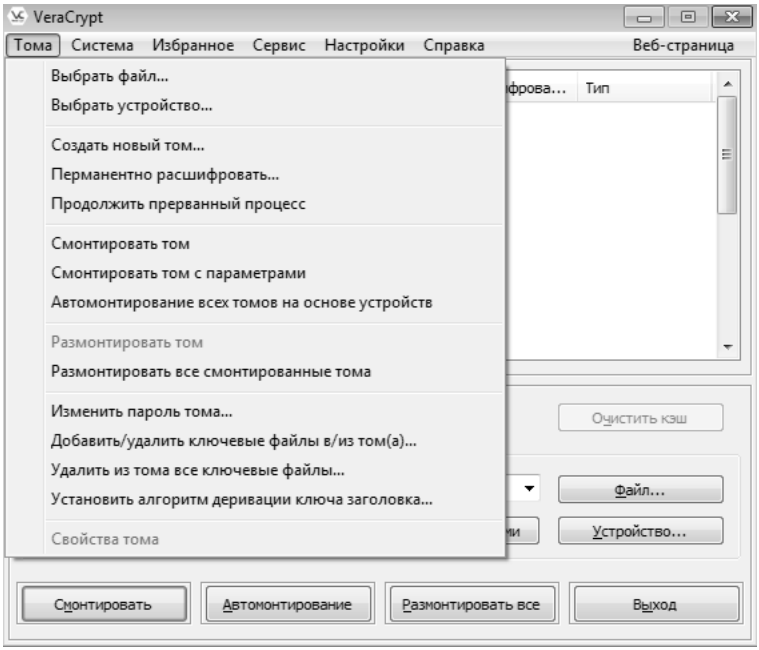

Рис. 2. Меню «Тома»

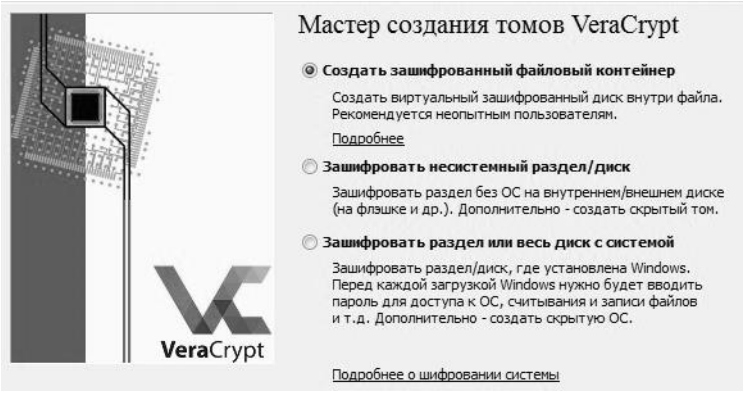

Рис. 3. Мастер создания томов

Далее нужно выбрать тип создаваемого тома. Если выбрать тип «Обычный том VeraCrypt», то контейнер будет просто зашифрован. Если же выбрать «Скрытый том VeraCrypt», то будут созданы два тома, один будет вложен в другой и вложенный будет скрыт. При этом не

обязательно постоянно вводить оба пароля, достаточно ввести только один для тома, который хотите открыть.

Следует учитывать, что **НЕ** скрытый том динамически расширяется и если у вас контейнер занимает 10Гб, Вы запишите в скрытый том 9Гб информации, а в не скрытый 2 Гб, то скрытый будет поврежден и сузится до 8Гб. Выберите тип тома «Обычный том» (рис. 4).

Рис. 4. Выбор типа тома

Выберите путь, где будет располагаться контейнер, и название файла в соответствии с группой и инициалами (рис. 5).

Рис. 5. Выбор места размещения тома

Далее выберите алгоритм шифрования в соответствии со своим вариантом (рис. 6-7).

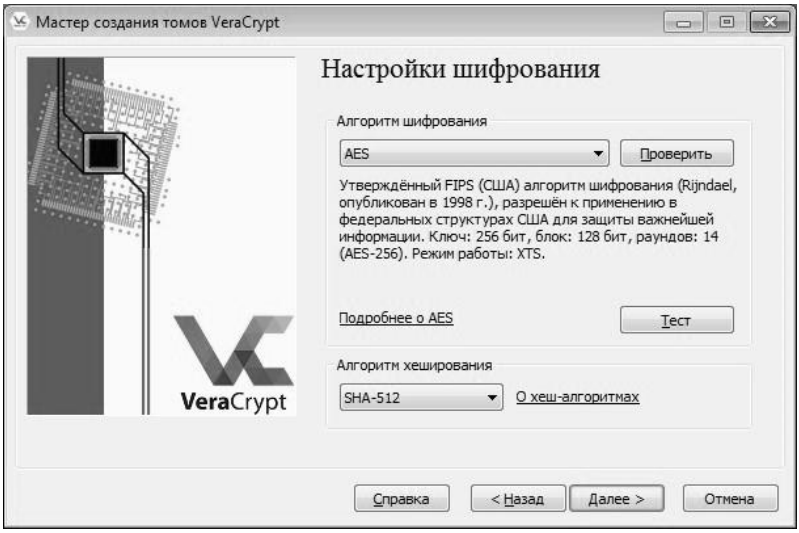

Рис. 6. Настройка режима шифрования

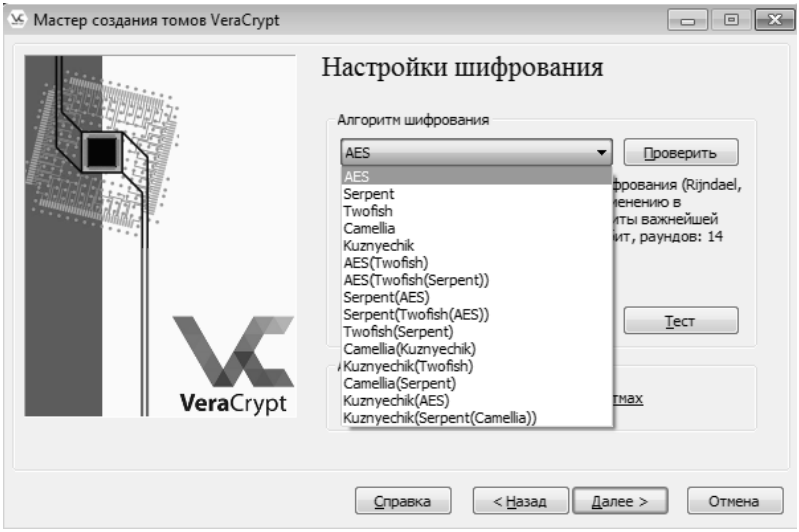

Рис. 7. Выбор алгоритма шифрования

Алгоритм хеширования оставьте по умолчанию «SHA-512» (рис. 8). Далее нажмите кнопку «Проверить» в разделе «Алгоритм

шифрования». Выполните проверку выбранного алгоритма шифрования (рис. 9).

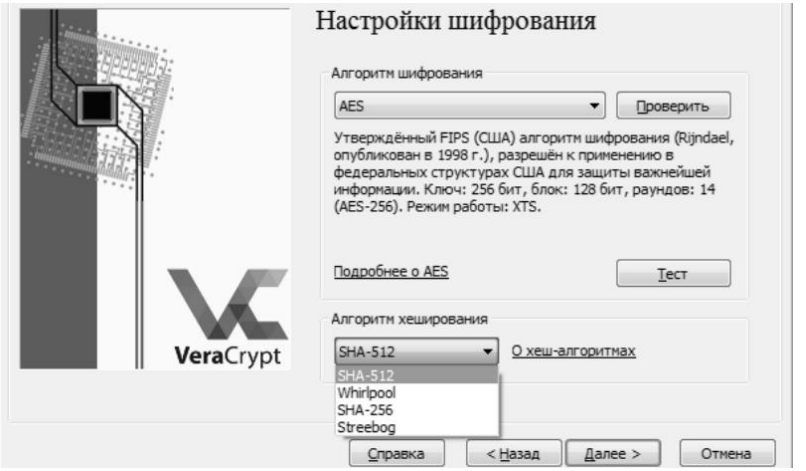

Рис. 8. Выбор алгоритма хеширования

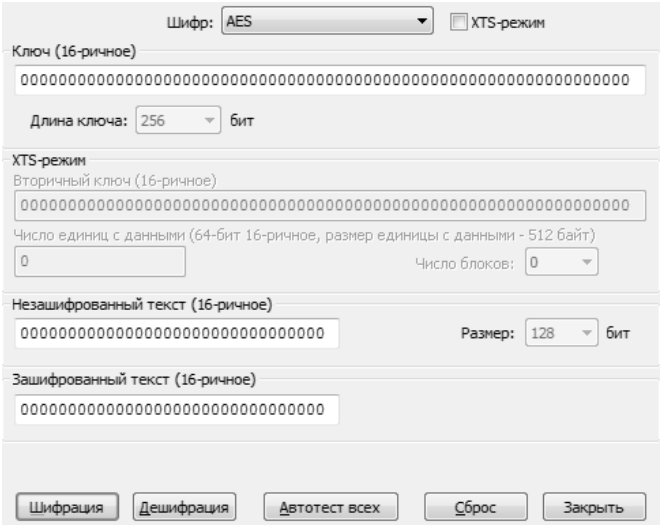

Рис. 9. Тестирование алгоритма шифрования

Выполните тест скорости алгоритмов шифрования нажав на кнопку «Тест» (рис. 10). Проанализируйте полученные данные.

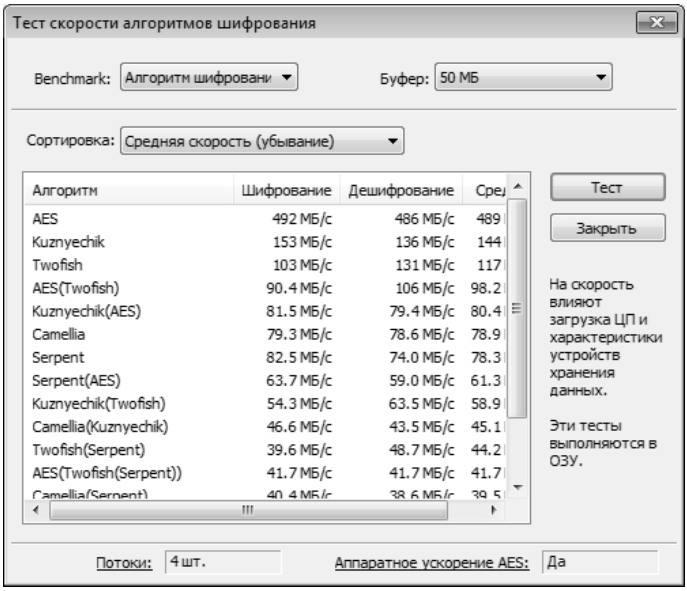

Рис. 10. Результаты теста скорости алгоритмов шифрования

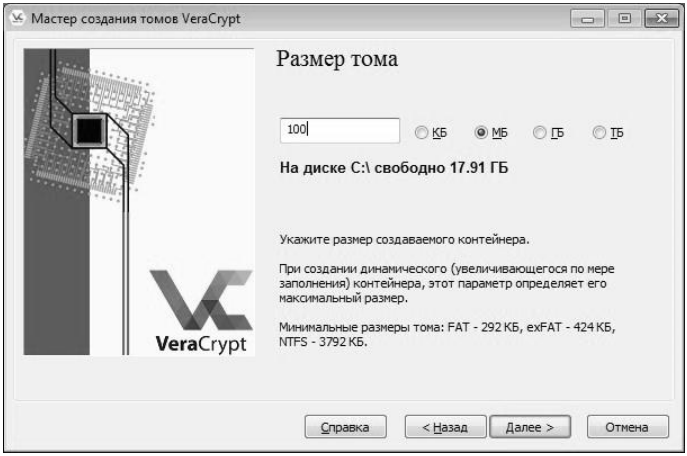

Рис. 11. Указание размер создаваемого файлового контейнера

Выберите размер создаваемого файлового контейнера (рис.11).

Далее необходимо создать ключевые файлы для создаваемого контейнера. Для этого поставим отметку в пункте «Ключ. Файлы» и

нажмем на кнопку «Ключ. Файлы» (рис. 12). Также возможно использовать пароль и PIM, но сейчас мы это делать не будем.

PIM – персональный умножитель итераций. Эта функция усложняет взлом перебором. При использовании PIM, при вводе пароля, потребуется постоянно его использовать.

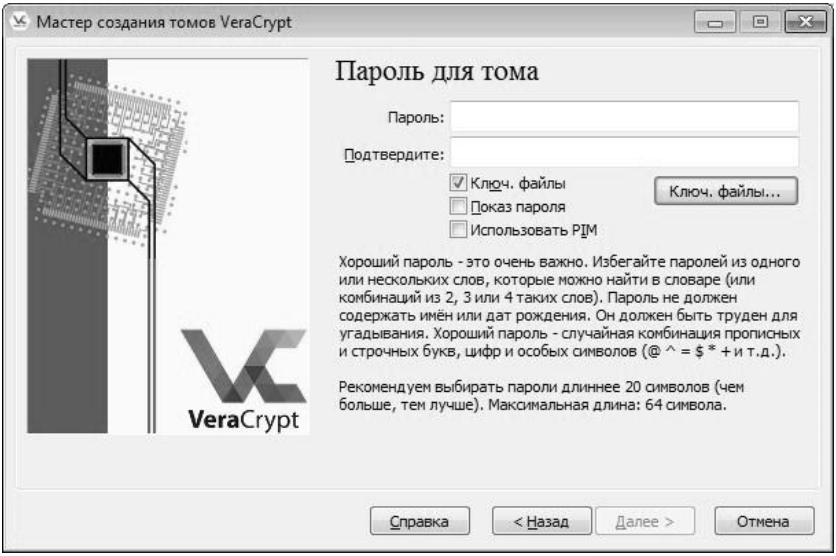

Рис. 12. Настройка доступа к тому

Создайте любой файл осмысленного содержания, например, картинку, в любом месте диска виртуальной машины. Файл может иметь любое содержимое и расширение. В интерфейсе программы на кнопку «Файл» и выберите созданный файл. Нажмем кнопку «Ок» и «Далее» (рис. 13).

Файлов может быть несколько. Они могут иметь различный формат и содержание, располагаться в любом месте, включая флеш-диск и электронный ключ. Но учтите, что, потеряв его, Вы больше никогда не сможете получить доступ к зашифрованным файлам.

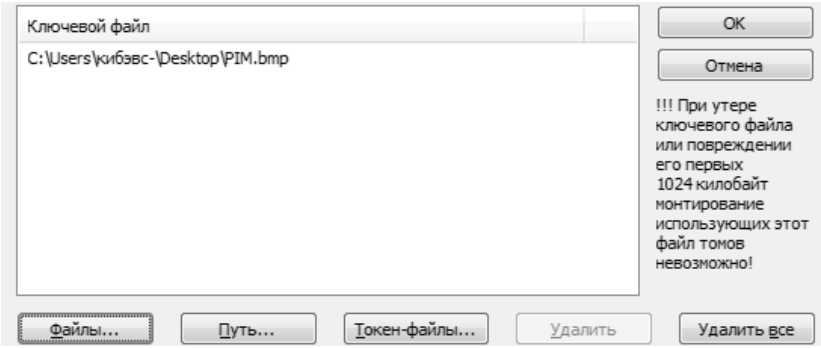

Рис. 13. Добавление ключевого файла

Далее выберите файловую систему FAT. Соберите энтропию. Для этого необходимо случайно перемещать мышь по интерфейсу окна программы. В процессе будет заполняться шкала «Собрано энтропии из перемещений мыши». Чем больше будет заполнена шкала – тем сложнее будет взломать Ваш зашифрованный том. По окончании сбора энтропии нажмите кнопку «Разметить» (рис. 14).

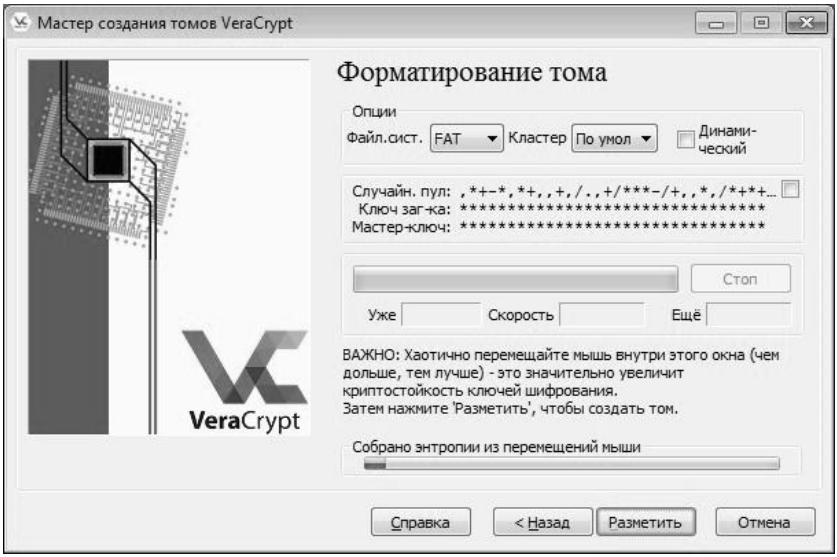

Рис. 14. Разметка тома

После завершения разметки будет выдано сообщение об успешном создании тома (рис. 15).

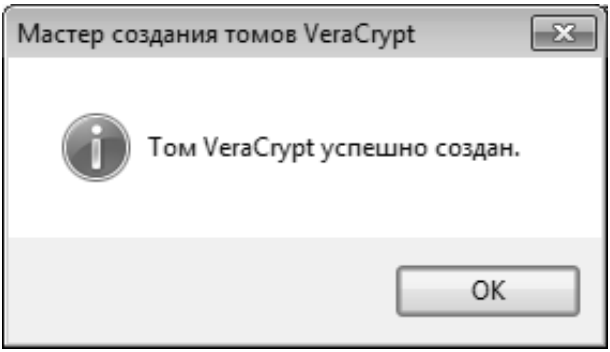

Рис. 15. Успешное создание тома

Перейдите в основной интерфейс программы. Для открытия созданного контейнера необходимо выбрать любую из доступных в интерфейсе программы букв диска, нажать кнопку «Файл» и выбрать контейнер. Далее необходимо нажать кнопку «Смонтировать» (рис. 16).

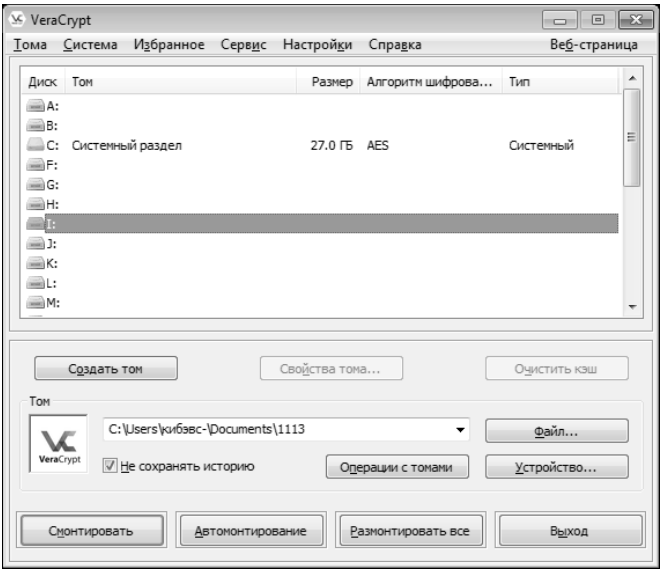

Рис. 16. Монтирование тома

Далее высветится окно, где необходимо выбрать ключевой файл и нажать «Ок» (рис. 17).

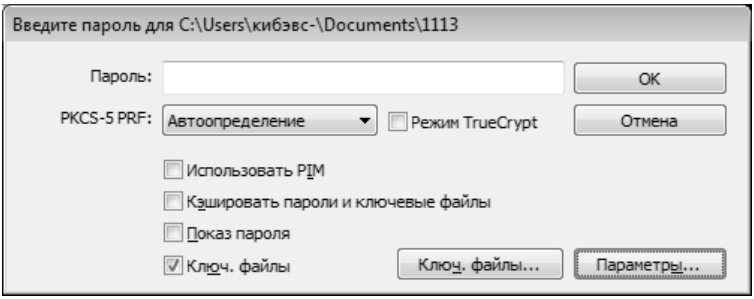

Рис. 17. Выбор ключевого файла

Дождитесь завершение монтирования тома. После того, как процесс завершится, диск станет доступен и его можно использовать как обычный локальный диск (рис. 18).

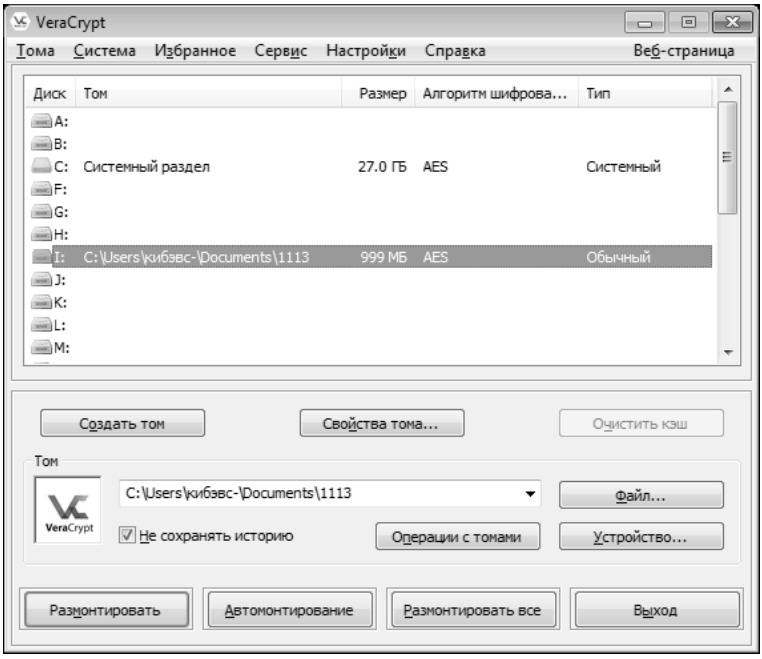

Рис. 18. Смонтированный раздел

Бывают ситуации, когда необходимо смонтировать том таким образом, чтобы он отображался как сменный носитель. Для этого

необходимо поставить отметку в окне параметров, нажав кнопку «Параметры» в окне ввода пароля.

После завершения работы с контейнером его следует размонтировать в целях повышения безопасности. Откройте использованный ключевой файл и убедитесь, что файл не был изменен.

3.2 Шифрования раздела жесткого диска

Откройте мастер томов, как и в предыдущем разделе, и выберите пункт «Зашифровать несистемный раздел/диск» (рис. 19).

Программа может шифровать не только раздел жесткого диска или полностью жесткий диск, но и внешние накопители.

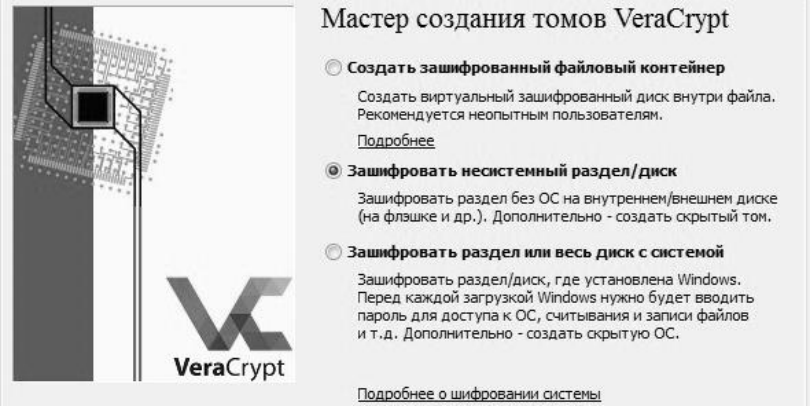

Рис. 19. Мастер создания томов

В этот раз выберите вариант «Скрытый том VeraCrypt» (рис. 20).

Рис. 20. Выбор скрытого типа тома

Выберите обычный режим (рис. 21). Далее выберите диск, который будет зашифрован (рис. 22). В данном случае — это диск E.

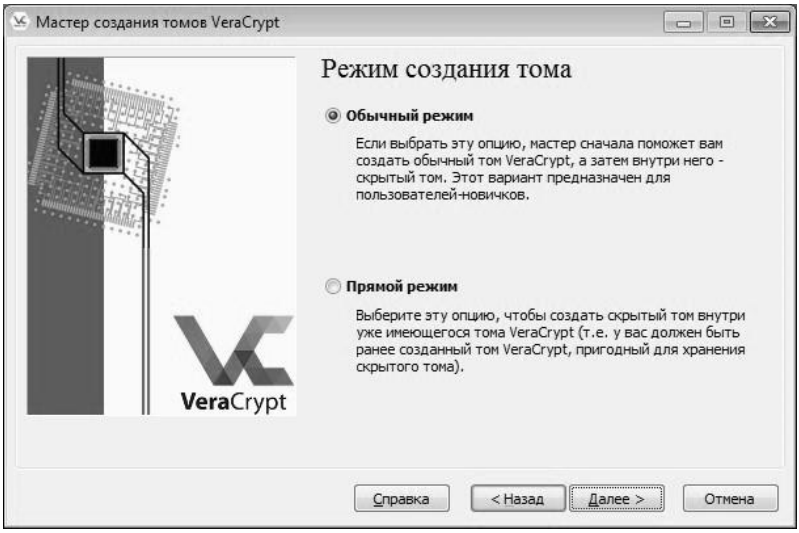

Рис. 21. Выбор режима

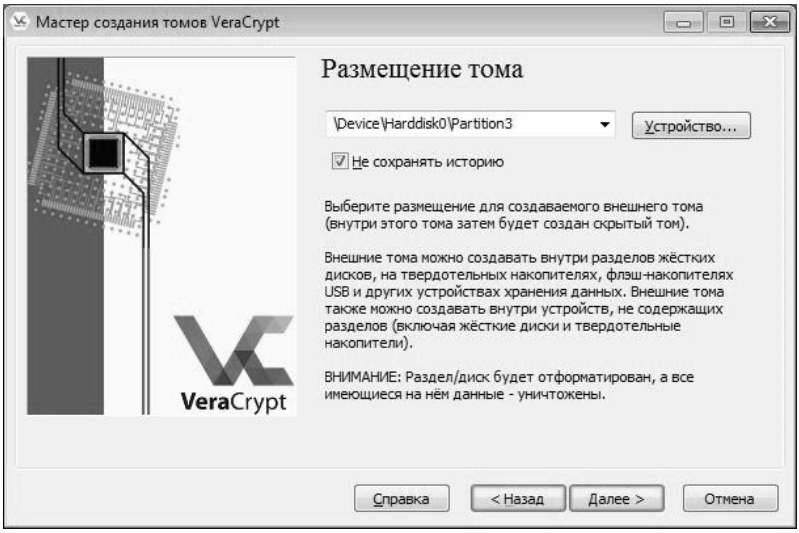

Рис. 22. Выбор диска

Ознакомьтесь с сообщением программы и нажмите кнопку «Далее» (рис. 23).

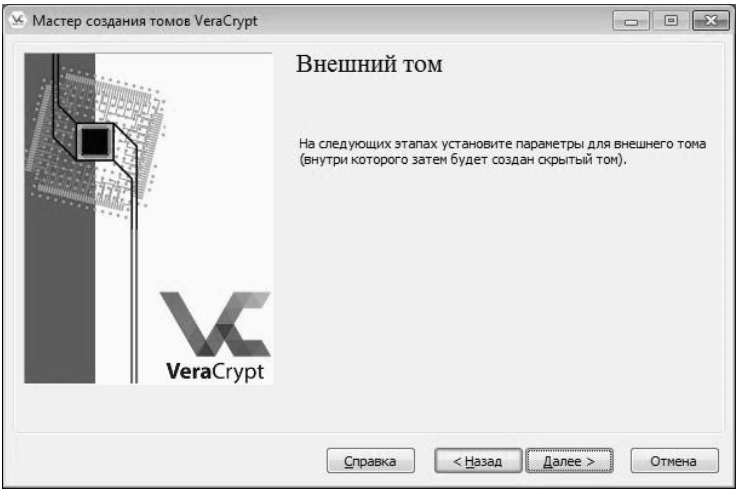

Рис. 23. Предупреждение о дальнейших этапах работы

Выберите алгоритм шифрования в соответствии с вариантом и проверьте алгоритм (рис. 24).

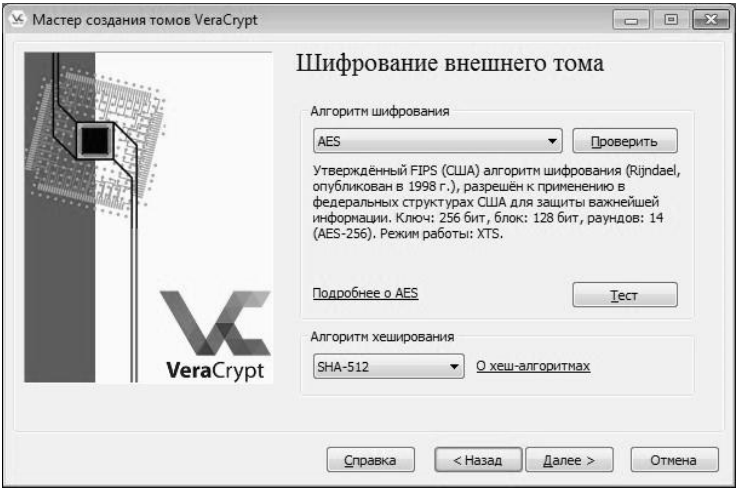

Рис. 24. Алгоритм шифрования

Внешний том займет все доступное пространство. Нажмите кнопку «Далее» (рис. 25).

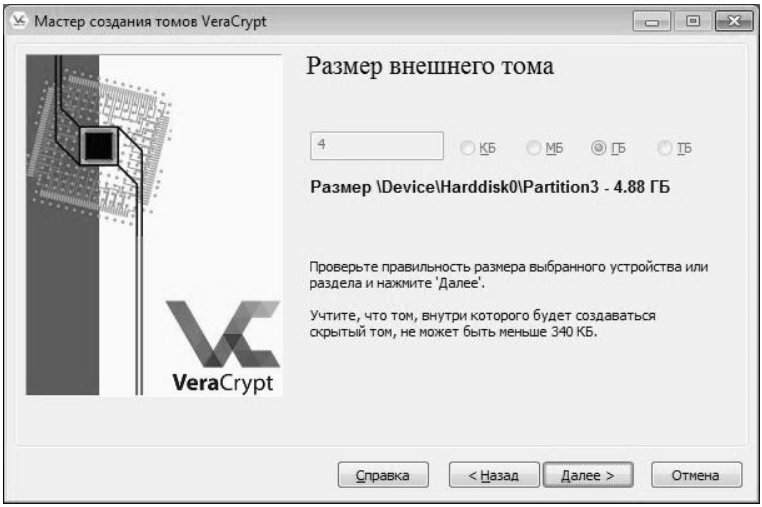

Рис. 25. Выбор размера внешнего тома

Для примера укажите только пароль (рис.26).

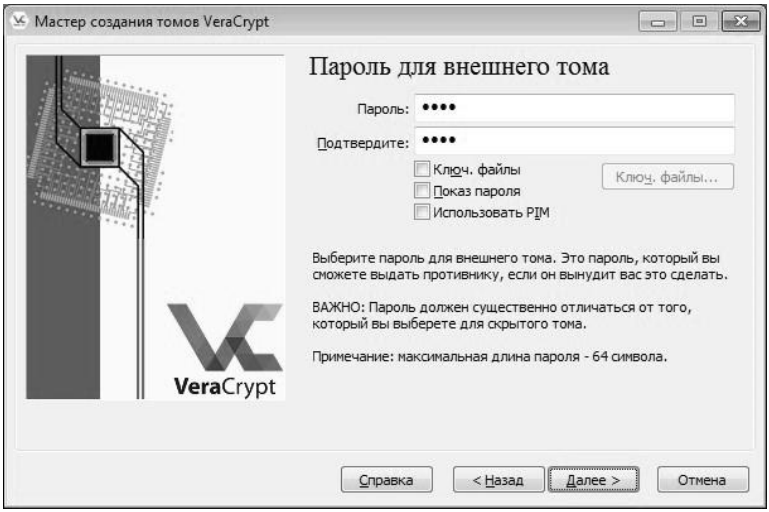

Рис. 26. Ввод пароля для внешнего тома

Прочтите предупреждение по поводу хранения больших файлов в томе и поставьте отметку «Да» (рис. 27).

Рис. 27. Предупреждение о хранении больших файлов

Выберите файловую систему NTFS, соберите энтропию и нажмите кнопку «Разметка» (рис. 28).

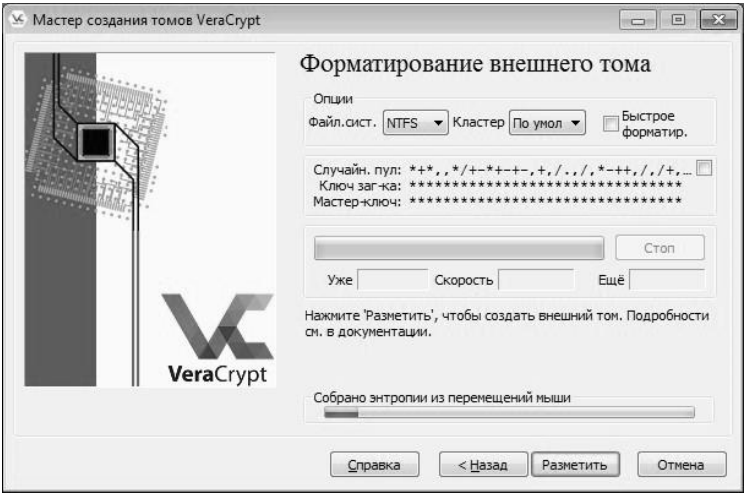

Рис. 28. Разметка внешнего тома

Прочтите предупреждение и нажмите кнопку «Да» (рис. 29).

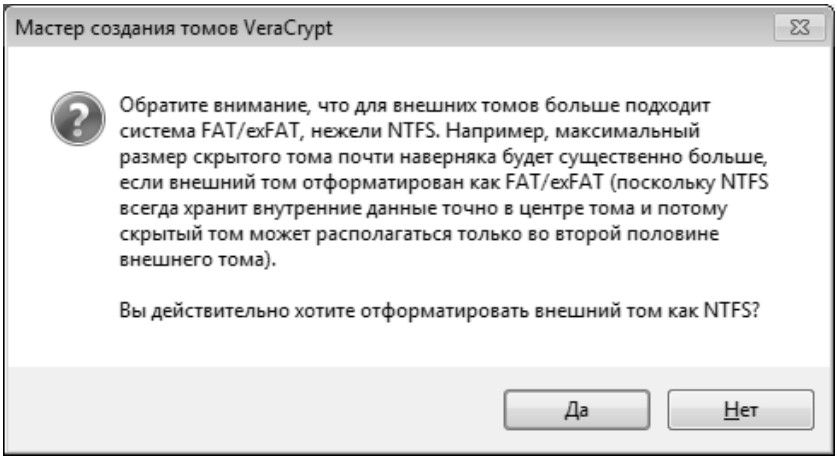

Рис. 29. Предупреждение о файловой системе

Дождитесь завершения процедуры разметки диска (рис. 30).

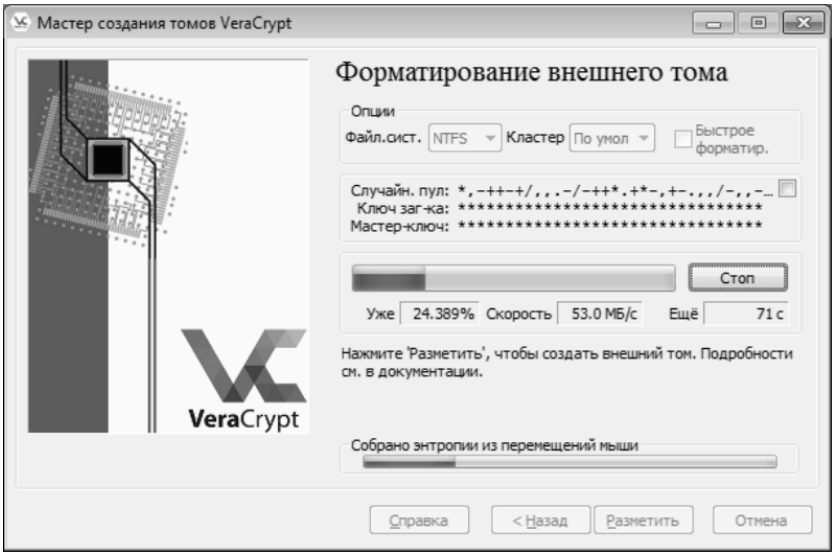

Рис. 30. Процесс разметки диска

После завершения разметки будет показан информационный раздел о работе с внешним томом. Нажмите кнопку «Далее» (рис. 31).

Рис. 31. Информационная страница

Далее мастер создания томов предложит настроить скрытый том. Нажмите кнопку «Далее» (рис. 32).

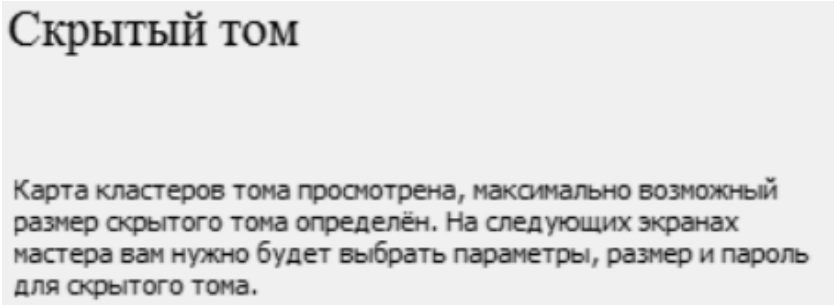

Рис. 32. Скрытый том

Выберите алгоритм шифрования, который выбрали для внешнего тома, и нажмите «Далее» (рис.33).

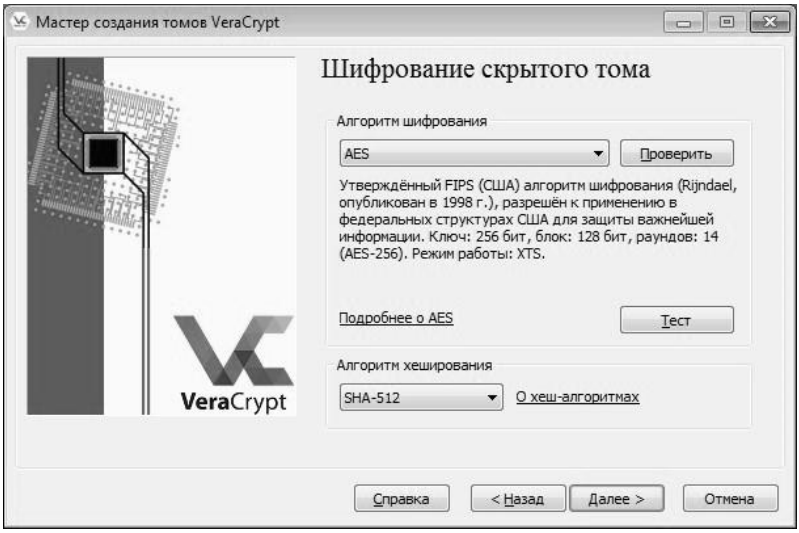

Рис. 33. Шифрование скрытого тома

Далее введите пароль, отличный от пароля для внешнего тома, и нажмите кнопку «Далее» (рис. 34).

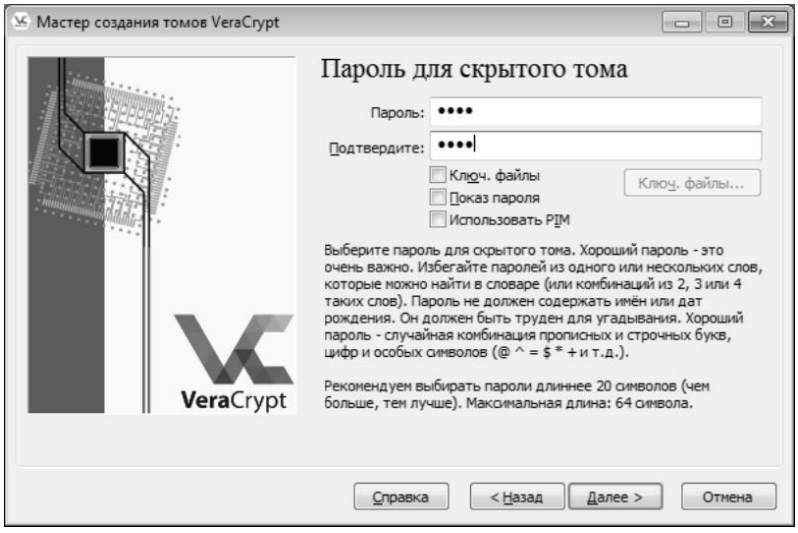

Рис. 34. Пароль для скрытого тома

Соберите энтропию и выполните разметку тома (рис. 35).

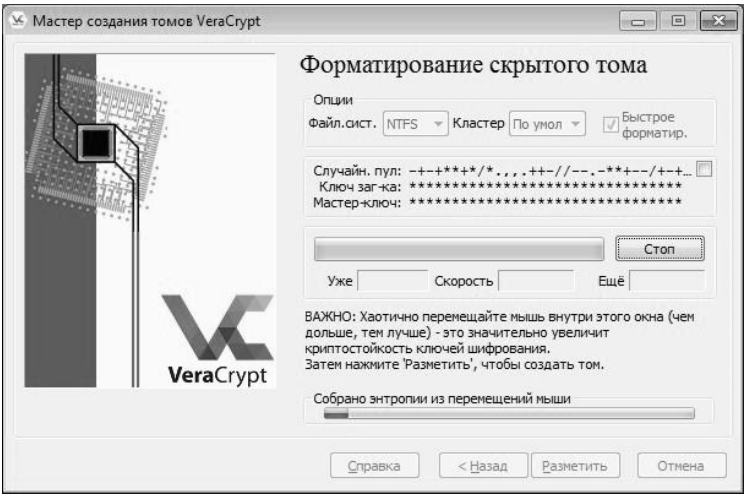

Рис. 35. Форматирование скрытого тома

Далее прочитайте выпадающие сообщения и согласитесь с ними. После этого будет выдано окно с уведомлением об успешности создания скрытого тома (рис. 36).

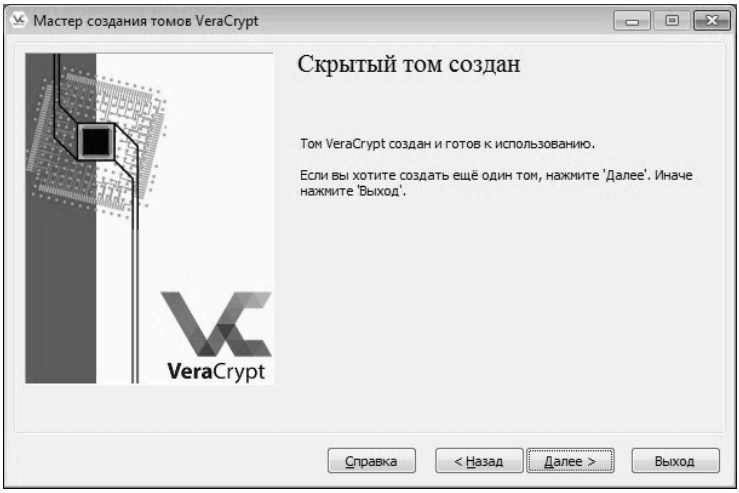

Рис. 36. Успешное создание скрытого тома

Работа с внешним и скрытым томом аналогична работе с файловым контейнером, но при инициализации тома необходимо ввести пароль от тома, который хотите открыть, от внешнего или скрытого.

3.3 Шифрование системного диска

В окне создания томов выберите раздел «Шифровать раздел или весь диск с системой» (рис. 37).

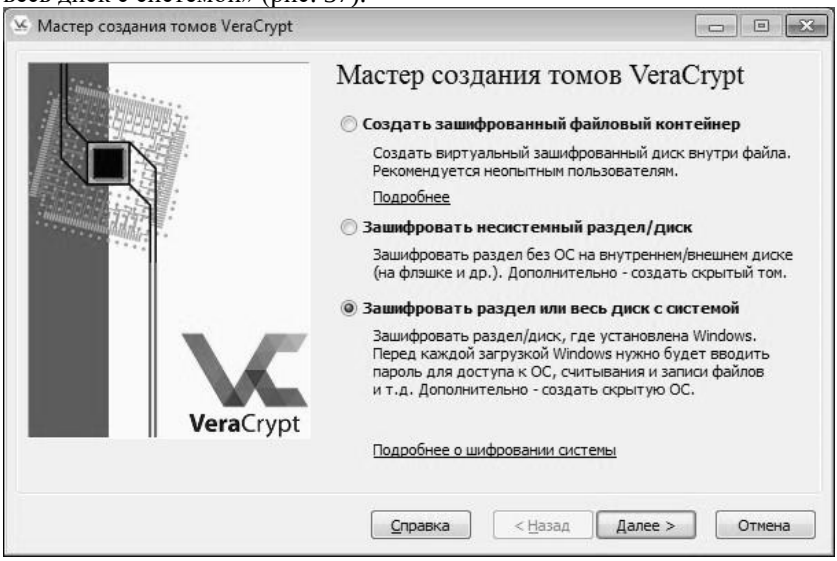

Рис. 37. Шифрование системного диска

Есть два типа шифрования системы – скрытый или обычный. В случаи с обычным типом системный диск будет полностью зашифрован и при загрузке компьютера будет предложено ввести пароль.

В случаи со скрытым будет создан поддельный системный раздел куда пользователь должен установить систему и загрузить неважные файлы.

Главное отличие этих двух типов в том, что если вас вынудят сообщить пароль, то вы можете сказать пароль от поддельного системного диска. В этом случаи злоумышленнику потребуется гораздо больше усилий, чтобы понять, что существует еще одна система.

Выберите обычный тип шифрования (рис. 38). Далее необходимо выбрать пункт «Зашифровать систем раздел Windows» и нажать кнопку «Далее» (рис. 39).

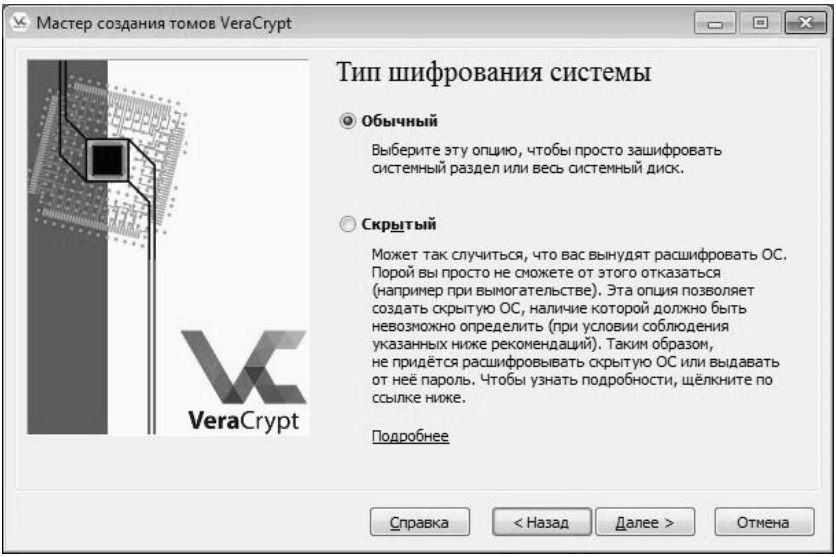

Рис. 38. Тип шифрования системы

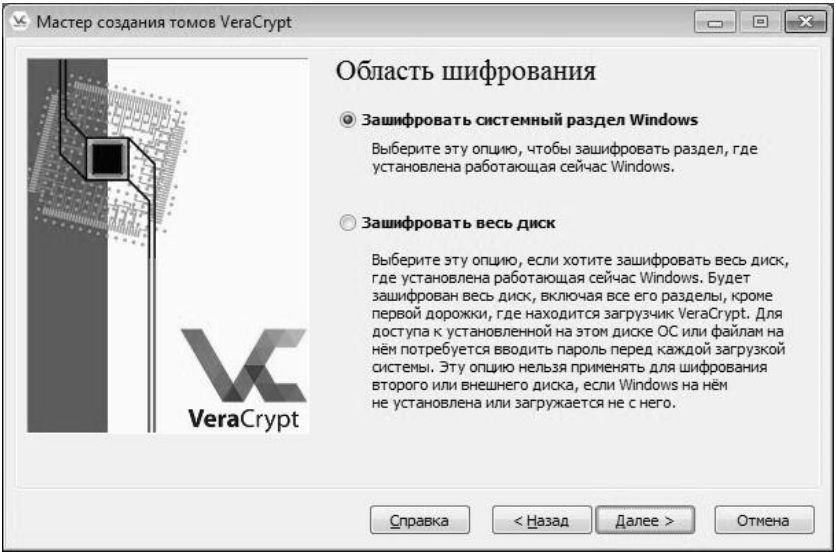

Рис. 39. Область шифрования

В нашем случаи установлена одна Windows, следовательно, нужно выбрать пункт «Одиночная загрузка» (рис. 40).

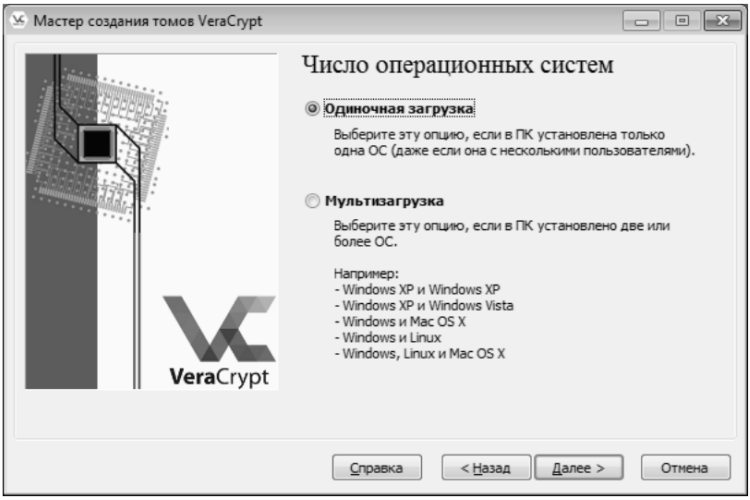

Рис.40. Число операционных систем

Далее следует оставить настройки шифрования по умолчанию (рис. 41).

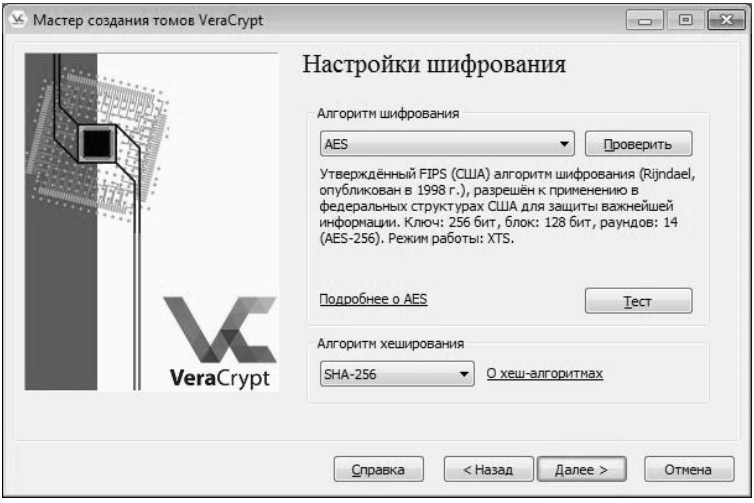

Рис. 41. Настройки шифрования

Поставьте галочку на пункте «Использовать PIM» и введите пароль и PIM (рис. 42).

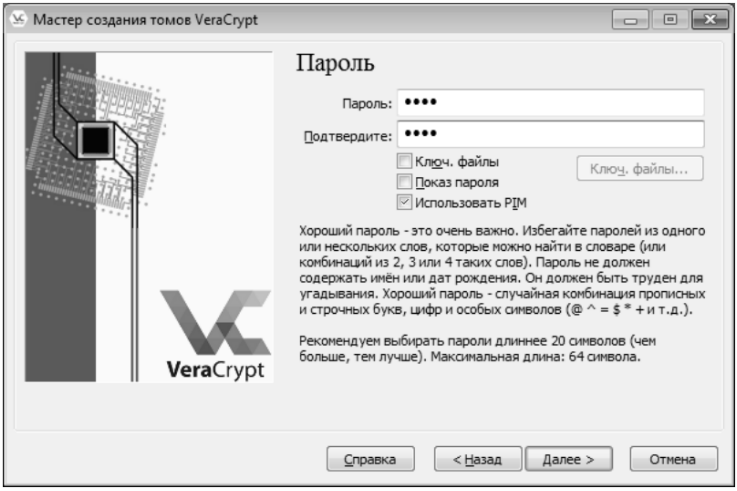

Рис. 42. Ввод пароля и PIM для доступа к тому

Дайте необходимо собрать энтропию и нажать кнопку «Далее» (рис. 43).

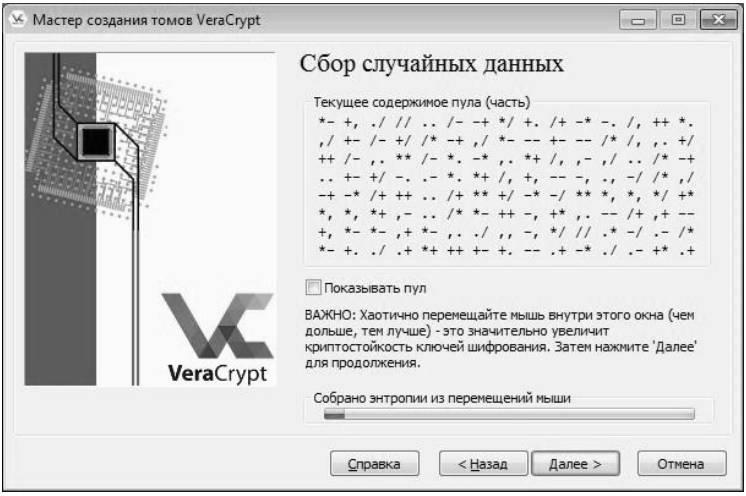

Рис. 43. Сбор случайных данных

В случае успешного создания ключей, нажмите кнопку «Далее» (рис. 44).

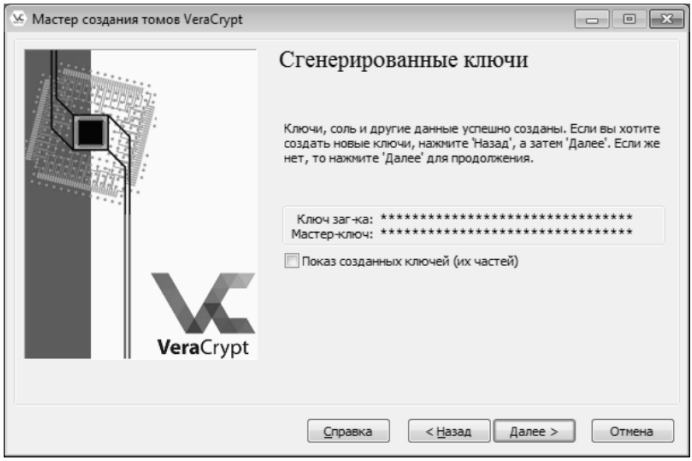

Рис. 44. Сгенерированные ключи

В случае, если утрачен доступ к системе, необходимо предоставить диск восстановления для восстановления доступа. Рекомендуется тщательно спрятать его. Для его создания выберите путь хранения диска и нажмите «Далее» (рис. 45).

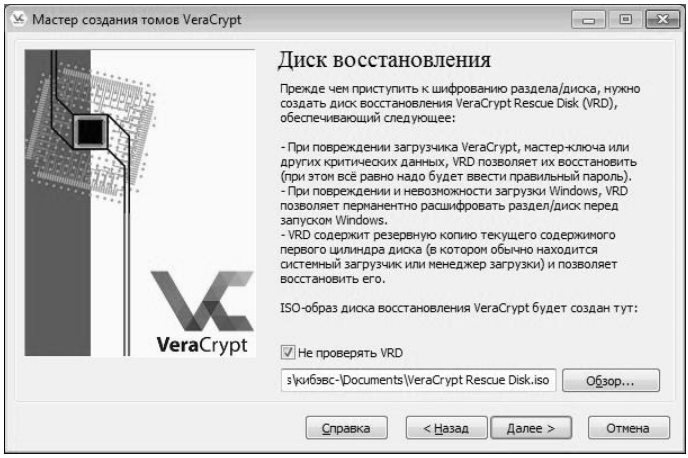

Рис. 45. Создания диска восстановления

После успешного создания диска восстановления будет показано соответствующее окно, где будет предложено прожечь диск восстановления на компакт-диск. Нажмите кнопку «Далее» (рис. 46).

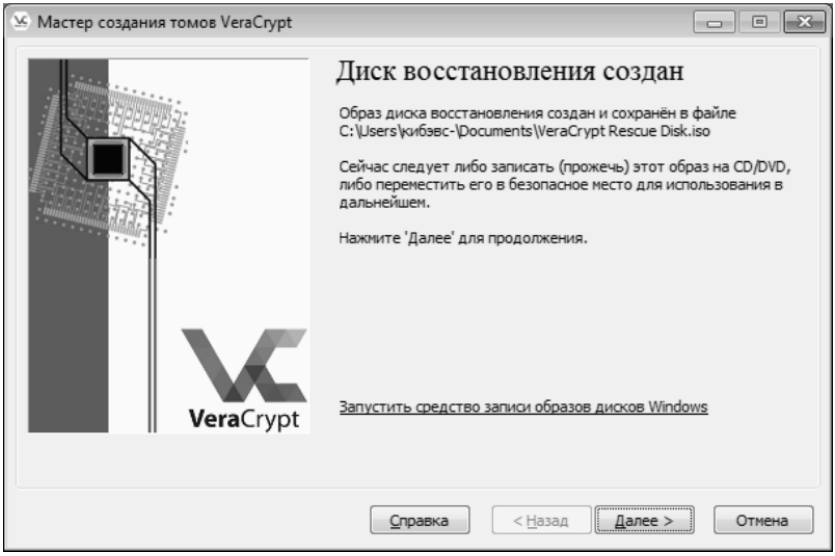

Рис. 46. Успешное создание образа восстановления

Внимательно ознакомьтесь с предупреждением и нажмите кнопку «Да» (рис. 47).

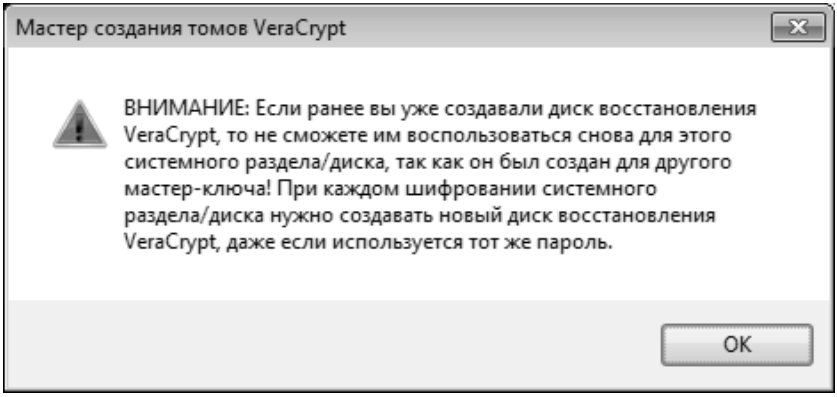

Рис.47. Предупреждение мастера создания томов

Следующим шагом будет выбор режима очистки диска. Очистка необходима в связи с особенностью хранения информации на диске. При удалении какого-либо файла с диска, фактически он не удаляется, а обнуляются только указатели на этот файл. Процедура очистки

заключается в многократной перезаписи псевдослучайной информации в ячейки памяти жесткого (или какого-либо другого) диска, что затрудняет считывание остаточной незашифрованной информации с диска. Следовательно, если не провести эту процедуру, то физически на диске останутся незашифрованные данные.

В нашем случае необходимо отказаться от очистки, выбрав из выпадающего меню пункт «Нет» (рис. 48). Следует учесть, что сейчас очень популярны SSD накопители. Они имеют меньше циклов записи. В связи с этим стоит подумать, нужно ли вам выполнять эту процедуру, если, например, была переустановлена ОС, но до этого системный диск был зашифрован программой VeraCrypt и доступ не был скомпрометирован.

Рис. 48.Режим очистки

Следующим шагом необходимо провести тестирование на ошибки, которые могут возникнуть во время шифрования. Нажмите кнопку «Тест» (рис. 49) и прочитайте предупреждение. Нажмите кнопку «Да» в окне предупреждения (рис. 50).

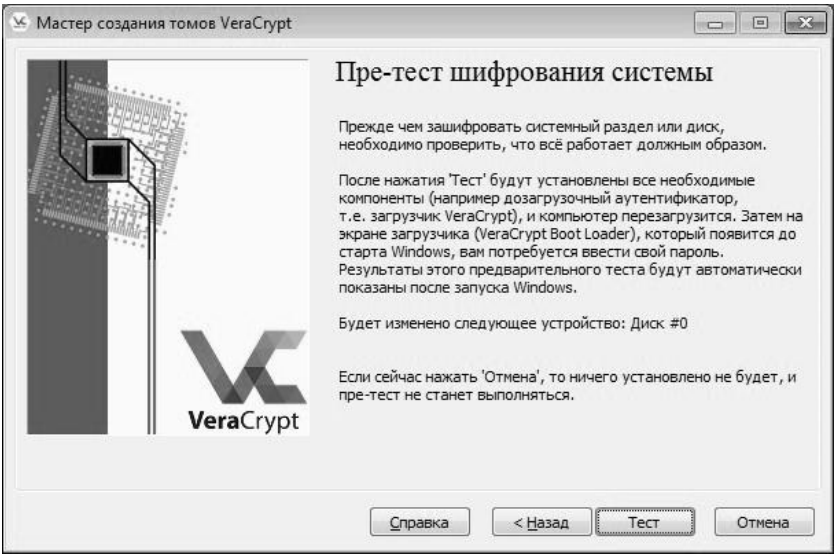

Рис. 49. Пре-тест

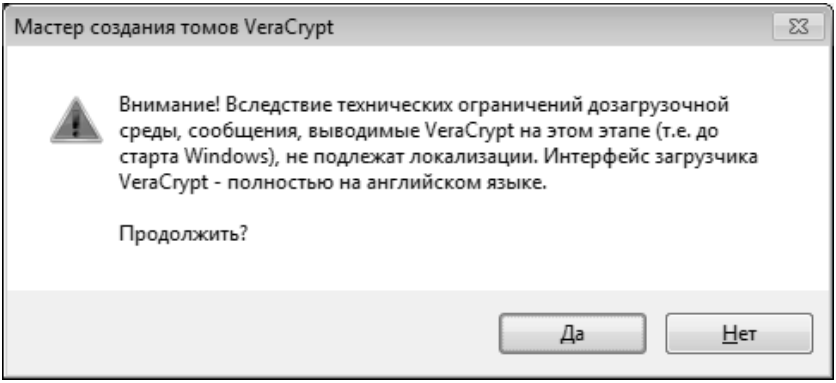

Рис. 50. Предупреждение

Прочитайте информационное сообщение и нажмите кнопку «ОК» (рисунок 51).

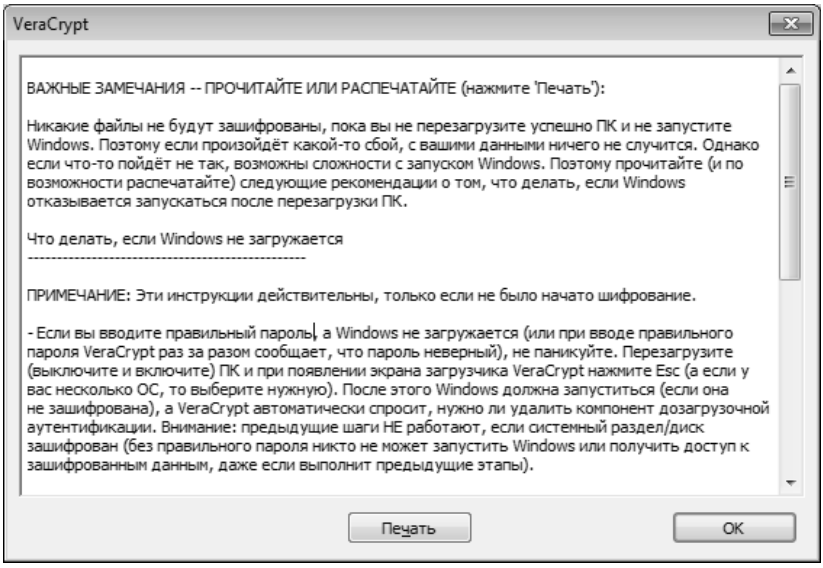

Рис. 51. Информационное сообщение

Выполните перезагрузку нажав кнопку «Да» (рисунок 52).

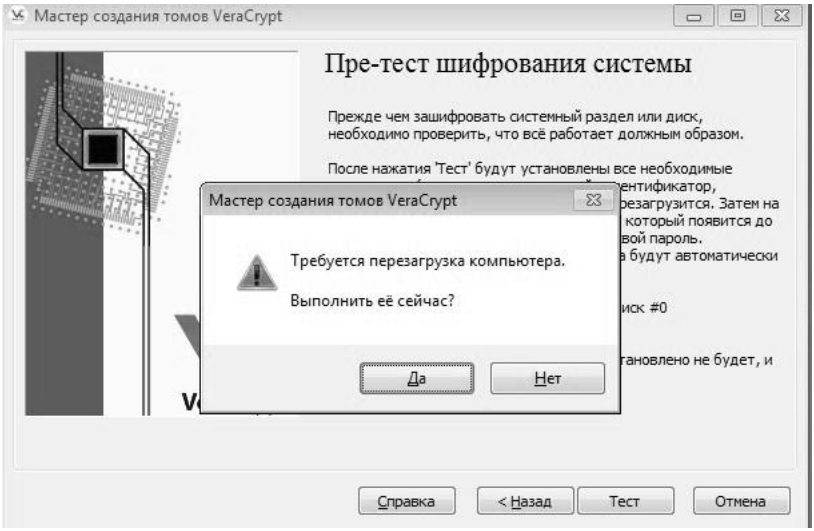

Рис. 52. Перезагрузка

В окне консоли, показанном на рис. 53, введите пароль и PIM от системы шифрования.

Рис. 53. Ввод паролей

Дождитесь, пока система не загрузится (рис. 54). Может показаться, что все подвисло и ничего не работает, но это не так. Обязательно дождитесь загрузки системы или ошибки.

Рис. 54. Пароли введены

После того, как система будет загружена, появится сообщение о успешном прохождении пре-теста. Прочитайте информационное сообщение и нажмите на кнопку «Шифрация» (рис. 55).

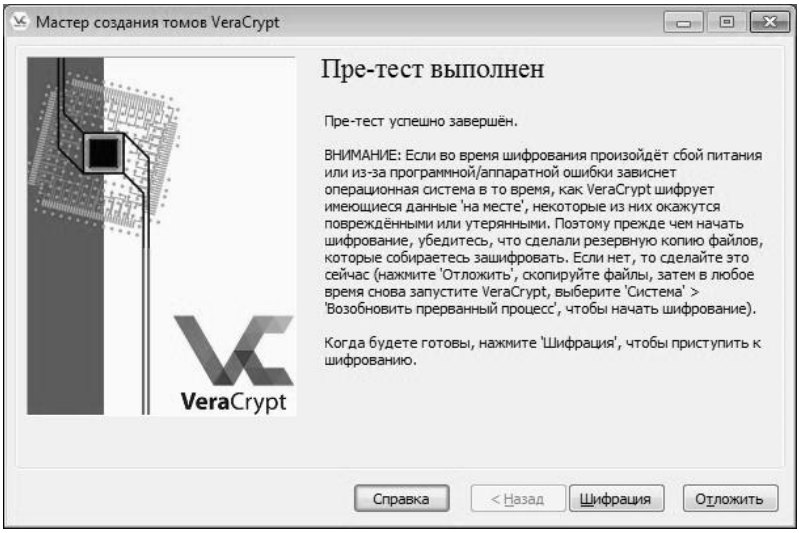

Рис. 55. Успешное выполнение пре-теста

Шифрование может занять некоторое время. Обязательно дождитесь окончания этого процесса (рис. 56).

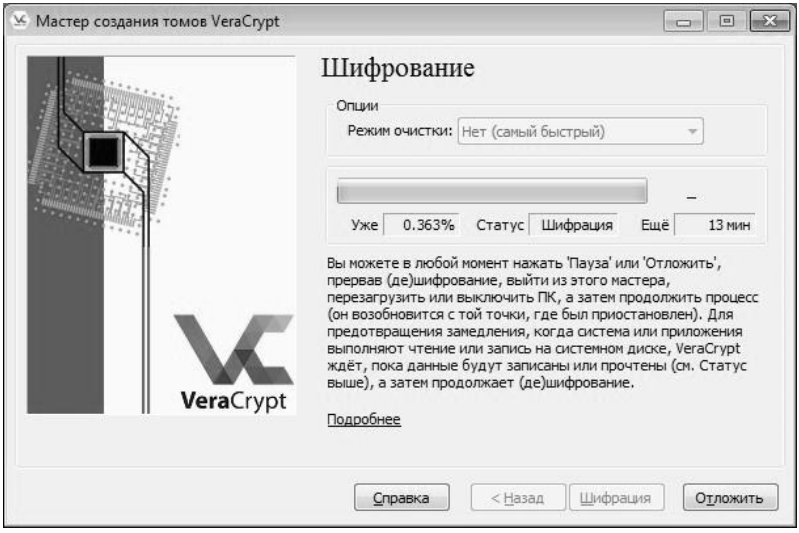

Рис. 56. Процесс шифрования системного диска

После успешного шифрования будет выдано соответствующее сообщение (рис. 57).

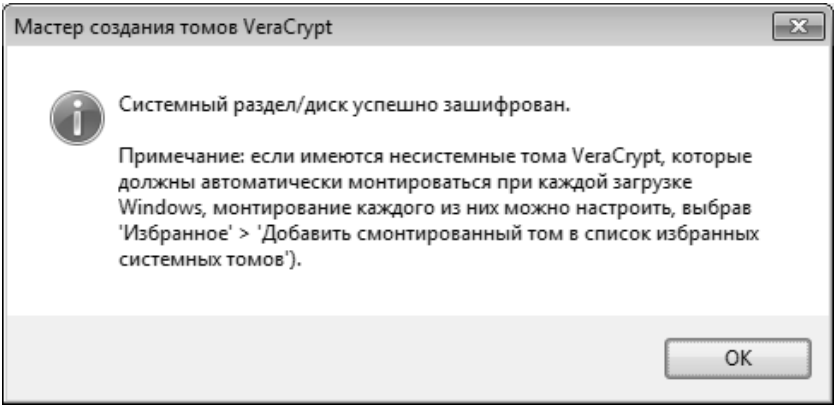

Рис. 57. Успешное шифрование системного диска

Перезагрузитесь, введите пароль и PIM (рис. 58).

Рис. 58. Введенный пароль и PIM

Откройте программу VeraCrypt и посмотрите, как отображается в ней диск C (рис. 59).

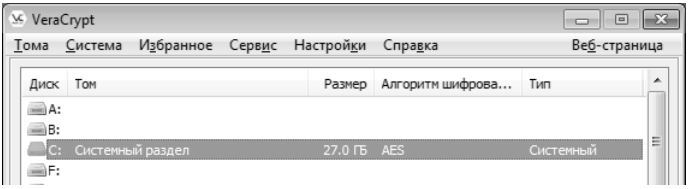

Рис. 59. Отображение диска C в программе

4. Задание на лабораторную работу

1. Создайте зашифрованный файловый контейнер с алгоритмом шифрования по своему варианту (табл. 1).

2. Проведите шифрование раздела жесткого диска в соответствии с вариантом из табл. 1.

3. Проведите шифрование системного диска.

4. Составьте по проделанной работе отчет.

Таблица 1

Варианты для индивидуального выполнения работы

	Файловый контейнер	Шифрование диска
1	AES	AES(Twofish)
2	Serpent	AES(Twofish(Serpent))
3	Twofish	Camellia
4	Camellia	Kuznyechik
5	Kuznyechik	Serpent
6	AES(Twofish)	Twofish
7	AES(Twofish(Serpent))	AES
8	Serpent(AES)	Kuznyechik(Serpent(Camellia))
9	Twofish(Serpent)	Camellia(Serpent)
10	Camellia(Kuznyechik)	Kuznyechik(AES)

5. Контрольные вопросы

1. Какие алгоритмы шифрования применяются в VeraCrypt?

2. Что такое файловый контейнер?

3. Чем отличается скрытый том от обычного?

4. Что влияет на скорость тестируемых алгоритмов шифрования?

5. Для чего необходима очистка диска при шифровании системного диска?

6. Что такое PIM?

7. Какие достоинства и недостатки у использования ключевых файлов?

8. Что такое скрытая операционная система?

9. Как отразится на скрытом томе, если в обычный том будет записан большой объем информации?

10. Как отразится на открытом томе, если в скрытый том будет записан большой объем информации?

ЛАБОРАТОРНАЯ РАБОТА №4
Установка и настройка служб удостоверяющего центра

1. Цель работы

Целью лабораторной работы является ознакомление с процессом установки и настройки служб необходимых для функционирования удостоверяющего центра на примере Active Directory Certificate Services (службы сертификации).

2. Краткие теоретические сведения

Организации могут использовать службы сертификации AD CS в инфраструктуре открытых ключей PKI (Public Key Infrastructure), чтобы создать центр сертификации для выдачи цифровых сертификатов, которые привязывают объект идентификации пользователя, устройства либо службы к соответствующему частному лицу.

Структура Active Directory включает пять технологий. Эти технологии полностью реализуют идентификацию и доступ (IDA):

1. Доменные службы Active Directory (Active Directory Domain Services) – Идентификация: проверяются подлинность и авторизация в сети, а также поддерживается управление объектами с помощью групповой политики.

2. Службы облегченного доступа к каталогам (Active Directory Lightweight Directory Services) – Приложения: поддерживает множество хранилищ данных в одной системе, чтобы каждое приложение можно было развернуть с собственным каталогом, схемой, назначенным облегченным протоколом доступа к каталогам LDAP (Lightweight Directory Access Protocol), портами SSL и журналом событий приложений.

3. Службы сертификации Active Directory (Active Directory Certificate Services) – Доверие: организации могут использовать службы сертификации AD CS в инфраструктуре открытых ключей PKI (Public Key Infrastructure), чтобы создать центр сертификации для выдачи цифровых сертификатов, которые привязывают объект идентификации пользователя, устройства либо службы к соответствующему частному лицу.

4. Службы управления правами Active Directory (Active Directory Rights Management Services) – Целостность: предоставляют технологию защиты информации, с помощью которой можно реализовать шаблоны устойчивых политик использования, задающих разрешенное и

неавторизованное применение в сети, вне ее, а также внутри и вне периметра брандмауэра.

5. Службы федерации Active Directory (Active Directory Federation Services) – Партнерские отношения: с помощью служб AD FS организация может расширить инфраструктуру «IDA» на множестве платформ, включая среды Windows и другие, а также обеспечить для доверенных партнеров защиту прав идентификации и доступа вне периметра безопасности.

3. Ход работы

3.1 Установка и настройка Active Directory Certificate Services

3.1.1 Установка необходимых ролей и компонентов

Для начала работы с удостоверяющими центрами создадим клон виртуальной машины. Для этого добавьте в библиотеку виртуальных машин PKI lab и в контекстном меню выберите пункт «Клонировать» (рис. 1). Исходная версия пригодится в другой лабораторной работе. Среди параметров клонирования обратите внимание на необходимость генерации новых MAC-адресов всех сетевых адаптеров (рис. 2).

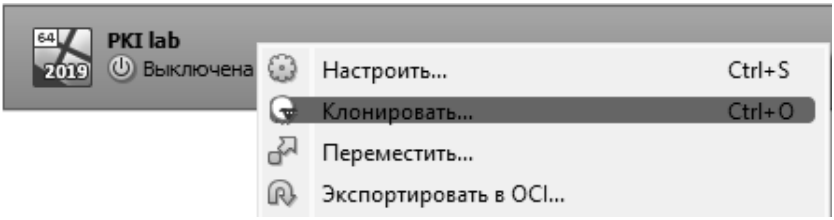

Рис. 13. Клонирование виртуальной машины

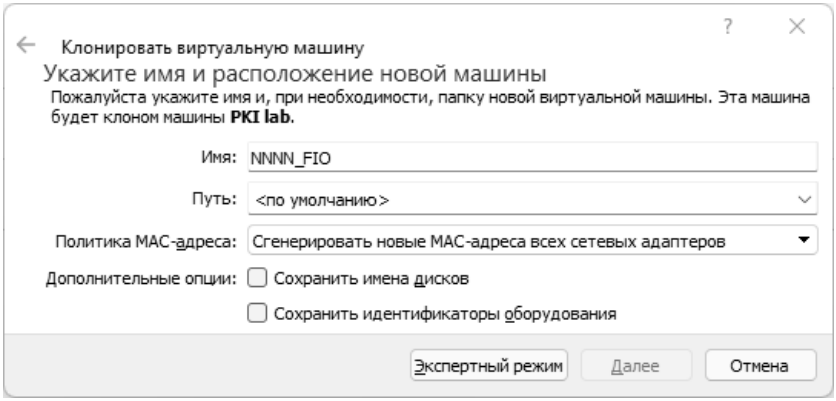

Рис. 2. Параметры клонирования виртуальной машины

Тип клонирования выберите как «Полное клонирование» (рис. 3).

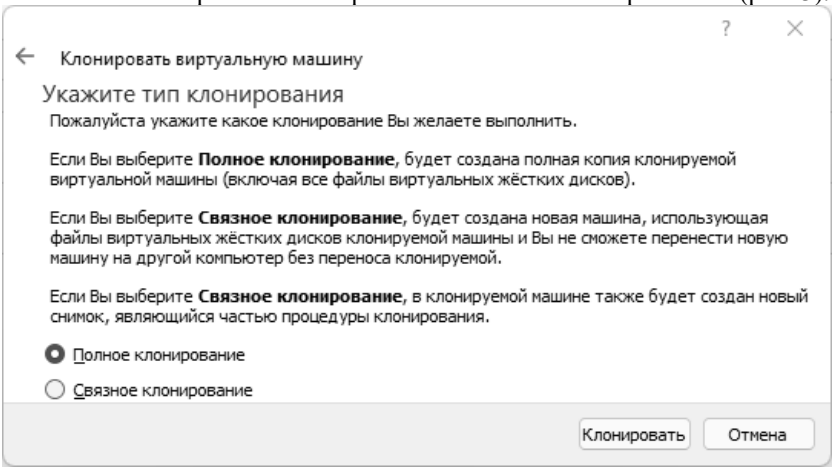

Рис. 3. Пункт «Добавить роли и компоненты»

Запустите полученную виртуальную машину, имеющую операционную систему Windows Server 2019. После загрузки системы появится окно диспетчера сервера. Перейдите к установке доменных служб Active Directory. Для этого в диспетчере сервера выберите пункт «Добавить роли и компоненты» (рис. 4).

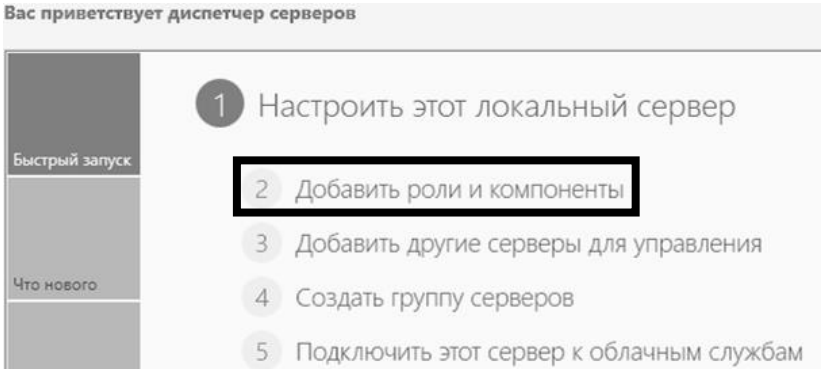

Рис. 4. Пункт «Добавить роли и компоненты»

После этого откроется мастер добавления ролей, где нужно пропустить первое окно, после чего выбрать пункт «Установка ролей или компонентов», затем выберете пункт «Выберете сервер из пула серверов». Далее отметьте галочкой пункты «DNS-сервер» и

«Доменные службы Active Directory» (рис. 5). Добавьте необходимые для установки компоненты в появляющемся окне, нажимая на кнопку «Добавить компоненты» (рис. 6). Если появится предупреждение, нажмите кнопку «Продолжить». Остальные пункты оставьте по умолчанию, запустите установку.

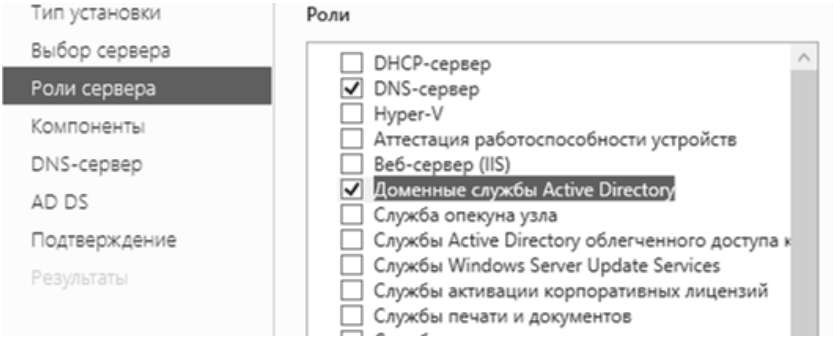

Рис. 5. Выбор ролей сервера для установки

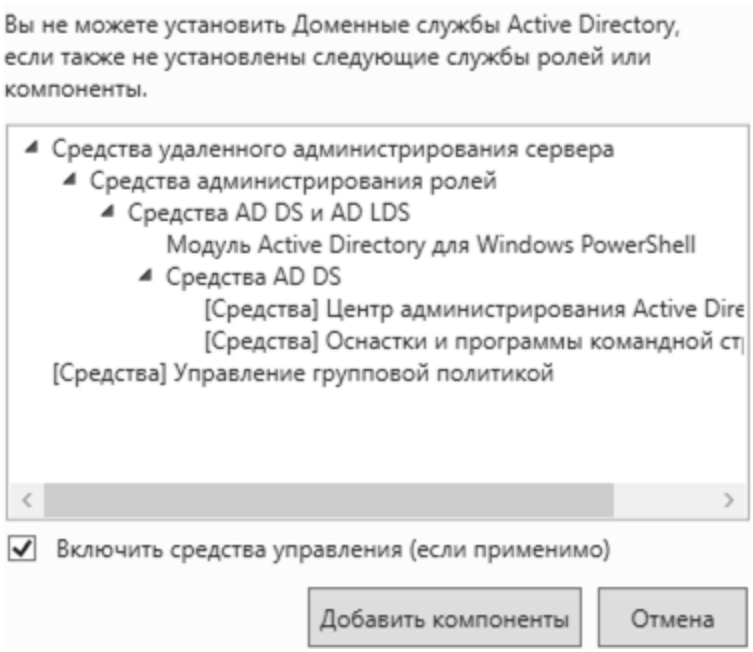

Рис. 6. Добавление компонентов для установки роли

Дождитесь окончания установки и нажмите на синюю строку «Повысить роль этого сервера до уровня контроллера домена» (рис. 7).

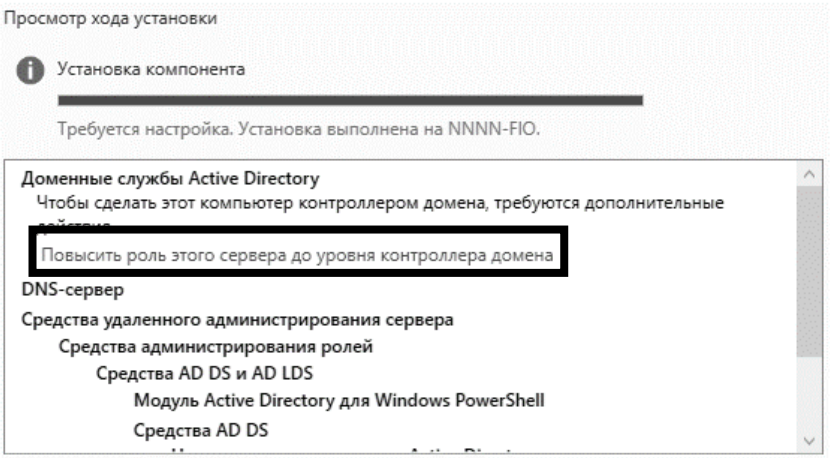

Рис. 7. Пункт «Повысить роль этого сервера до уровня контроллера домена»

В мастере выберете «Добавить новый лес», задайте имя корневого домена как «(Имя).ru» (рис. 8). В качестве примера выбран домен ***tusur.ru***. Вы можете выбрать любой домен для своего персонального УЦ.

Как вариант, можете задать имя корневого домена как ***nnnn-fio.ru***, где ***nnnn*** – это номер Вашей группы, а ***fio*** – Ваши инициалы на английском языке.

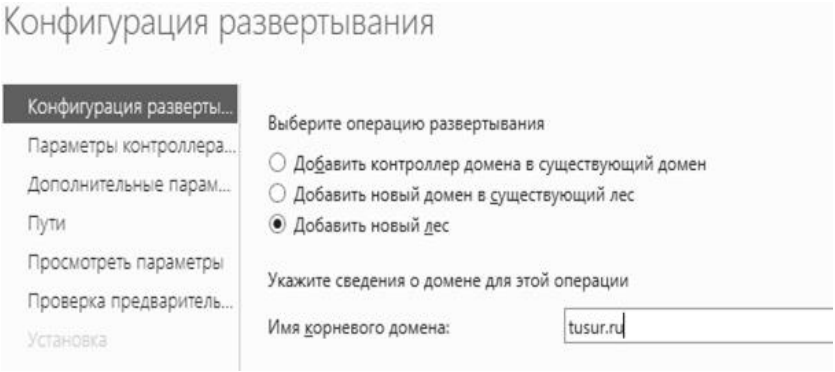

Рис. 8. Имя корневого домена

В следующем окне введите пароль для режима восстановления служб каталогов (DSRM) (рис. 9). Учтите, что пароль должен соответствовать требованиям безопасности. С учетом того, что данная работа посвящена не политике паролей, можно использовать простой пароль. Например: «123Qwer», «Tusur123» и т.д. Остальные настройки оставьте по умолчанию.

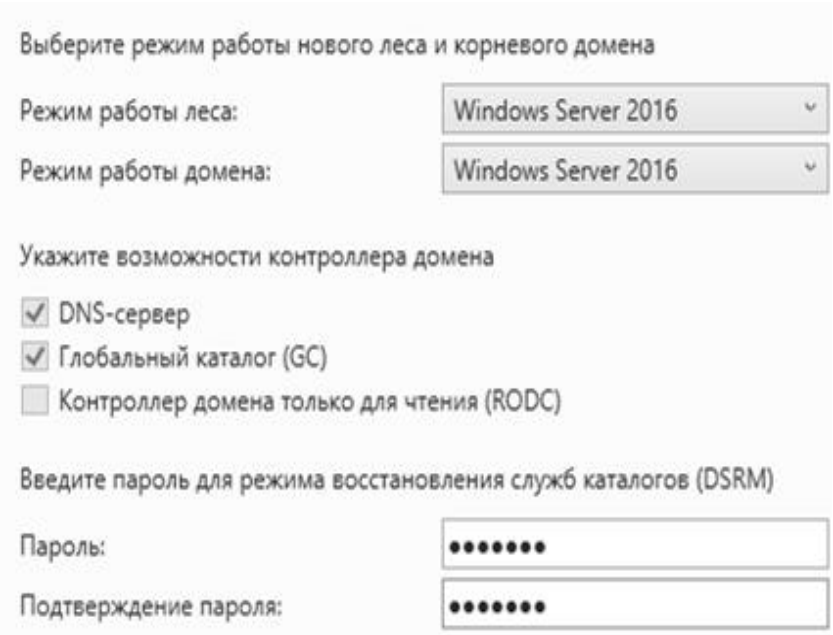

Рис. 9. Задание пароля для режима восстановления

Запустите установку, после её окончания будет предложена перезагрузка машины. Перезагрузите виртуальную машину.

После загрузки системы установите роль «Службы сертификации Active Directory». Для этого в диспетчере серверов снова выберете пункт «Добавить роли и компоненты» (рис. 1). Тип установки – «Установка ролей или компонентов», выбор сервера – «Выберете сервер из пула серверов». При выборе ролей сервера отметьте галочкой пункт «Службы сертификатов Active Directory» (рис. 2). Добавьте необходимые для установки компоненты в появившемся окне.

При выборе служб отметьте галочкой пункты «Центр сертификации» и «Служба регистрации в центре сертификации через Интернет». Добавьте необходимые для установки компоненты (рис. 10).

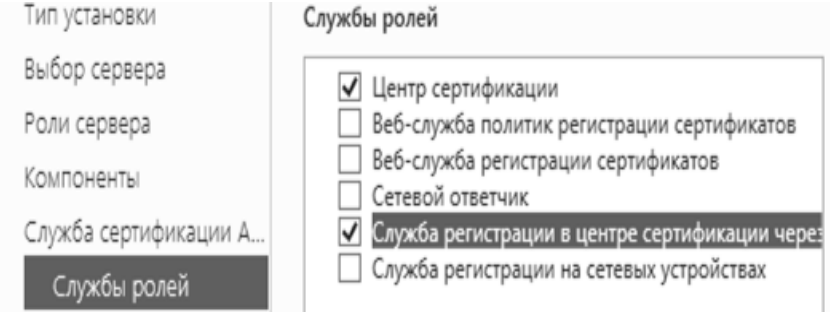

Рис. 10. Выбор служб ролей

Остальные настройки оставьте по умолчанию, запустите установку. Дождитесь окончания установки нажмите на синюю строку «Настроить службы сертификатов Active Directory на конечном сервере» (рис. 11).

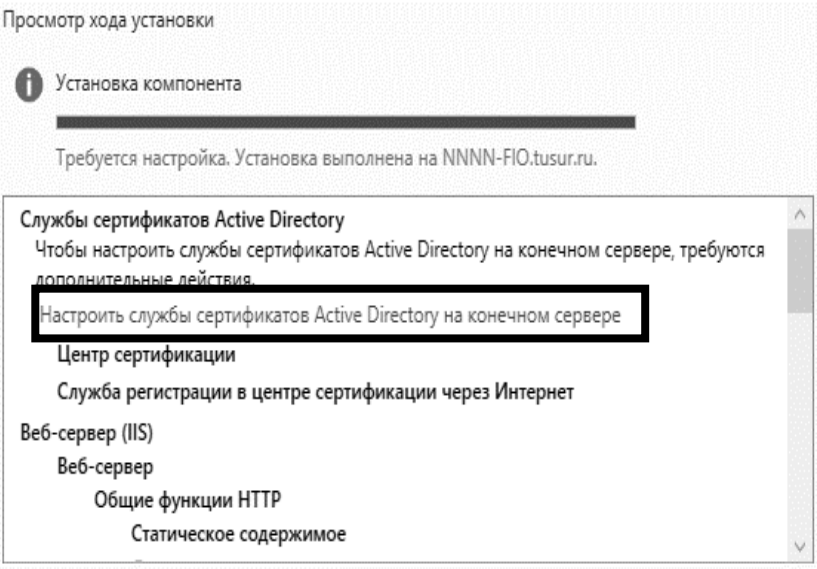

Рис. 11. Пункт «Настроить службы сертификатов AD на конечном сервере»

В появившемся окне при выборе служб ролей выберете пункты «Центр сертификации» и «Служба регистрации в центре сертификации через Интернет» (рис. 12). Выберите вариант установки – «ЦС предприятия» (рис. 13).

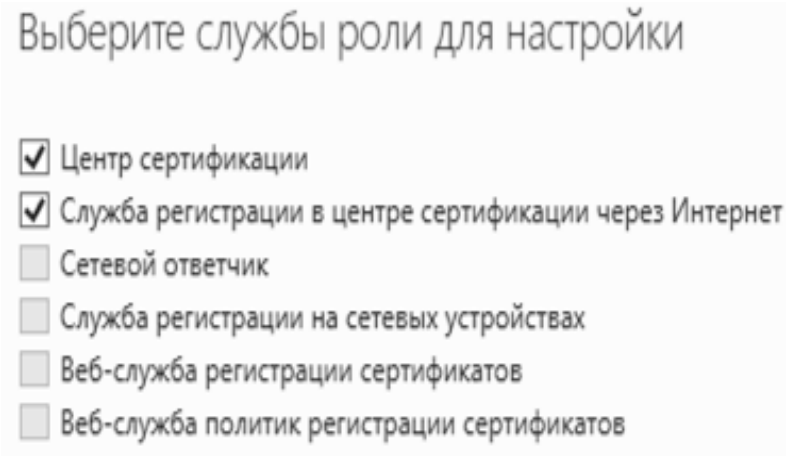

Рис. 12. Выбор служб ролей при настройке службы сертификатов AD

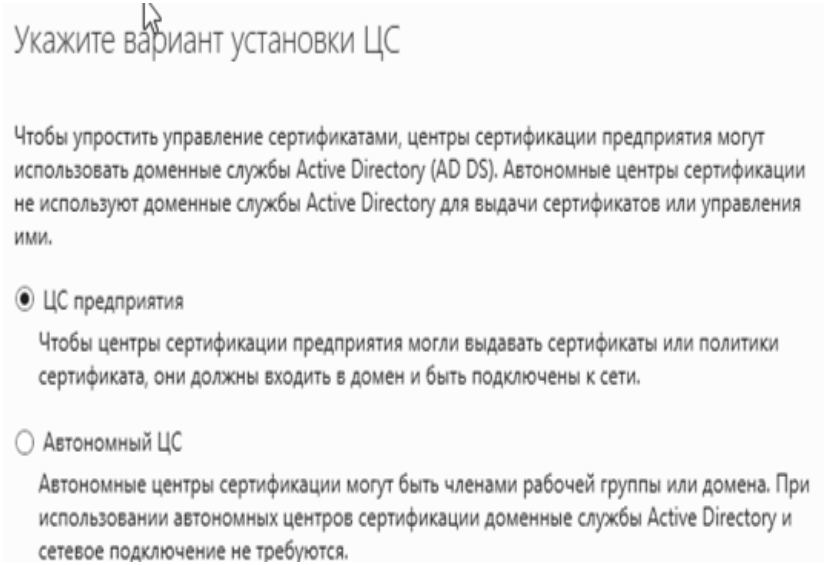

Рис. 13. Выбор варианта установки ЦС

При задании типа ЦС выберете «Корневой ЦС», так как для дальнейшей работы необходим «самостоятельный» ЦС (корневой), который способен сам выдавать и подписывать сертификаты (рис. 14).

Корневой центр сертификации может самостоятельно выдавать себе сертификаты. Такие сертификаты называются самоподписанными. В случае, если дальше необходимо будет относительно данного удостоверяющего центра построить иерархическую архитектуру, необходимо будет добавить подчиненные центры сертификации. Данный вопрос будет рассмотрен в следующих лабораторных работах.

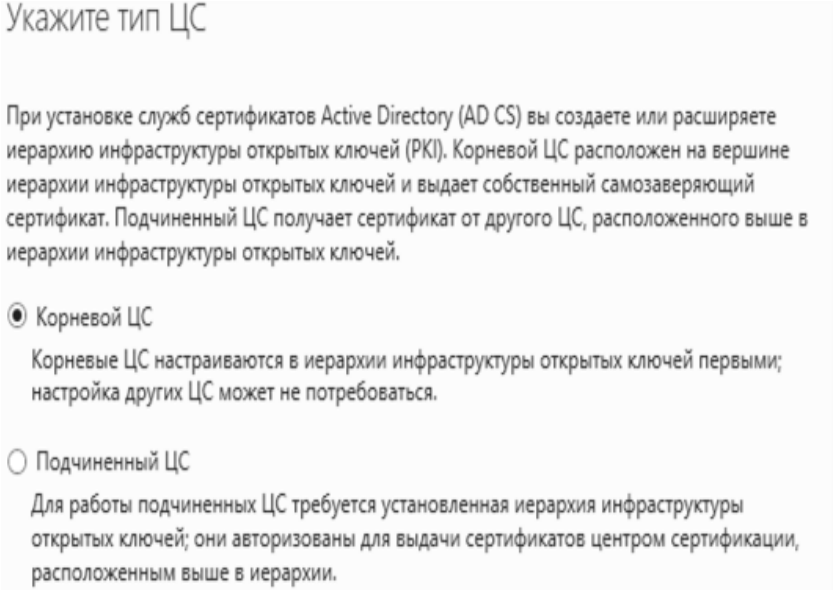

Рис.14. Выбор типа центра сертификации

Следующее окно позволяет выбрать тип закрытого ключа для работы будущего ЦС: готовый или новый закрытый ключ. Для выполнения лабораторной работы необходим новый ключ. Поэтому, выберете пункт «Создать новый закрытый ключ» (рис. 15).

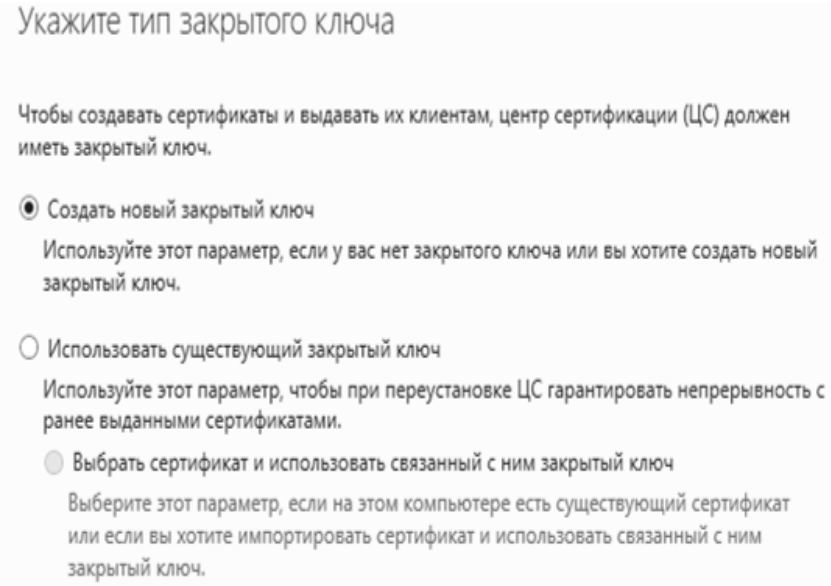

Рис. 15. Выбор типа закрытого ключа

После шага с выбором установки закрытого ключа требуется произвести некоторые настройки шифрования будущего ЦС. В данном окне нужно выбрать поставщика служб шифрования (CSP, дословно, **C**ryptographic **S**ervice **P**rovider).

Компания Microsoft по умолчанию предлагает для выбора CSP собственной разработки, который называется «RSA #Microsoft Software Storage Provider». Но также предоставляется возможность работы с другими поставщиками. Недостатки посторонних CSP в том, что не всегда имеется стабильность в их работе, а также если все-таки возникают проблемы в ходе работы, то, в отличии от поставщика Microsoft, для получения руководства пользователя необходимо будет обращаться к разработчикам данного CSP, что бывает затруднительно.

Данная лабораторная работа предусматривает работу с поставщиком по умолчанию – «RSA #Microsoft Software Storage Provider». Поэтому, настройки шифрования оставим по умолчанию, как и имя ЦС, срок действия ЦС (по умолчанию 5 лет) и расположение базы данных сертификатов.

В окне «Подтверждение» можно посмотреть все выбранные параметры. Для начала установки нажмите кнопку «Настроить».

3.1.2 Работа с веб-службой регистрации сертификатов

Теперь нужно добавить службу роли под названием «Веб-служба регистрации сертификатов», которая была пропущена в ходе основной установки службы сертификации Active Directory.

Для этого в диспетчере серверов перейдите на вкладку «Служба сертификации Active Directory». В рабочей зоне «Роли и компоненты», в выпадающем меню «ЗАДАЧИ», выберете пункт «Добавить роли и компоненты» (рис. 16).

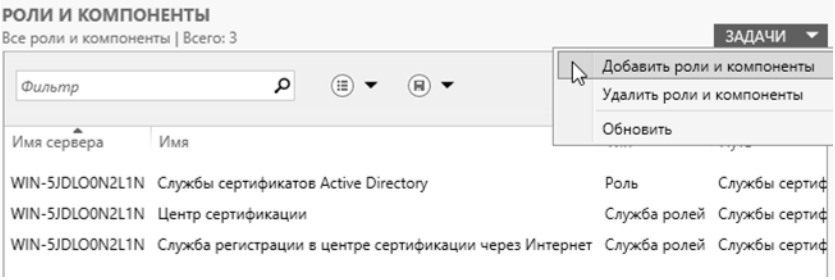

Рис. 16. Выбор пункта «Добавить роли и компоненты»

В появившемся окне выберете тип установки – «Установка ролей или компонентов», выбор сервера – «Выберете сервер из пула серверов». Во вкладке «Роли сервера» раскройте пункт «Службы сертификатов Active Directory» и отметьте галочкой пункт «Веб-служба регистрации сертификатов», добавьте необходимые компоненты для установки (рис. 17).

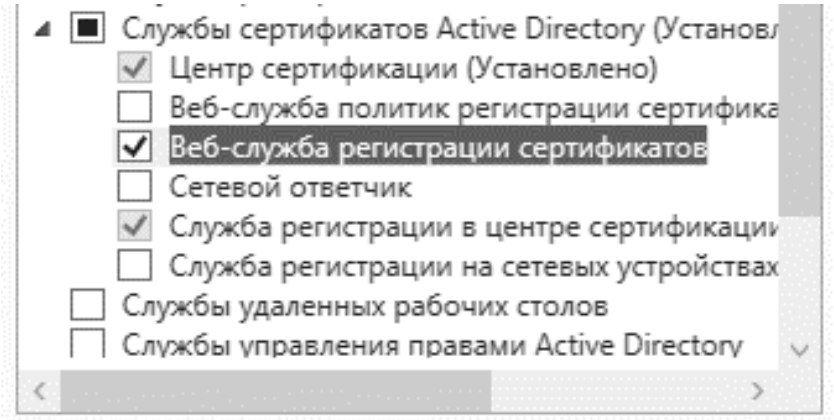

Рис. 17. Выбор службы «Веб-служба регистрации сертификатов»

Остальные настройки оставьте по умолчанию, после завершения установки нажмите на синюю строку «Настроить службы сертификатов Active Directory на конечном сервере» (рис. 18).

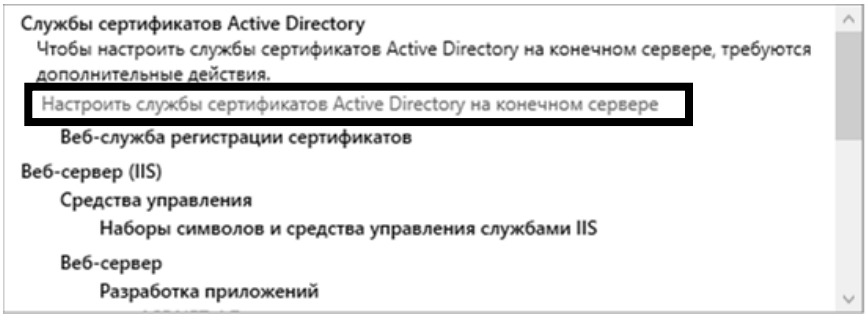

Рис. 18. Установка службы «Веб-служба регистрации сертификатов»

В появившемся окне выберите галочкой пункт «Веб-служба регистрации сертификатов». Далее необходимо выбрать ЦС, к которому будет прикреплена данная служба. Так как ранее был создан ЦС, выберете пункт «Имя ЦС» и убедитесь, что в строке ниже указанно верное имя ЦС (рис. 19).

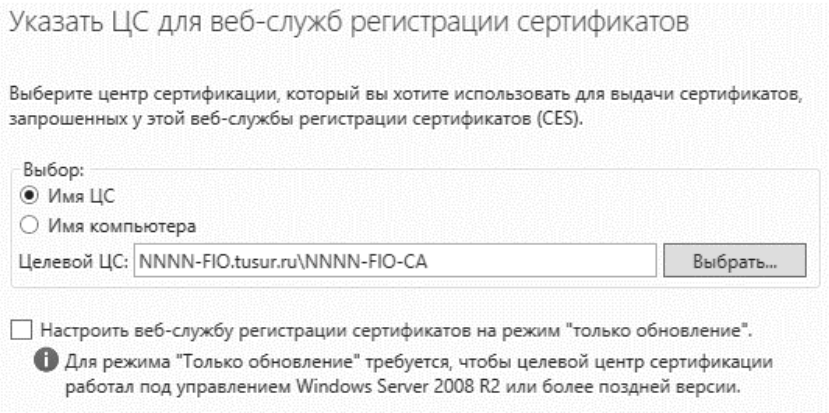

Рис. 19. Выбор ЦС для службы

В следующем окне выберите пункт «Имя и пароль пользователя». Учетная запись службы CES – «Использовать встроенный идентификатор пула приложений», сертификат сервера – «Выбрать существующий сертификат для шифрования SSL (рекомендуется)».

Далее в окне «Подтверждение» можно проверить все выбранные параметры. Запустите установку, после окончания установки перезагрузите виртуальную машину.

3.2 Настройка удостоверяющего центра

Вызовите консоль управления Microsoft. Для этого запустите командную строку меню «Пуск» – «Выполнить», после чего наберите команду «mmc». Появится окно консоли.

Далее, для работы с сертификатами в данной консоли необходимо добавить соответствующую оснастку. Нажмите сочетание клавиш на клавиатуре Ctrl+M или в меню «Файл» выберете пункт «Добавить или удалить оснастку…». В появившемся окне в левом поле выберите оснастку «Сертификаты» и нажмите кнопку «Добавить». Появится окно, в котором нужно выбрать пункт «учетной записи компьютера», потом – «локальным компьютером» (рис. 20-21).

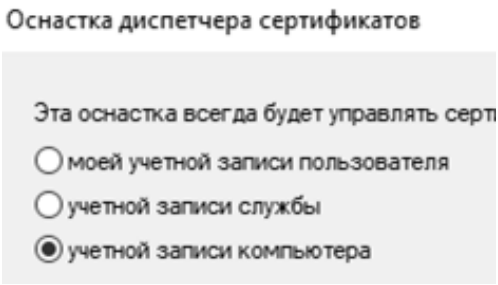

Рис. 20. Выбор управляющего оснасткой

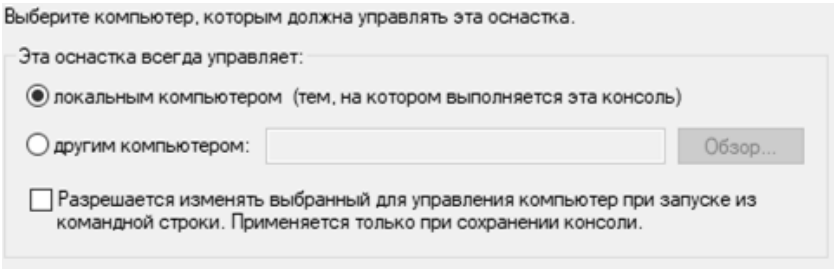

Рис. 21. Выбор компьютера

Если нажать в левом окне на вкладку «Сертификаты», то далее в выпадающем списке можно увидеть 11 папок, каждая из которых имеет физическое место хранения на жестком диске и свое имя,

характеризующее типы сертификатов, которые она содержит. Нажмите на папку с именем «Личное».

Вы можете увидеть в центральном поле существующий сертификат. После активации роли Active Directory Certificate Services - в списке сертификатов уже есть сертификат с коротким именем, совпадающим с именем ЦС (именно тот, в столбце «Назначения» которого указано «Проверка подлинности»). Но этот сертификат непригоден для доступа к веб-серверу по защищенному каналу, то есть необходимому протоколу HTTPS.

Получим сертификат для веб-сервера с новым ключом. Для чего в контекстном меню данного сертификата, выберем «Все задачи» – «Запросить сертификат с новым ключом» (рис. 22).

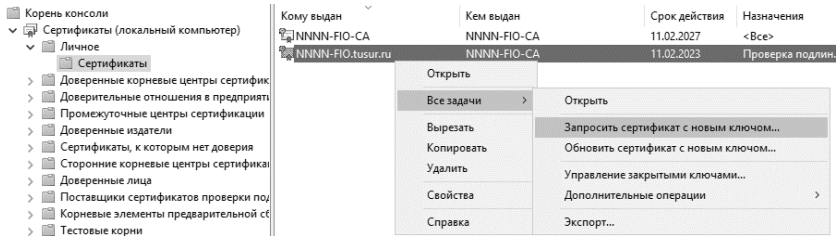

Рис. 22. Выбор пункта «Запросить сертификат с новым ключом»

В появившемся окне необходимо выбрать типы сертификатов. Ранее существующий сервер был сделан контроллером домена, поэтому в списке по умолчанию уже доступен сертификат типа контроллера домена. На данном этапе вмешательства не требуется. Нажмите кнопку «Заявка» (рис. 23).

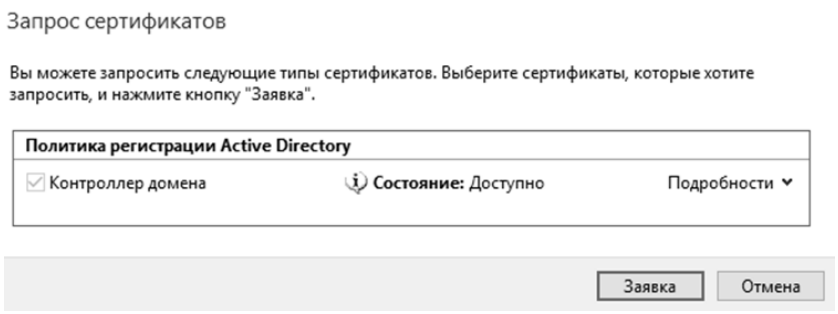

Рис. 23. Запрос сертификата

Далее будет выполнена установка сертификата. После успешной установки появится окно. Если все сходится и нет никаких ошибок, нажмите «Готово».

Приступим к связыванию сертификата с веб-сервером. Нажмите меню «Пуск» – «Выполнить». Наберите команду «InetMgr» (рис. 24). Или (без командной строки) меню «Пуск» – «Средства администрирования Windows» – «Диспетчер служб IIS».

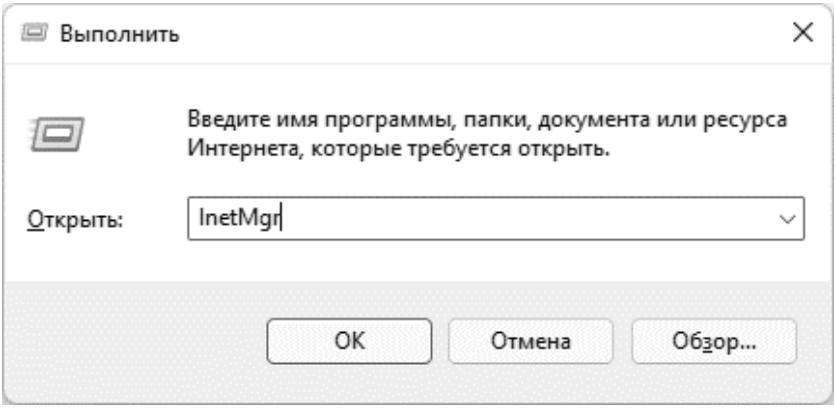

Рис. 24. Вызов программы управления информационными службами интернета

В левой части открывшегося окна необходимо нажать на название сервера, а затем «Сайт» – «Default Web Site» (правой кнопкой мыши) – «Изменить привязки» (рисунок 25).

В появившемся окне можно задать адрес, по которому с помощью браузера можно просто и беспрепятственно работать уже с веб-оболочкой ЦС. В данном случае не задано никакого конкретного адреса.

Для протокола https с помощью кнопки «Изменить» настроим параметры. Откроется окно изменения привязки сайта. Чтобы определить корректный IP-адрес виртуальной машины, к которому необходимо обращаться при работе с веб-сервером, в командной строке вызовите команду ***ipconfig*** (рис. 26).

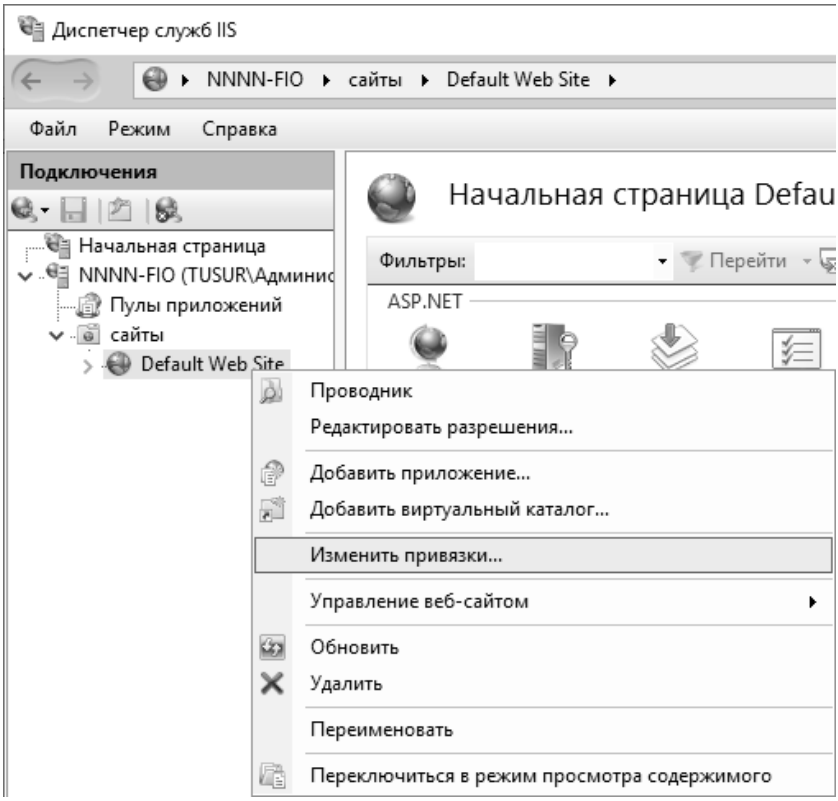

Рис. 25. Выбор пункта «Изменить привязки»

```
C:\Users\Администратор>ipconfig
Настройка протокола IP для Windows
Адаптер Ethernet Ethernet:
   DNS-суффикс подключения . . . . . :
   Локальный IPv6-адрес канала . . . : fe80::78f8:dc3e:6915:4227%6
   Автонастройка IPv4-адреса . . . . : 169.254.66.39
   Маска подсети . . . . . : 255.255.0.0
   Основной шлюз. . . . . :
```

Рис. 26. Определение IP-адреса виртуальной машины

Далее выберите IP-адрес виртуальной машины (в данном случае 192.254.66.39) и полученный недавно сертификат (рис. 27). В разделе «Имя узла» можно указать адрес в формате

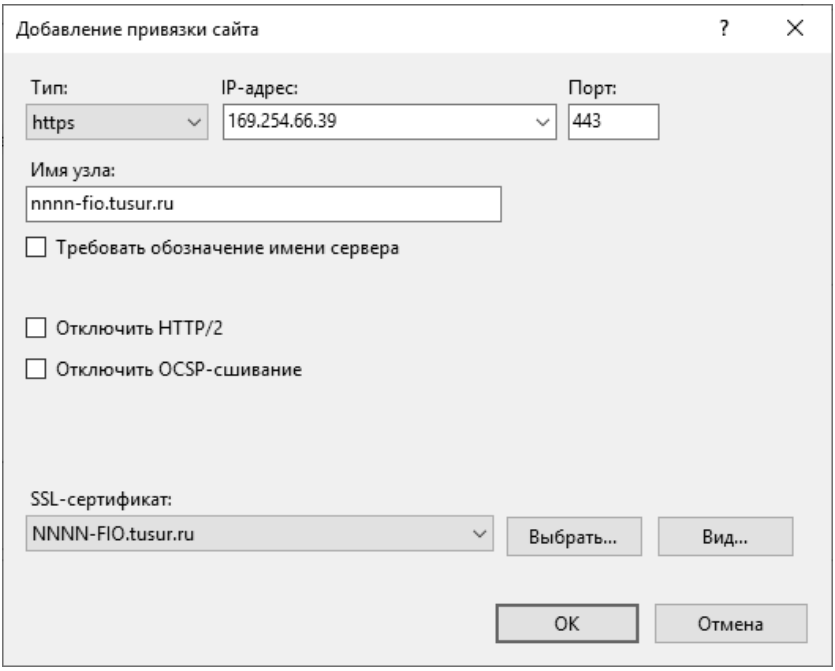

Рис. 27. Изменение привязки сайта

После изменения привязки сайта, в диспетчере служб IIS слева в разделе «Управление веб-сайтом», нажмите кнопку «Перезапустить» (рис. 28).

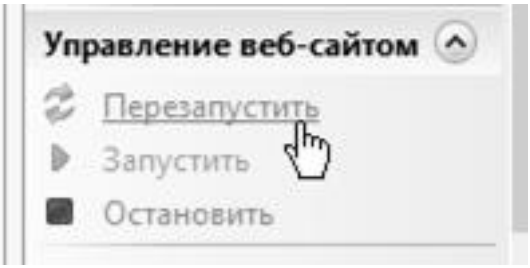

Рис. 28. Кнопка «Перезапустить»

Для проверки работоспособности Центра сертификации запустите браузер Internet Explorer. Можно перейти на сайт через обзор веб-сайта диспетчера службы IIS или в строке навигации набрать адрес

https://192.254.66.39/certsrv или ***https://nnnn-fio.tusur.ru/certsrv***, если указали данный адрес при привязке сайта (рис. 27).

При переходе на сайт может появиться (зависит от настроек браузера) сообщение как на скриншоте ниже (рис. 29).

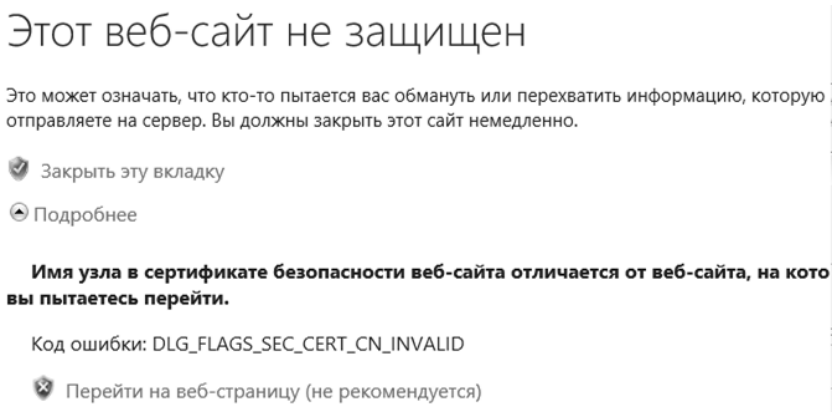

Рис. 29. Сообщение «Этот веб-сайт не защищен»

Нажмите «Перейти на веб-страницу (не рекомендуется)» или иную фразу, зависящую от браузера. Появится окно с вводом имени пользователя и пароля. Введите «администратор» и текущий пароль от учетной записи администратора.

При возникновении ошибки подобной на сообщении ниже (рисунок 30), добавьте веб-сайт в список надежных сайтов с помощью кнопки «Добавить».

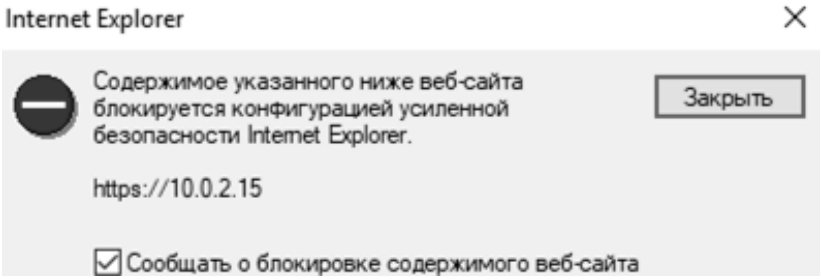

Рис. 30. Сообщение о блокировке содержимого веб-сайта

4. Задание на лабораторную работу

1. Ознакомиться с теорией (включая лекционные материалы).
2. Настроить удостоверяющий центр на виртуальной машине в соответствии с методическими указаниями.
3. Составить по проделанной работе отчет.

5. Контрольные вопросы

1. Опишите протокол взаимодействия в симметричных криптосистемах.
2. Приведите пример симметричных криптосистем.
3. В чем заключается проблема распределения ключей в симметричных криптосистемах?
4. Какие криптографические алгоритмы относятся к бесключевым?
5. Опишите протокол взаимодействия в криптосистемах с открытым ключом.
6. Приведите пример криптосистем с открытым ключом.
7. В чем заключается атака типа «Человек посередине»?
8. Каким образом можно обеспечить защиту ключей от подмены?
9. Перечислите технологии, входящие в Active Directory?
10. Какая технология Active Directory позволяет организовать работу инфраструктуры открытых ключей?

ЛАБОРАТОРНАЯ РАБОТА №5
Изучение функций удостоверяющего центра

1. Цель работы

Целью лабораторной работы является ознакомление базовыми функциями удостоверяющего центра: особенностями работы с оснастками, выдачей сертификатов и шаблонов сертификатов.

2. Краткие теоретические сведения

Функциональными элементами PKI-инфраструктуры являются: центры сертификации, центры регистрации, репозитарии и архивы.

Центры сертификации (УЦ – удостоверяющий центр, certification authority) выступает в роли нотариуса. Он подтверждает параметры подлинности взаимодействующих сторон в процессе электронного документооборота. УЦ выпускает сертификаты открытого ключа (СЕРТ| ОК) для каждого параметра подлинности, подтверждая, что параметр включает соответствующие зарегистрированные данные. Сертификаты открытого ключа обычно включают открытый ключ, информацию о параметре подлинности взаимодействующей стороны, обладающей закрытым ключом, период действия сертификата и электронной подписью удостоверяющего центра.

К основным функциям ЦС относятся:

- формирование собственного секретного ключа и сертификата ЦС;
- формирование сертификатов подчиненных Центров;
- формирование сертификатов открытых ключей конечных пользователей;
- формирование списка отозванных сертификатов;
- ведение базы всех изготовленных сертификатов и списков отозванных сертификатов.

Сертификат представляет собой структуру данных, которая содержит открытый ключ владельца сертификата и подписана электронной цифровой подписью его издателя. Назначение сертификата - удостоверение издателем подлинности связи между открытым ключом субъекта и информацией, его идентифицирующей.

Имеется десять основных полей (рис. 1): шесть обязательных и четыре опциональных. Большая часть информации, указываемой в сертификате, не является обязательной, а содержание обязательных полей сертификата может варьироваться. К обязательным полям относятся:

- серийный номер сертификата ***Certificate Serial Number***;
- идентификатор алгоритма подписи ***Signature Algorithm Identifier***;
- имя издателя **Issuer Name**;
- период *действия* ***Validity (Not Before/After)***;
- открытый ключ субъекта ***Subject Public Key Information***;
- имя субъекта сертификата ***Subject Name***.

Рис. 1. Структура сертификата X.509

Политикой применения сертификатов должно быть четко определено, в какой момент времени сертификаты и ключи становятся валидными и как долго сохраняют свой статус, а также когда необходимо их заменять или восстанавливать.

Важнейшим вопросом в смысле возможных правовых последствий применения электронной цифровой подписи является вопрос: когда сертификат становится валидным. Выпуск сертификата открытого ключа и подписание его УЦ после аутентификации лица, обращающегося с запросом о выдаче сертификата, не являются достаточным условием для придания сертификату статуса валидного. Сертификат становится валидным только после его открытой публикации в репозитории PKI, и наоборот, сертификат теряет статус валидного после его включения в список аннулированных сертификатов и публикации последнего.

3. Ход работы

3.1 Изучение механизма выдачи сертификата

Следующая лабораторная работа заключается в изучении особенностей выдачи сертификатов с помощью готовой веб-оболочки Центра сертификации. Перед Вами главная веб-страница ЦС (рис. 2).

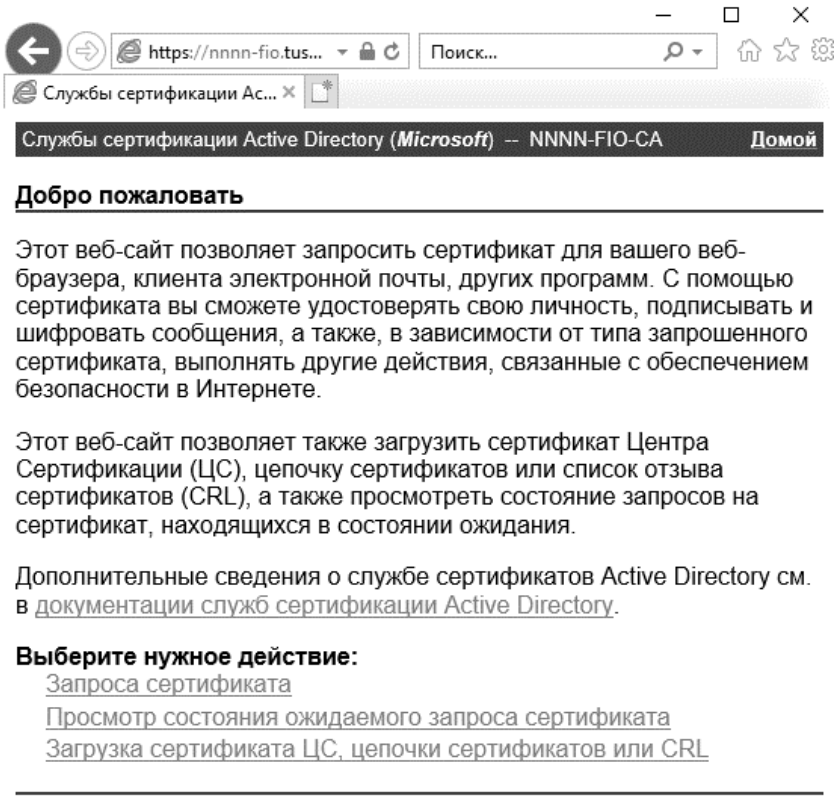

Рис. 2. Главная веб-страница ЦС

Прочитайте внимательно все написанное на странице. Также рекомендуется прочитать раздел «документация служб сертификации Active Directory».

Для того чтобы выдать сертификат данного ЦС необходимо нажать на «Запрос сертификата». На следующей странице можно выбрать уже готовый сертификат пользователя, либо воспользоваться

расширенными настройками запроса сертификата. Выберите второй вариант (рис. 3).

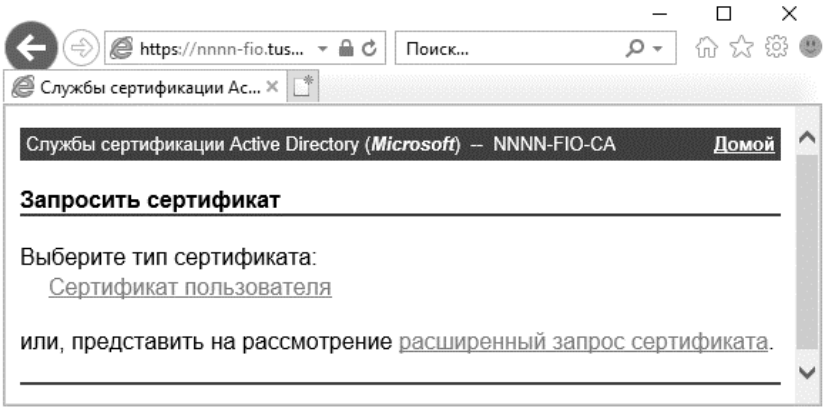

Рис. 3. Расширенный запрос сертификата

На следующей странице необходимо выбрать тип генерирования сертификата: либо полностью с первого шага создать сертификат, либо по имеющемуся запросу сертификата создать сертификат. Выберите «Создать и выдать запрос к этому ЦС» (рис. 4).

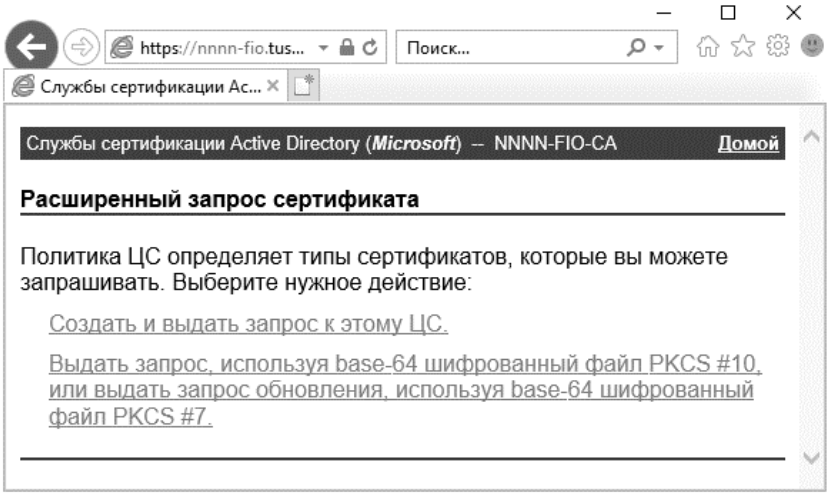

Рис. 4. Расширенный запрос сертификата

При появлении очередного сообщения нажмите кнопку «Да» и продолжите работу (рис. 5).

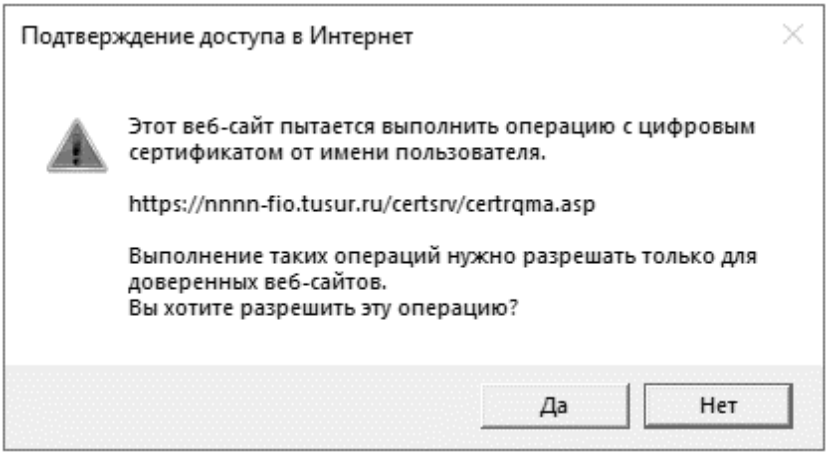

Рис. 5. Подтверждение доступа в Интернет

На следующей странице появится множество полей, которые необходимо заполнить. Тем самым пополняется информация о запрашиваемом сертификате: его назначение, кем он выдан и т.п. Разберем каждое из полей подробно.

Первый пункт – «Шаблон сертификата. При создании сертификата можно выбрать его готовый шаблон. В Active Directory доступно всего шесть шаблонов сертификатов. В таблице (табл. 1) представлено описание и возможности каждого из сертификатов.

Таблица 1

Шаблоны сертификата

Имя	**Описание**	**Использование ключа**	**Тип субъекта**
Пользователь	Используется пользователями для проверки электронной почты, EFS и клиента	Подпись и шифрование	Пользователь
Базовое шифрование EFS	Используется шифрованной файловой системой (EFS) для шифрования данных	Шифрование	Пользователь
Администратор	Разрешает подписывание списка доверия и проверку подлинности пользователя	Подпись и шифрование	Пользователь

Продолжение таблицы 1

Имя	Описание	Использование ключа	Тип субъекта
Агент восстановления EFS	Позволяет субъекту расшифровать файлы, ранее зашифрованные с помощью EFS	Шифрование	Пользователь
Веб-сервер	Удостоверяет подлинность веб-сервера	Подпись и шифрование	Компьютер
Подчиненный центр сертификации	Используется для доказательства подлинности корневого ЦС. Выдается родительским или корневым ЦС	Подпись	ЦС

Выберите шаблон сертификата – «Пользователь». Переходим к следующему параметру – «Параметры ключа». Для начала необходимо выбрать: создать новый набор ключей или использовать существующие. Выберите «Создать новый набор ключей» (рис. 6).

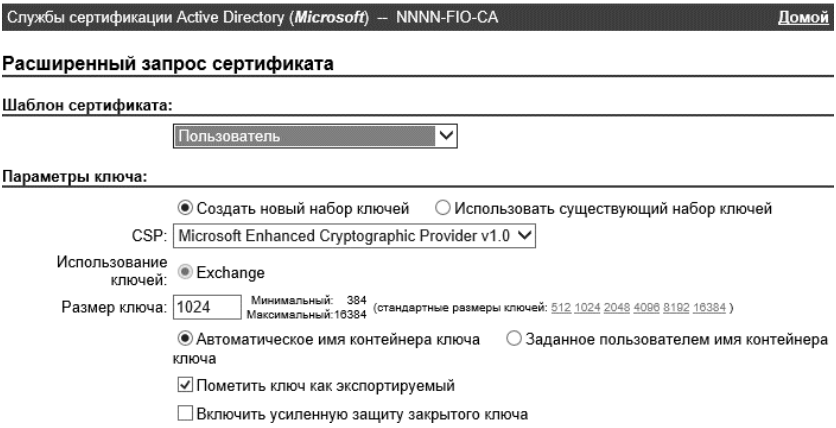

Рис. 6. Составленный запрос

В пункте (CSP - Cryptography Service Provider - криптопровайдер) по умолчанию выбран «Microsoft RSA SChannel Cryptographic Provider». Поставщик службы шифрования (CSP) отвечает за создание, уничтожение и использование ключей в различных криптографических операциях. Одни поставщики предоставляют криптографические алгоритмы повышенной надежности, другие используют аппаратные компоненты, такие как смарт-карты. Существует несколько версий

данного криптопровайдера от компании Microsoft. У каждого свое назначение. Что касается Microsoft RSA SChannel Cryptographic Provider, он предоставляет функциональность для реализации электронной подписи.

Далее идет пункт, касающийся размера ключа. По умолчанию для него задан размер в 1024 бит. Для улучшения безопасности можно выбрать больший размер, но вместе с тем в геометрической прогрессии будет расти и время генерации ключа. Рекомендуется выбрать значение 2048, являющееся достаточным с точки зрения соотношения безопасность/время генерации.

Следующими идут 2 параметра: «Пометить ключ как экспортируемый» и «Включить усиленную защиту закрытого ключа». Если ключи помечены как экспортируемые, открытый и закрытый ключи можно сохранить в файле PKCS 12. Это может быть полезно при смене компьютера и перенесении пары ключей или при удалении пары ключей и сохранении ее в безопасном месте. Второй параметр означает следующее: если усиленная защита закрытого ключа включена, пароль будет запрашиваться при каждом использовании закрытого ключа. Данные пункты не являются ключевыми в выдаче сертификата, поэтому обучающийся самостоятельно может выбрать изменять или нет данные пункты.

Теперь переходим к параметру «Формат запроса». При работе с данным ЦС можно воспользоваться двумя типами форматов запросов: CMC и PKCS10. Запрос на новый сертификат создается в формате PKCS10, а запрос на обновление действующего сертификата — в формате CMC (RFC 5272).

Настройка параметра «Алгоритмы хэширования» влияет только на подписание запроса. Хороший алгоритм хэширования не позволяет создать два независимых набора входных данных, имеющих одинаковые хэш-коды. Примерами алгоритмов хеширования являются MD2, MD4, MD5 и SHA-1.

Если требуется отправить запрос позже, можно также выбрать пункт «Сохранить запрос». Данный запрос сохранится на вашем жестком диске в виде текстового файла. После создания запроса, нажмите кнопку «Выдать».

Появится окно выдачи сертификата (рис. 7). Нажмите «Установить этот сертификат». После скачивания сертификата появится уведомление об этом (рис. 8).

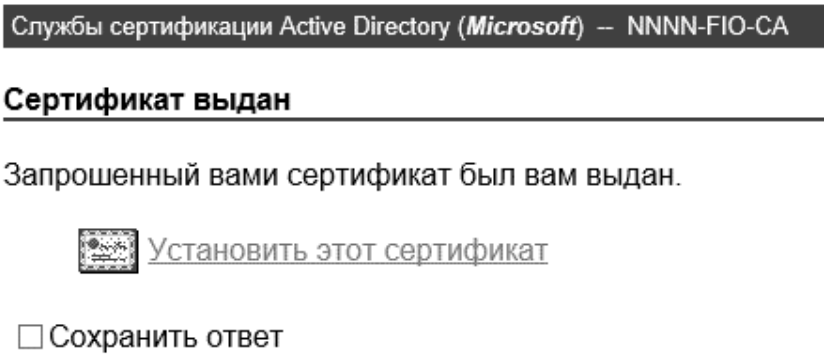

Рис. 7. Окно выдачи сертификата

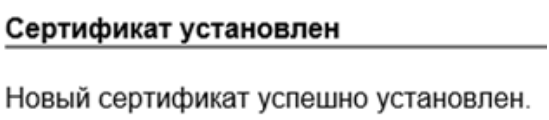

Рис. 8. Окно выдачи сертификата

3.1 Работа с шаблонами сертификатов

Добавьте в консоль управления Microsoft оснастки «Шаблоны сертификатов» и «Центр сертификации». Выданный сертификат можно увидеть в оснастке «Центр сертификации», в папке «Выданные сертификаты» (рис. 9).

Перейдем к созданию и настройке собственного шаблона. В качестве основы будет использоваться один из существующих шаблонов для упрощения настройки. В контекстном меню шаблона «Вход со смарт-картой» и выберите «Скопировать шаблон» (рис. 10).

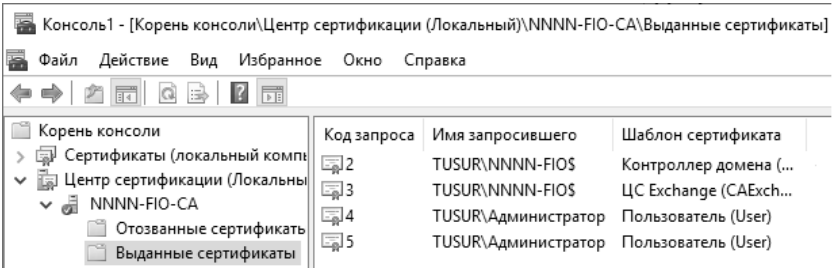

Рис. 9. Установленный сертификат

Появится окно свойств нового шаблона.

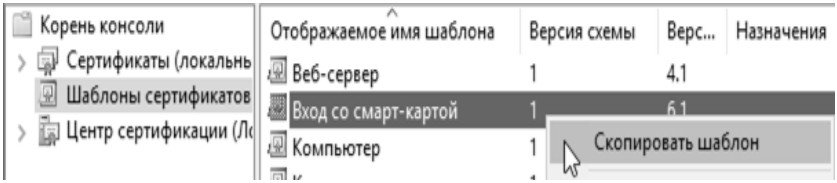

Рис. 10. Копирование шаблона

Вкладка «Общее», в поле «Отображаемое имя шаблона» вводится имя для шаблона. Можно применить имя, предложенное по умолчанию. Строка «Имя шаблона» будет тем же самым что и «Отображаемое имя шаблона», только без пробелов.

Параметры достоверности по умолчанию и периода обновления для сертификатов, выдаваемых службами сертификатов Active Directory (AD CS), предназначены удовлетворить большинство требований безопасности. Однако для сертификатов, используемых определенными группами пользователей, может потребоваться указать другие параметры достоверности и обновления, такие как более короткие срок действия или периоды обновления. За это отвечают два поля «Период действия» и «Период обновления».

Параметр «Опубликовать сертификат в Active Directory» определяет, будут ли сведения о шаблоне сертификата доступными по всему предприятию.

Параметр «Не использовать автоматическую перезаявку, если такой сертификат уже существует в Active Directory» дает возможность обновлять сертификаты, но предотвращает выдачу нескольких дубликатов сертификатов. С помощью этого параметра автоматическая подача заявки на сертификат не подаст запрос повторной заявки, если в доменных службах Active Directory существует дубликат сертификата.

Запишите в поле «Отображаемое имя шаблона» – свой номер группы и инициалы на английском языке в формате: NNNN-FIO (в качестве примера на дальнейших изображениях будет использоваться именно это название), поля Период действия» и «Период обновления» оставим по умолчанию, отметим пункт «Опубликовать сертификат в Active Directory» (рис. 11).

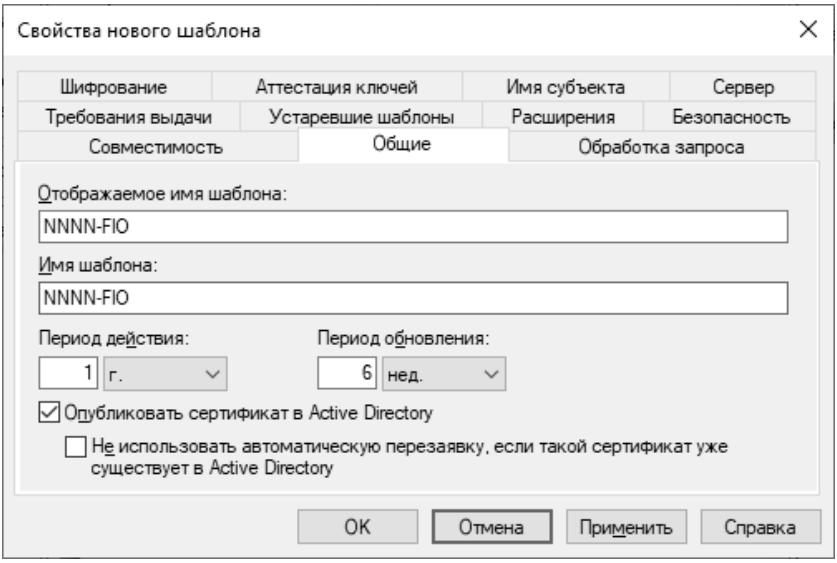

Рис. 11. Свойства шаблона, вкладка «Общие»

Далее перейдите на вкладку «Обработка запроса». В строке «Цель» указывается назначение сертификата определяет предполагаемое основное использование сертификата и, может быть, одним из четырех параметров, описанных в табл. 2.

Таблица 2

Назначения сертификатов

Параметр	Назначение
Шифрование	Содержит шифровальные ключи для шифрования и дешифрования.
Подпись	Содержит шифровальные ключи только для подписи данных.
Подпись и шифрование	Охватывает все основные применения шифровального ключа сертификата, включая шифрование данных, дешифрование данных, первоначальный вход в систему и цифровое подписывание данных.
Подпись и вход со смарт-картой	Разрешает первоначальный вход в систему с помощью смарт-карты и цифровую подпись данных. Нельзя использовать для шифрования данных.

Параметр «Включить симметричные алгоритмы, разрешенные субъектом» позволяет администратору выбрать алгоритм стандарта AES для шифрования закрытых ключей, когда они передаются в ЦС для архивации ключа. Если установлен этот параметр, клиент будет использовать симметричное шифрование AES-256 (наряду с сертификатом обмена ЦС для асимметричного шифрования), чтобы отправить закрытый ключ в ЦС для архивации. Если этот параметр не установлен, используется симметричный алгоритм 3DES. Поскольку архивация ключа предназначена для ключей шифрования (а не для ключей подписывания), этот параметр задействован, только если в поле «Цель» установлено значение «Шифрование».

Установите значение следующих поля «Цель» – «Подпись и шифрование», поставьте галочки напротив пунктов Включить симметричные алгоритмы, разрешенные субъектом» и «Архивировать закрытый ключ» (рис. 12).

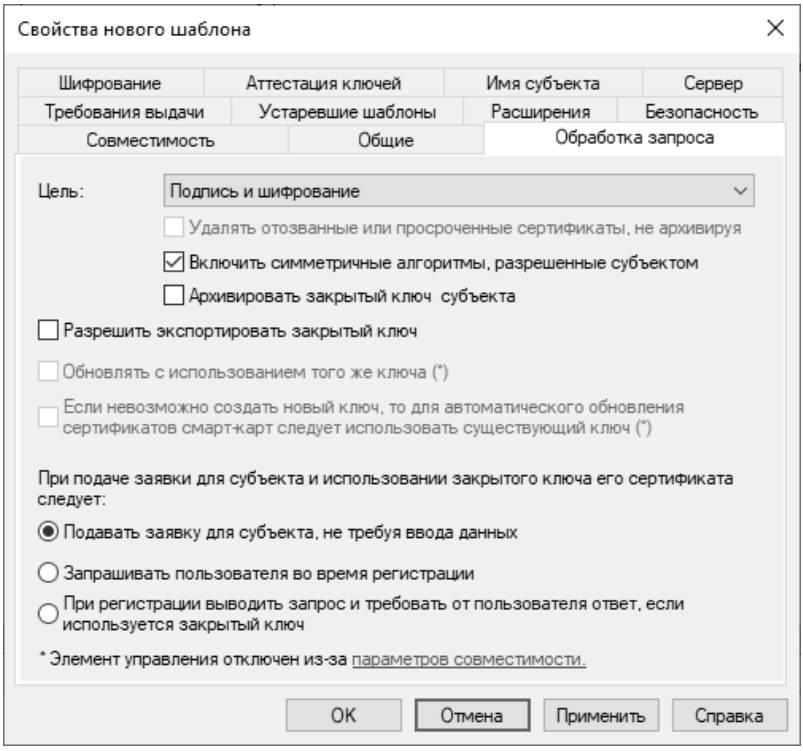

Рис. 12. Свойства шаблона, вкладка «Обработка запроса»

В данном примере не выделена опция «Архивировать закрытый ключ субъекта». Ее настоятельно рекомендуется использовать с базовым шаблоном сертификата шифрованной файловой системы (EFS), чтобы защитить пользователей от потери данных. Полезной она, может быть, и для других типов. Архивация ключа не защищает пользователей, пока они не подали заявку на сертификат, для которого включено восстановление ключа. Если они обладают идентичными сертификатами, выданными до включения восстановления ключа, архивация ключа не охватывает их. Клиенты, если у них уже есть действительный сертификат, основанный на старом шаблоне, должны заново подать заявку на получение сертификата, основанного на измененном шаблоне.

На вкладке «Шифрование» в поле «Минимальный размер ключа» рекомендуется сохранить значение по умолчанию. Нажмите кнопку «ОК». В результате получается собственно созданный новый шаблон сертификата «NNNN_FIO» (рис. 13).

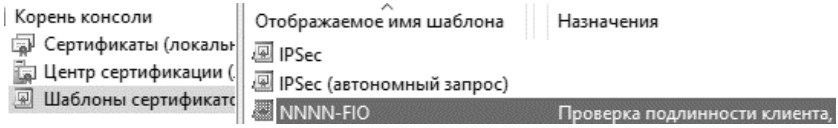

Рис. 13. Созданный шаблон сертификата «NNNN_FIO»

В предыдущих пунктах было описание того, как создавать новый шаблон. Но как можно заметить, в столбце «Назначение» у созданного шаблона сертификата значение исходного шаблона, который был продублирован: «Вход со смарт-картой, проверка подлинности клиента, Проверка подлинности сервера, Проверка подлинности центра распространения ключей». Это все является расширением (политикой применения) шаблона «Проверка подлинности Kerberos».

Политика применения шаблонов строится на основании так называемых объектных идентификаторов или иначе «деревьев-OID».

Объектный идентификатор (OID) — это уникальный набор чисел, разделенных точками. OID имеет уникальное значение, которое связано с объектом и однозначно идентифицирует его в мировом адресном пространстве объектов. Объектные идентификаторы распределяются иерархически. Как правило, рекомендуется назначать объектные идентификаторы политикам сертификатов, разрабатываемым организацией, и включать ссылки на них, а также ссылки на регламент удостоверяющего центра в сертификаты открытых ключей, издаваемые в соответствии с этими политиками сертификатов. Так же можно

назначать OID сертификатам центров сертификации, спискам отозванных сертификатов, регламентам и любым другим объектам, используемым при организации работы удостоверяющего центра.

Следует определить правила построения дерева объектных идентификаторов. Российский корень дерева идентификаторов объектов имеет следующий вид: {iso(1) member-body(2) ru(643)}.

Суффиксы следующего уровня:

{Операторы связи (1)} — регистрирующая организация REG1;

{Производители ПО (2)} — регистрирующая организация REG2;

{Удостоверяющие центры (3)} — регистрирующая организация REG3;

{Банки (4)} — регистрирующая организация REG4.

Соответственно, какая–либо организация, предоставляющая услуги удостоверяющего центра в России, может иметь OID 1.2.643.3.XXX. Зарегистрировавшись, организация получает статус организации-эмитента и может инициировать создание новых объектных идентификаторов. Порядок инициирования нового OID определяется организацией-эмитентом. То есть, организация разрабатывает свой порядок и принципы инициализации объектных идентификаторов. Можно при этом воспользоваться понятиями объектный класс и подкласс. Например, введем объектный класс документ. Уточним его подклассом тип документа. В этом контексте типами документов могут являться политики сертификатов, регламенты и т. п. Теперь мы можем определить конкретный объект — регламент корневого удостоверяющего центра, принадлежащий классу документов и подклассу регламентов.

Объектные идентификаторы OID шаблонов, уже по умолчанию хранящихся в УЦ, можно посмотреть. Для этого в консоли вызовете контекстное меню оснастки «Шаблоны сертификатов» и выберете пункт «Просмотр идентификаторов объектов» (рис. 14).

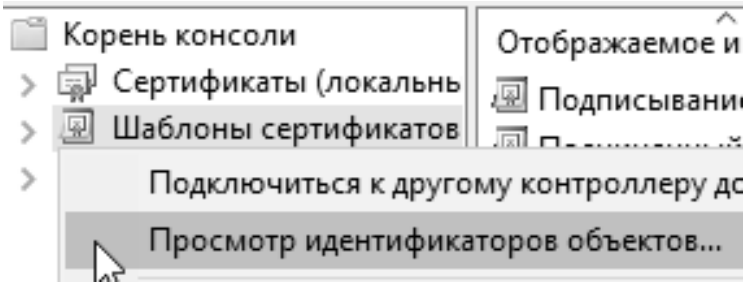

Рис. 14. Пункт «Просмотр идентификаторов объектов»

Появится окно просмотра идентификаторов объектов. Данное окно содержит три поля «Имя политики», «Идентификатор объекта» и «Тип политики» (рис. 15). Проанализируете несколько идентификаторов.

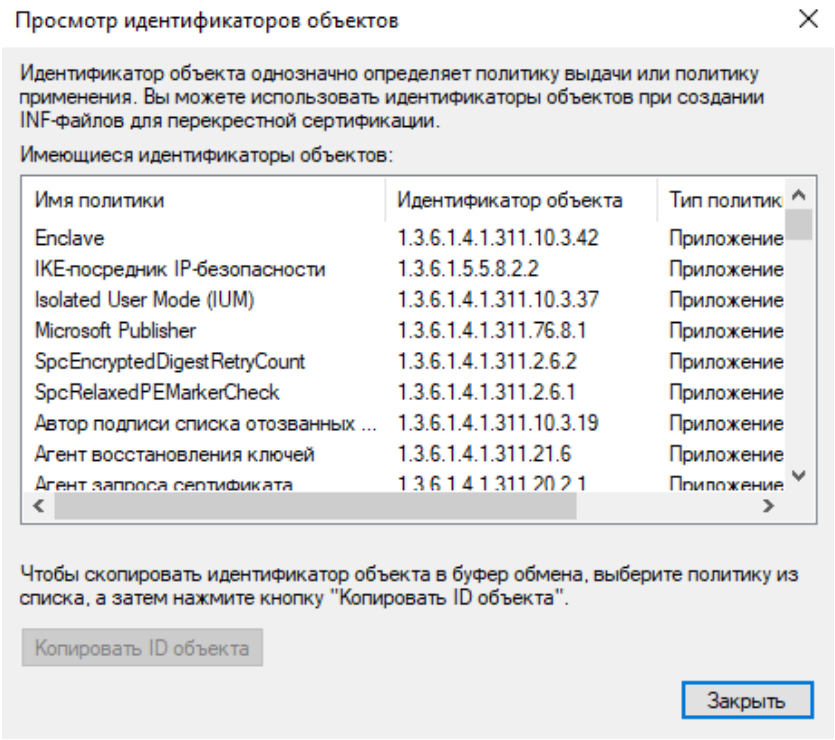

Рис. 15. Окно просмотра идентификаторов объектов

Теперь для созданного шаблона пропишите свой OID. Для этого перейдите в оснастку «Шаблоны сертификатов», нажмите правой кнопкой на шаблоне «NNNN_FIO» и выберите пункт «Свойства». Перейдите на вкладку «Расширения» (рис. 16).

Выберите расширение «Политики применения» и нажмите кнопку «Изменить». В новом окне удалите все существующие политики. После этого добавьте новый объектный идентификатор. Для этого нажмите кнопку «Добавить». В появившемся окне можно выбрать уже готовую политику, но для наглядности создайте свою собственную, нажмите «Создать».

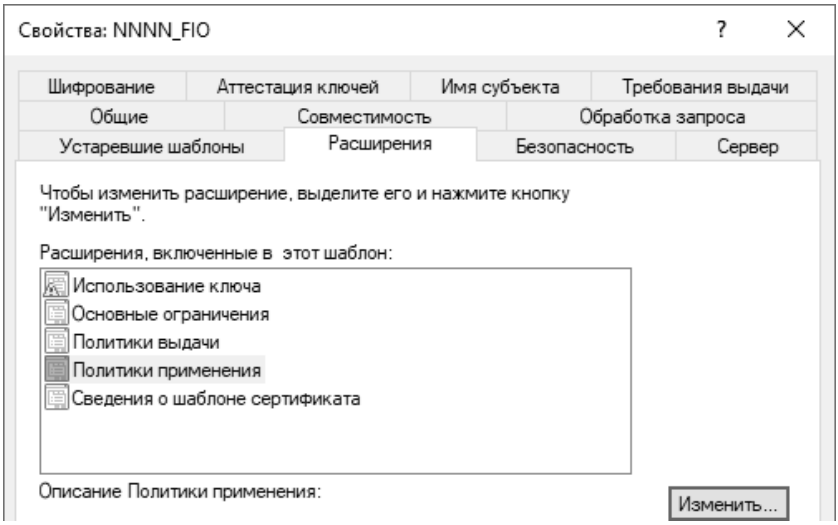

Рис. 16. Свойства шаблона, вкладка «Расширения»

Создайте персональный идентификатор OID. Очистите поле «Идентификатор объекта» и запишите туда OID «1.2.643.3.NNNN.M», где NNNN – это номер Вашей группы, а M – порядковый номер в списке группы. В поле ИМЯ запишите «Ключи электронной подписи» (рис. 45).

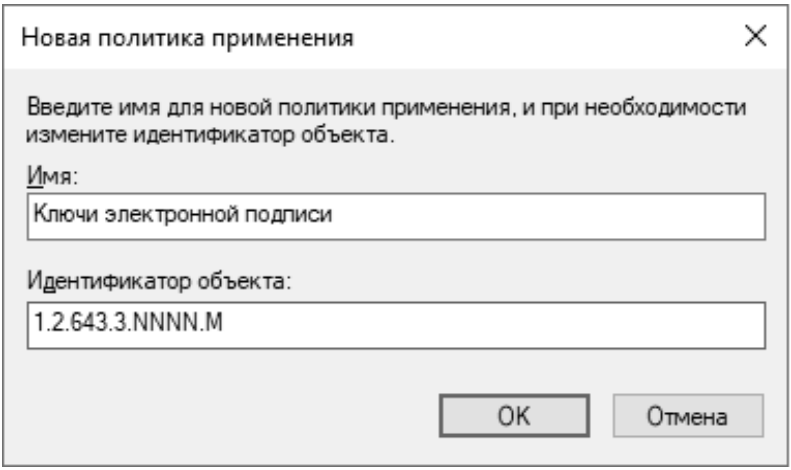

Рис. 17. Новая политика применения

Нажмите «ОК» и добавьте новую политику применения (рис. 18).

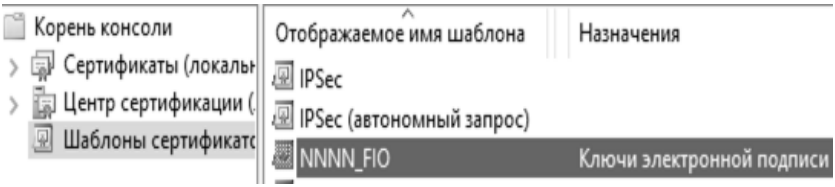

Рис. 18. Измененный шаблон

Перейдите в оснастку «Центр сертификации», вызовите контекстное меню папки «Шаблоны сертификатов», выберите пункт «Создать» – «Выдаваемый шаблон сертификата» (рисунок 47).

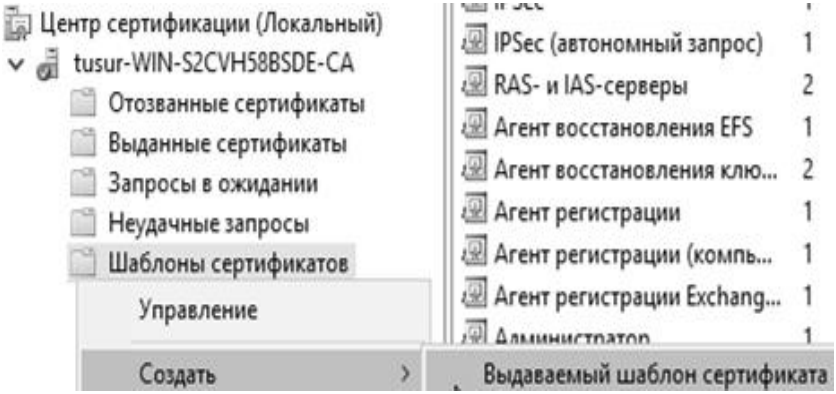

Рис. 19. Пункт «Выдаваемый шаблон сертификата»

В появившемся окне выберете созданный шаблон (рис. 20). Нажмите «ОК». Обратите внимание, что в столбце «Назначение» у Вас будет отображен объектный идентификатор, заданный Вами в процессе создания новой политики. В качестве примера при составлении методического руководства был использован OID «1.2.643.3.0000.0». Настоятельно рекомендуется в процессе выполнения работы ориентироваться не только на изображения, но и читать текст, который дается к ним.

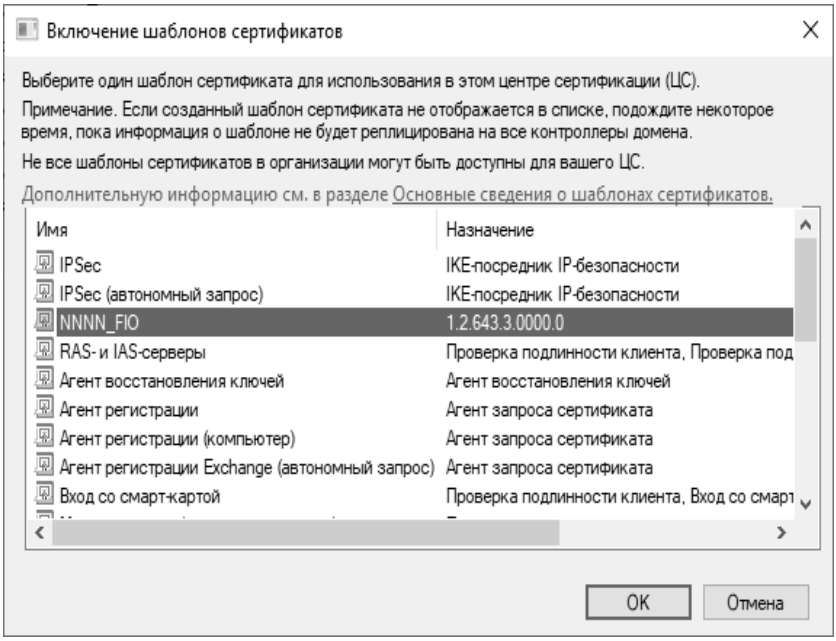

Рис. 20. Включение шаблонов сертификатов

Теперь при работе с сертификатами через веб-интерфейс можно выбрать созданный вами шаблон с уже прописанными объектным идентификатором.

Для этого вновь перейдем к веб-интерфейсу центра сертификации и сформируем расширенный запрос сертификата. В поле «Шаблон сертификата» в выпадающем списке будет представлен добавленный нами шаблон (рис. 21). Поскольку каких-либо важных изменений в его параметрах мы не осуществляли, оставим заполнение всех полей стандартным. Нажмите на кнопку «Выдать».

В результате центр сертификации выдаст сертификат, сформированный по нашему шаблону. Можете открыть полученный сертификат и проверить значения полей. То, что у сертификата используется объектный идентификатор, заданный добавленной Вами политикой, можно увидеть по полю «Улучшенный ключ».

Рис. 21. Выбор созданного шаблона сертификатов для выдачи

4. Задание на лабораторную работу

1. Ознакомиться с теорией (включая лекционные материалы).

2. Настроить удостоверяющий центр на виртуальной машине в соответствии с методическими указаниями.

3. Создать собственный шаблон сертификата с индивидуальный объектным идентификатором и выдать сертификат по данному шаблону.

4. Составить по проделанной работе отчет.

5. Контрольные вопросы

1. Какие функции выполняет удостоверяющий центр?
2. Что такое сертификат и какую функцию он выполняет?
3. Какие форматы сертификатов Вам известны?
4. Перечислите основные поля, содержащиеся в сертификате формата X.509?
5. Объясните разницу между централизованным и децентрализованным изданием сертификатов. Какой вид рассматривается в лабораторной работе?
6. Что такое объектный идентификатор (OID)?
7. Для чего нужен объектный идентификатор (OID)?
8. Для каких шаблонов рекомендуется использование опции «Архивировать закрытый ключ субъекта»?
9. Опишите жизненный цикл сертификата.
10. Приведите примеры ситуаций, при которых доверие к сертификату может быть подорвано до истечения срока его действия.

ЛАБОРАТОРНАЯ РАБОТА №6
Кросс-сертификация удостоверяющих центров

1. Цель работы

Целью лабораторной работы является ознакомление с процедурой кросс-сертификации - установление доверия между двумя удостоверяющими центрами.

2. Краткие теоретические сведения

Функциональными элементами PKI-инфраструктуры являются:

Ключевой аспект PKI — это доверие. То есть оба участника аутентификации или обмена сообщениями должны доверять центрам сертификации, которыми выданы сертификаты.

Рассмотрим обращение, например, к банковскому сайту по HTTPS. Прежде чем создается защищенное соединение, пользователь должен убедиться, что подключается именно к тому сайту, к которому планировал. Аутентификация сайта происходит с использованием SSL-сертификата. Среди прочего проверяется, что сертификат выдан именно для того сайта, к которому происходит обращение, что сертификат может быть использован для аутентификации сервера, что сертификат не был отозван, что данные в сертификате не были изменены третьей стороной. Последняя проверка требует проверки подписи УЦ, который выдавал сертификат для сервера. То есть необходимо получить сертификат ключа УЦ и выполнить аналогичные проверки для этого сертификата. Опять же, сертификат УЦ должен быть заверен какой-то подписью… До какого момента длятся такие проверки? До тех пор, пока не встретится сертификат УЦ, который находится в списке доверенных сертификатов удостоверяющих центров на стороне клиента. Откуда берутся такие списки? Есть несколько вариантов: списки поставляются вместе с ОС и обновлениями, или доверенные УЦ добавляются администратором или самим пользователем.

Стоит упомянуть еще и самоподписанные сертификаты. Корневые удостоверяющие центры выдают сертификаты сами себе, то есть УЦ1 выдает сертификат для ключа УЦ1, заверенный подписью УЦ1. Такие самоподписанные сертификаты являются основой доверия, и с одной стороны они должны быть доступны всем участникам PKI, а с другой — в случае компрометации или подмены такого сертификата вся система должна перестраиваться заново, с перевыпуском всех сертификатов и защищенным распространением всем пользователям нового корневого сертификата. Существуют коммерческие

удостоверяющие центры, которым автоматически доверяют все пользователи ОС, а также пользователи различных браузеров, от Konqueror до Google Chrome.

С партнерами, или в случае слияний, строятся различные отношения доверия между несколькими УЦ. Для этого используются кросс-сертификаты (сертификат с ключом УЦ1 заверяется подписью УЦ2 и наоборот), которые показывают взаимное доверие между УЦ нескольких организаций.

Рис. 1. Базовые схемы моделей доверия удостоверяющих центров

Наиболее распространены три модели доверия (рисунок 1):

Мостовая (Bridge CA Model). В данной модели существует центральный (мостовой) УЦ, которому доверяют все остальные УЦ.

Такая модель позволяет осуществлять централизованное управление при небольшом количестве кросс-сертификатов. В качестве примера можно привести реализацию US government's Federal Bridge Certification Authority.

В **сетевой** модели все УЦ считаются равноправными, и создается до n2 кросс-сертификатов. Кросс-сертификация на уровне корневых УЦ может быть не всегда желательной, в этом случае используются схемы кросс-сертификации на уровне подчиненных УЦ с ограничением доверия.

Иерархическая модель обычно используется в компаниях с разветвленной структурой, когда есть корневой УЦ и подчиненные, например, в филиалах.

Кроме того, иерархическая модель позволяет минимизировать затраты при перестроении инфраструктуры в случае компрометации ключа УЦ. Действительно, если происходит компрометация ключа одного из издающих (подчиненных) УЦ, то необходимо переиздать только те сертификаты, которые были выданы этим УЦ. Более того, такая модель позволяет создавать УЦ с различными регламентами в рамках одной инфраструктуры.

Еще встречаются гибридные модели и списки доверенных сертификатов, распространяемых между заинтересованными сторонами.

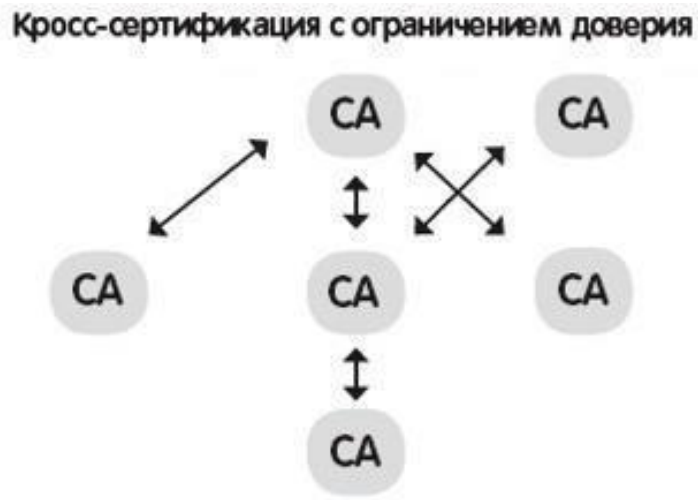

Рис. 2. Кросс-сертификация с ограничением доверия

При проверке сертификата необходимо построить цепочку сертификатов до доверенного УЦ и проверить, что ни один сертификат в этой цепочке не был отозван. Местоположение списков отзывов (Certificate Revocation List (CRL)) и сертификатов УЦ задается параметрами CRL Distribution Points (CDP) и Authority Information Access (AIA) соответственно. Для каждого параметра может быть указано несколько путей, и протоколов, по которым можно получить данные (например, HTTP, LDAP или FTP).

3. Ход работы

3.1 Подготовка к процедуре кросс-сертификации

В рамках данной лабораторной работы от Вас потребуется организовать доверенное взаимодействие между удостоверяющим центром, настроенным Вами в рамках предыдущих двух лабораторных работ, с уже настроенным отдельным удостоверяющим центром (рис. 3). Основные действия будут происходить на виртуальной машине с УЦ, который был настроен Вами ранее. При этом некоторые операции необходимо будет выполнить на второй виртуальной машине, чтобы доверие между удостоверяющими центрами было взаимным.

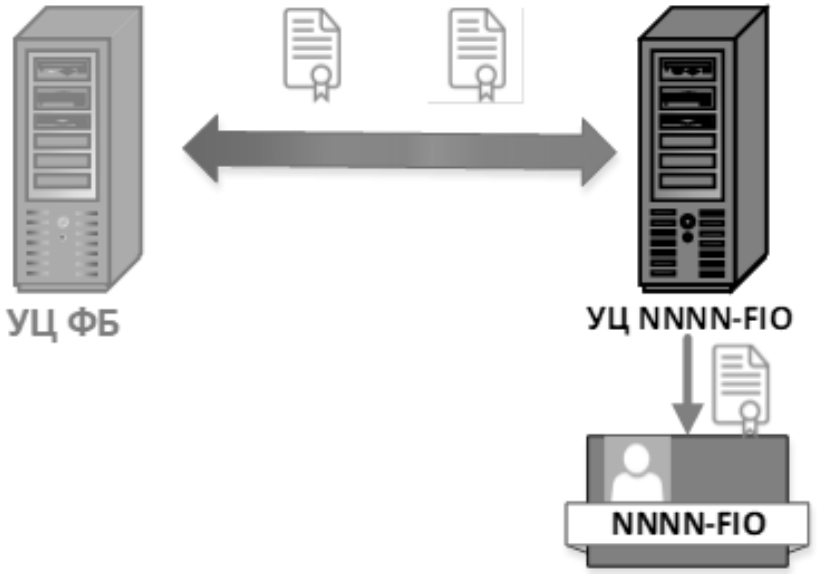

Рис. 3. Схема кросс-сертификации в лабораторной работе

В предыдущих лабораторных был настроен отдельный удостоверяющий центр (на схеме обозначен как УЦ NNNN-FIO). Для того, чтобы клиенты данного УЦ могли организовать защищенный документооборот с клиентами других УЦ, необходимо, чтобы у других клиентов возникло доверие к Вашему удостоверяющему центру. Для этого необходимо, чтобы их удостоверяющий центр выразил доверие Вашему и выдал соответствующий сертификат. В свою очередь, чтобы Вы могли доверять другим клиентам, Ваш удостоверяющий центр должен выдать сторонним УЦ соответствующие сертификаты. Таким образом, для организации взаимного доверия между двумя УЦ необходимо получение 2 сертификатов.

В качестве эксперимента скопируем сертификат пользователя NNNN-FIO, полученный в предыдущей лабораторной работе, на УЦ ФБ. Система сообщит, что у нее недостаточно информации для проверки сертификата (рис. 4).

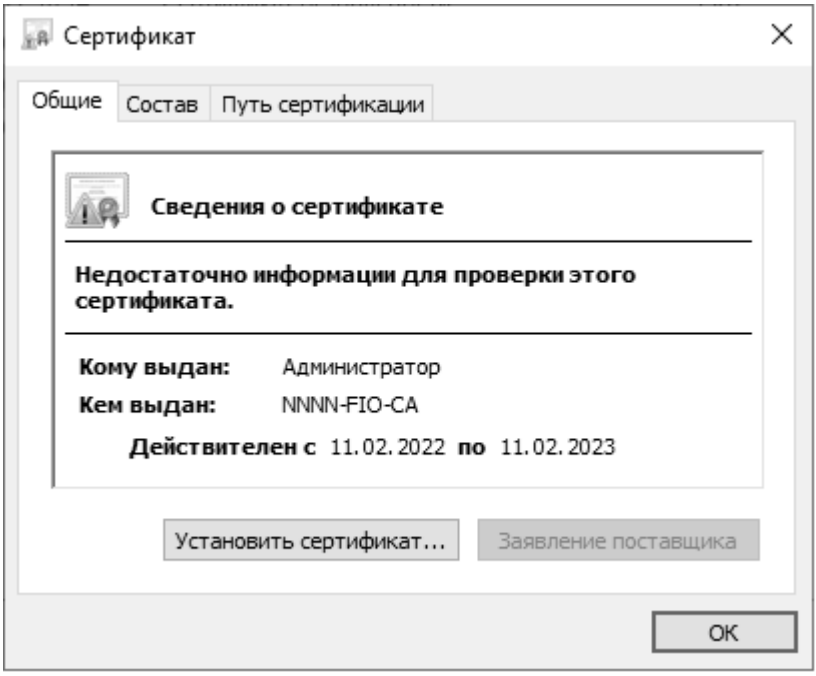

Рис. 4. Скопированный на другую виртуальную машину сертификат

Во вкладке «Пути сертификации» свойств сертификата говорится, что невозможно обнаружить поставщика этого сертификата (рис. 5).

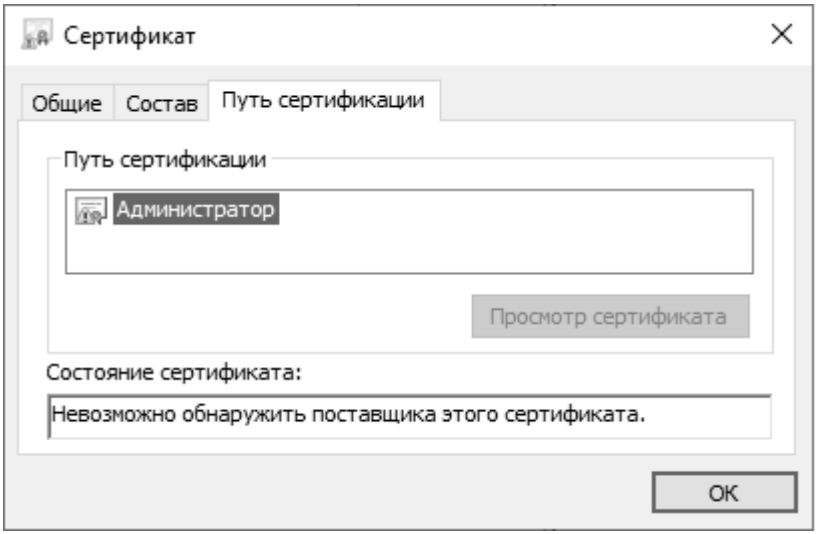

Рис.5. Путь сертификации для скопированного сертификата

Система на первой вкладке предлагает установить данный сертификат. Установите сертификат на локальном компьютере в раздел «Личное». Проверьте наличие сертификата в данном хранилище (рис. 6).

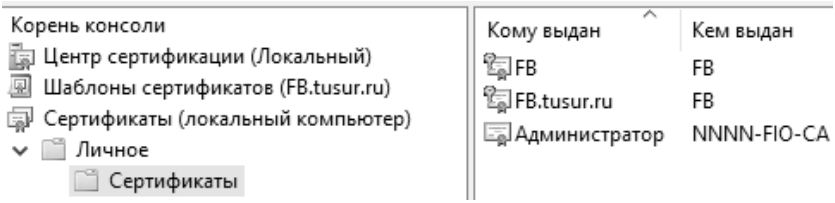

Рис.6. Наличие сертификата в целевом разделе

Если зайти в свойства сертификата в хранилище, то можно заметить, что данные во вкладках остались прежними. Доверия к данному сертификату в данный момент нет. Для того, чтобы это исправить можно осуществить 2 варианта подтверждения доверия к издателю. Первым вариантом является копирование корневого

сертификата УЦ, который выдал данный сертификат, и установка данного сертификата на данном компьютере в разделе «Доверенные издатели» (рис. 7). Другим вариантом является процедура кросс-сертификации.

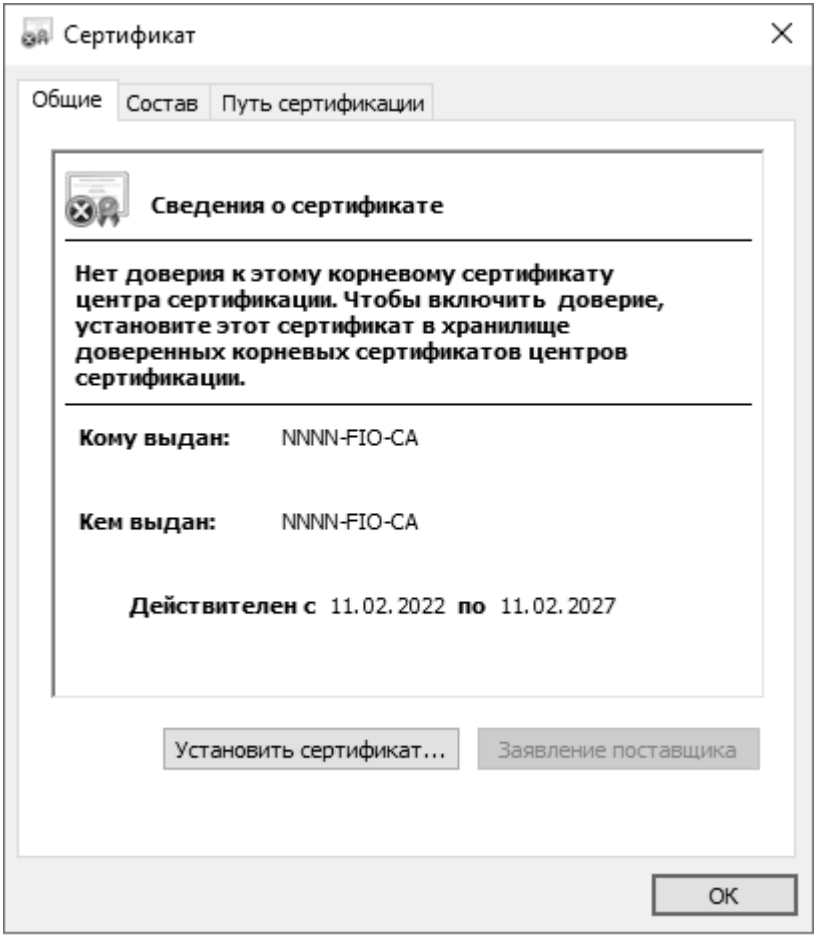

Рис. 7. Свойства корневого сертификата другого УЦ

Отличие между данными вариантами заключается непосредственно в отличии используемых сертификатов. Корневой сертификат выпускается удостоверяющим центром и содержит информацию о нем. При проверке подписи криптопровайдер строит

цепочку: сертификат пользователя — кросс-сертификат УЦ (может отсутствовать) — корневой сертификат головного УЦ (Минкомсвязи). Если такой сертификат не установлен в хранилище «Доверенные корневые», то все подписи, выданные на нем, будут отражаться с ошибкой «Последний сертификат цепи не является доверенным корневым сертификатом».

Корневой сертификат также называют самоподписанным, потому что УЦ выдает его самому себе. Кросс-сертификат – это сертификат, выпускаемый одним УЦ для другого для построения цепочки сертификации. В данных сертификатах значения полей «Издатель» и «Субъект» различны и определяют различные Центры Сертификации.

Помещаются данные сертификаты также в разные разделы:

- для установки корневого сертификата УЦ используется раздел «Доверенные корневые центры сертификации»;
- для кросс-сертификата УЦ используется раздел «Промежуточные центры сертификации»

Рассмотрим процедуру кросс-сертификации. Нажмите Win+R и введите «mmc» (рис. 8). Данные действия приведут к открытию Microsoft Management Console (консоль управления Microsoft).

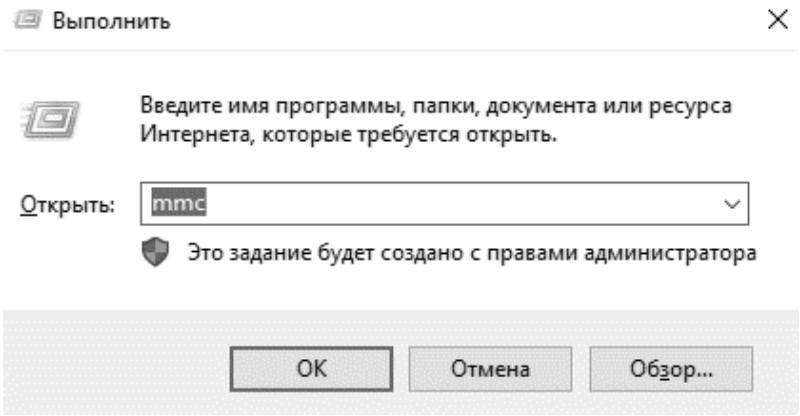

Рис. 8. Вызов консоли управления

В меню «Консоль» нажмите «Файл» → «Добавить/удалить оснастку» (рис. 9). Данное действие вызовет открытие соответствующего окна, в котором необходимо выбрать «Шаблоны сертификации» и нажать «Добавить» и «Ок» (рис. 10).

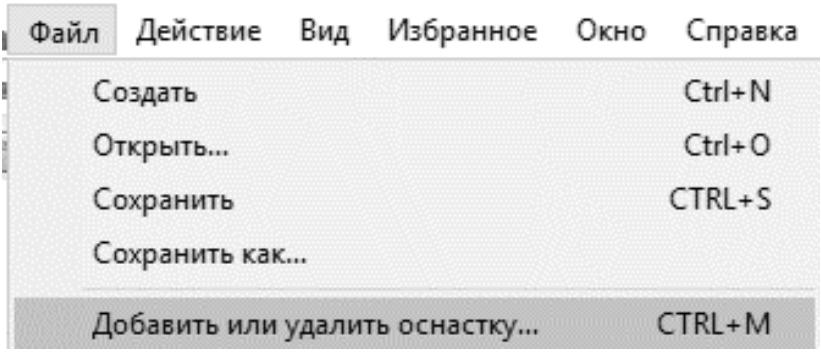

Рис.9. Вызов функции добавления оснастки

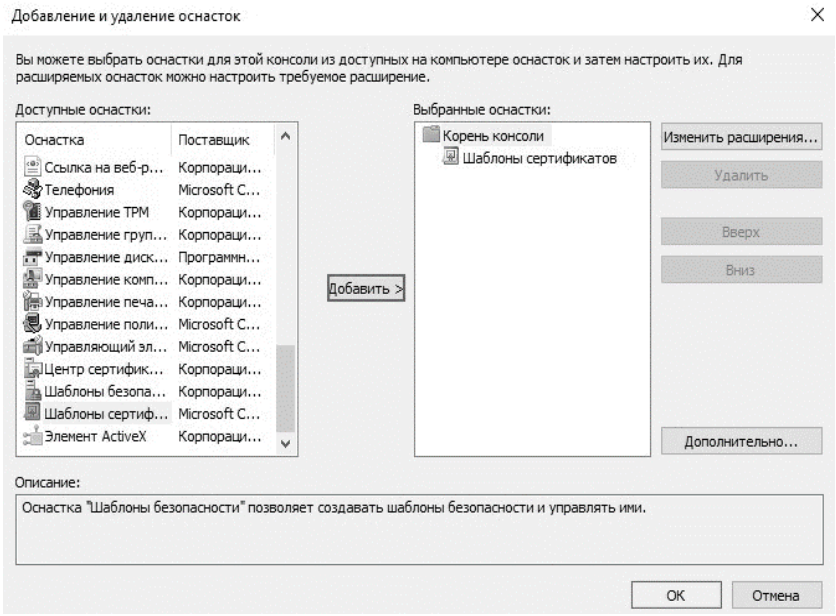

Рис. 10. Добавление оснастки «Шаблоны сертификатов»

В открывшейся оснастке найдите стандартный шаблон «Пользователь». Нажмите правой кнопкой на нём и выберите задачу «Скопировать шаблон» (рис. 11).

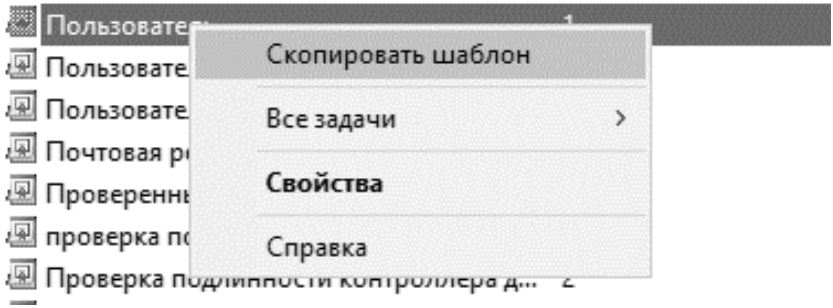

Рис. 11. Копирование шаблона сертификата «Пользователь»

Во вкладке свойств «Общие» у созданного шаблона укажите название шаблона «Кросс-сертификат». Во вкладке «Расширения» удалите в разделе «Политики применения» все политики и добавьте политику «Квалифицированное подчинение» (рис. 12). Во вкладке «Безопасность» удалите всех пользователей из разрешений, кроме глобальной и универсальной группы.

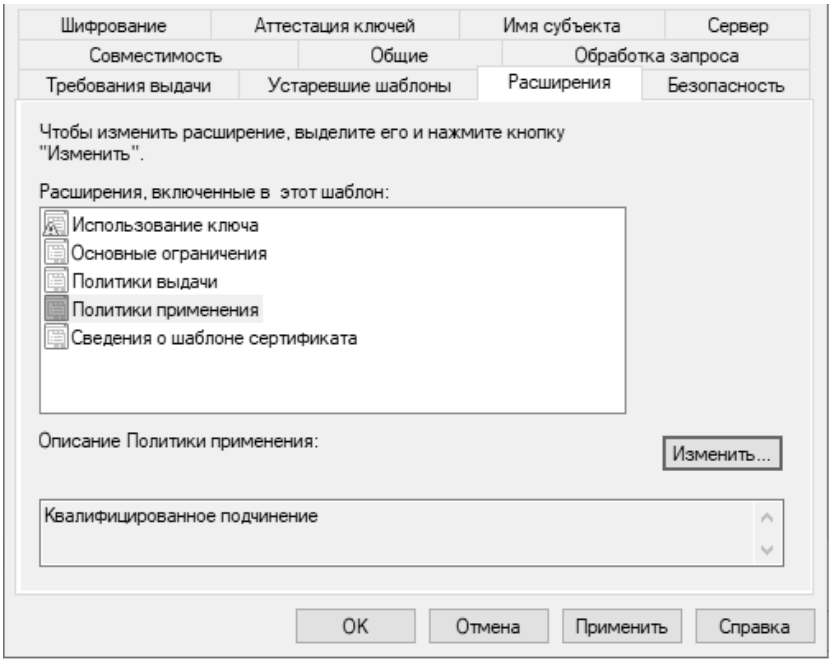

Рис. 12. Вкладка «Расширения»

Далее перейдите в оснастку «Файл» → «Центр сертификации» и добавьте нужные шаблоны в выдачу на СА. Для этого нажмите правой кнопкой мыши на «Шаблон сертификата» и выберите в меню «Создать» → «Выдаваемый шаблон сертификата» (рис. 13). В списке выделите только что созданный шаблон «Кросс-сертификация» и уже имеющийся «Перекрестный центр сертификации». Сделайте данные шаблоны доступными для выдачи.

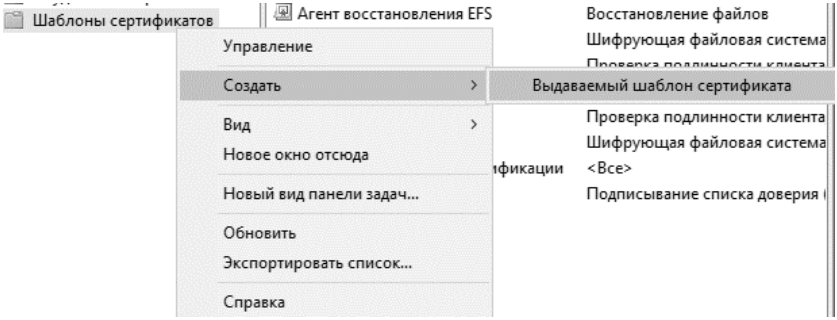

Рис. 13. Вкладка «Расширения»

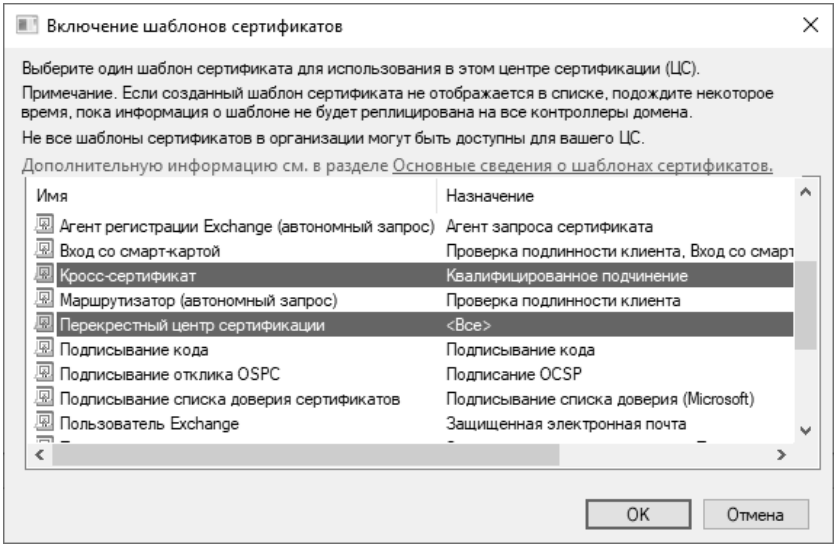

Рис. 14. Выбор включаемых шаблонов сертификатов

Поскольку удостоверяющий центр уже был настроен, далее можно перейти к запросу сертификата на основе созданного шаблона.

Для этого перейдите в Internet Explorer по адресу Вашего удостоверяющего центра. В качестве примера (рис. 15) показан результат включения шаблона на виртуальной машине, соответствующей УЦ ФБ, с которым необходимо выполнить кросс-сертификацию. У данного УЦ в сертификате был прописан адрес, по которому можно подключиться для работы с веб-службой: «https://fb.tusur.ru/certsrv».

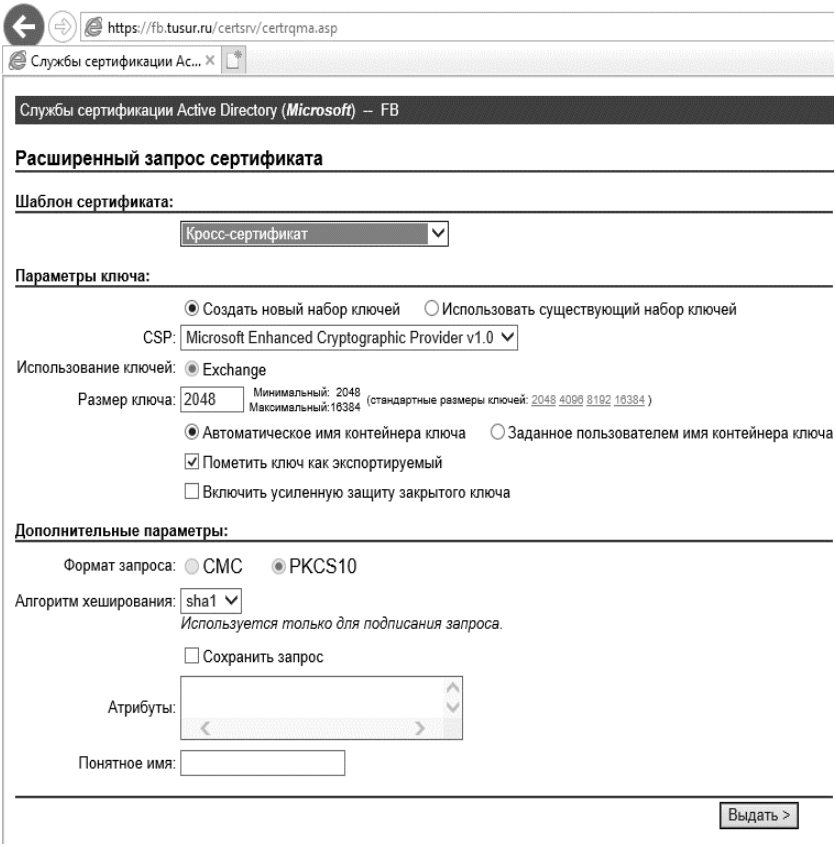

Рис. 15. Запрос сертификата по шаблону «Кросс-сертификат»

Запросите сертификат со стандартными параметрами. Обратите внимание, что данный запрос не будет успешным (рис. 16). Код запроса может отличаться – данный номер соответствует количеству осуществленных запросов на данном удостоверяющем центре

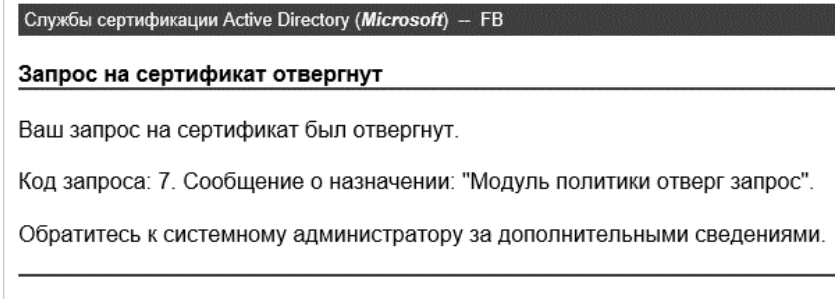

Рис. 16. Ошибка запроса сертификата

Данная ошибка была получена намерено, чтобы рассмотреть процедуру работы с подобными запросами. В данном примере запрос был отвергнут по причине отсутствия у администратора почтового адреса в профиле. Вы можете просмотреть неудачные запросы в оснастке «Центр сертификации» в соответствующем разделе (рис. 17).

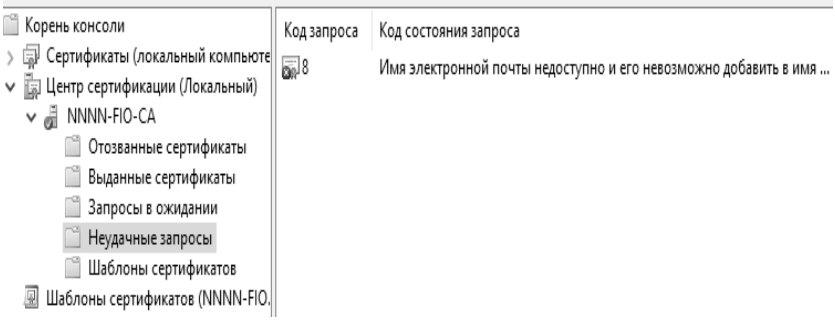

Рис. 17. Просмотр кода состояния запроса сертификата

Для данного запроса будет указан код состояния, содержащий следующий текст: имя электронной почты недоступно и его невозможно добавить в имя субъекта или в дополнительное имя субъекта. Далее идет код ошибки и обозначение типа ошибки. В данном варианте это CERTSRV_E_SUBJECT_EMAIL_REQUIRED. Связано это с тем, что при создании нового шаблона был скопирован шаблон «Пользователь». В вкладке «Имя субъекта» для базового шаблона задается принцип построения имени (рис. 18). В случае, если выбрать еще и DNS-имя, то система выдаст дополнительно ошибку типа CERTSRV_E_SUBJECT_DNS_REQUIRED.

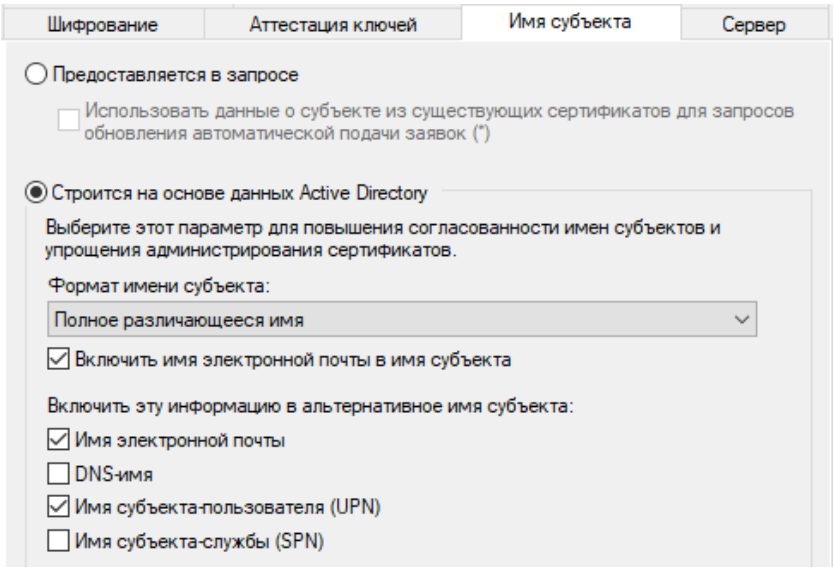

Рис. 18. Вкладка свойств шаблона «Пользователь»

Для исправления данной ошибки запустите оснастку управления пользователями и компьютерами в Active Directory. Это можно осуществить несколькими способами: добавить соответствующую оснастку в консоль mmc или вызвать командой «dsa.msc» в меню «Выполнить» (рис. 19).

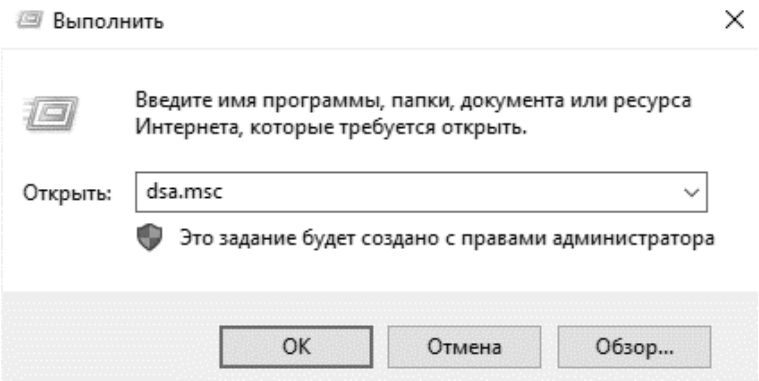

Рис. 19. Запуск оснастки «Active Directory – пользователи и компьютеры»

В оснастке выберите раздел, относящийся к домену данной виртуальной машины. В папке «Users» данного домена выберите пользователя «Администратор», от чьего имени осуществляются запросы на данной виртуальной машине. В свойствах пользователя во вкладке «Общие» укажите адрес своей студенческой электронной почты. В качестве примера указана почта admin@fb.tusur.ru (рис. 20). Обратите внимание, что наличие в отчете скриншота с персональным почтовым адресом будет являться еще одним из критериев при проверке самостоятельности выполнения данной работы.

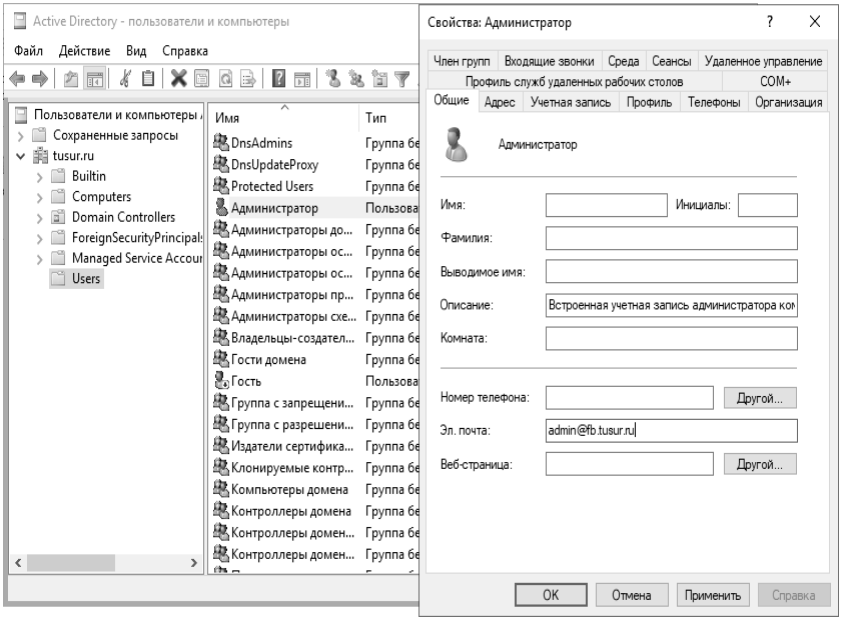

Рис. 20. Внесение адреса эл.почты в свойства пользователя «Администратор»

После проделанных действий перейдите в оснастке «Центр сертификации» в пункт «Неудачные запросы». Выберите неудачный запрос и повторно выдайте сертификат. Для этого в контекстном меню выберите «Все задачи»→ «Выдать». После удачной выдачи сертификата он отобразиться в папке «Выданные сертификаты».

Другим примером ошибок при попытке запроса сертификата может быть сообщение о недоступности сервера отзыва сертификатов (рис. 21).

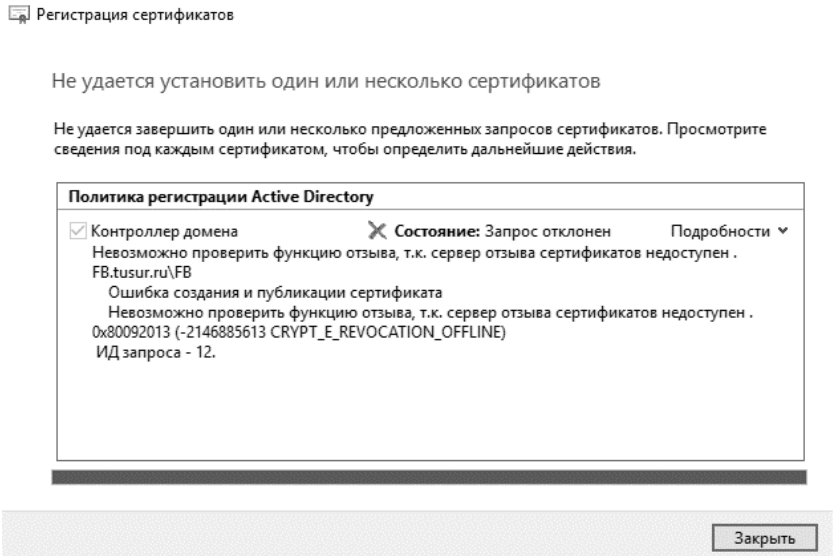

Рис. 21. Ошибка запроса, связанная с недоступностью сервера отзыва

По данной ошибке на сайте Microsoft есть справка, в которой объясняется, что это может быть вызвано несколькими причинами:

- недоступен список отзыва (CRL);
- не опубликовано местоположение CRL;
- истек срок действия CRL.

Удостоверяющий центр периодически выдаёт список, который он публикует в хранилище. Каждый COC включает поле nextUpdate, которое указывает время, когда будет выпущен следующий COC. Любая проверяющая сторона, которой требуется информация о статусе сертификата и у которой ещё нет текущего COC, получает текущий список из хранилища. Если сертификат, который проверяет клиент, не находится в списке, то работа продолжается в нормальном режиме и ключ считается подтверждённым сертификатом. Если же сертификат присутствует, то ключ считается недействительным и ему нельзя доверять.

Для решения данной проблемы необходимо в оснастке «Центр сертификации» для раздела «Отозванные сертификаты» опубликовать новый список отзыва сертификатов (Certificate Revocation List, CRL). Данный список используется для определения факта, был ли сертификат пользователя или удостоверяющего центра отозван в связи с компрометацией ключей (рис. 22).

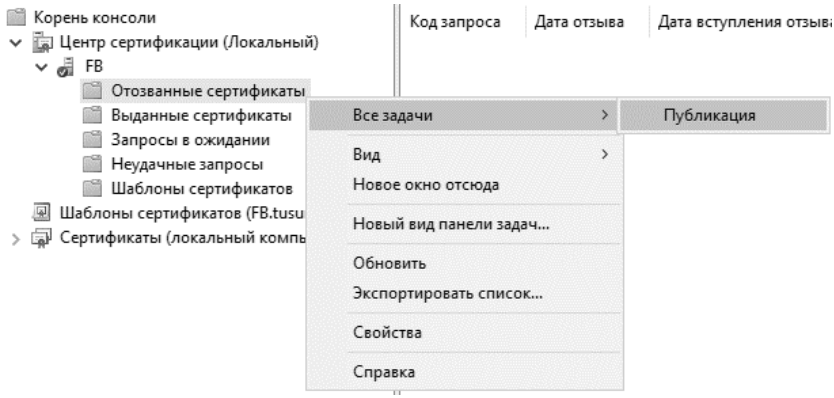

Рис. 22. Публикация нового списка отозванных сертификатов

Система предложит один из вариантов публикации нового списка. Как можно заметить (рис. 23), старый список является актуальным, что свидетельствует о сбое в работе УЦ, вызванным недоступностью точки распространения списка.

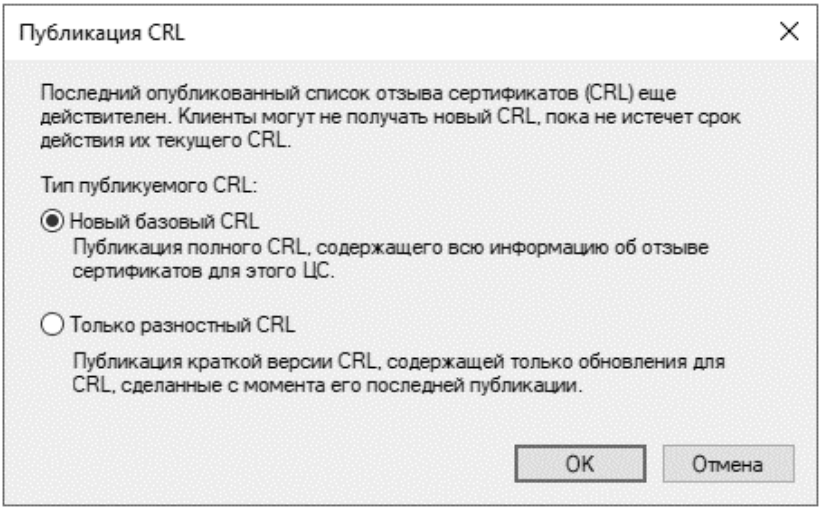

Рис. 23. Выбор варианта публикации списка отозванных сертификатов

В результате будет получен новый файл списка отозванных сертификатов, расположенный по следующему пути: C:\Windows\System32\CertSrv\CertEnroll (рис. 24).

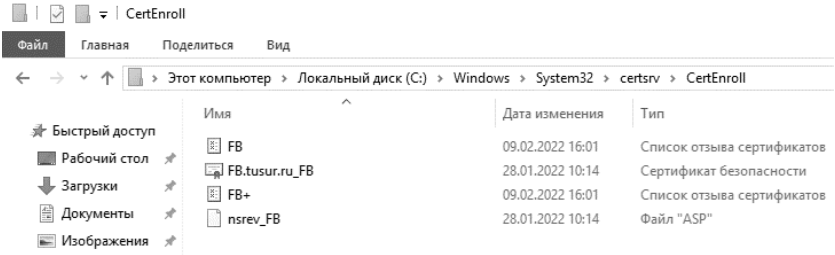

Рис. 24. Полученный файл списка отозванных сертификатов

В случае, если данный файл необходимо опубликовать на других контроллерах домена, необходимо скопировать данный файл и опубликовать его в другом Active Directory. Для этого используется следующая команда:

certutil -dspublish -f <Путь к файлу CRL> <Имя УЦ>

Если команда будет выполнена на том же контроллере (рис. 25), то система уведомит, что данный список отзыва сертификатов уже содержится в хранилище, но добавит его заново.

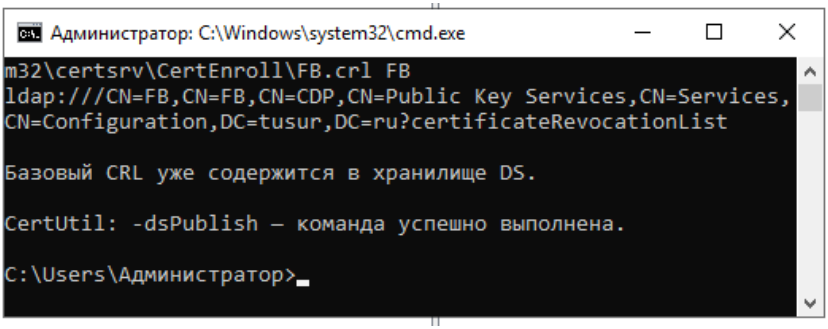

Рис. 25. Пример выполнения команды

3.2 Кросс-сертификация двух удостоверяющих центров

На виртуальной машине УЦ ФБ уже выполнены все те действия, которые требовалось выполнить Вам в рамках данной лабораторной работы на своем удостоверяющем центре. Отметим, что кросс-сертификация — это весьма обширная тема. Для нашего сценария нет необходимости рассматривать подробности т.н. qualified subordination, поэтому ограничимся самым простым вариантом, без дополнительных ограничений.

Для этого создайте текстовый файл с именем «Policy.inf» (рис. 26) и следующим содержанием:

[Version]
Signature = $WindowsNT$
[RequestAttributes]
CertificateTemplate = CrossCA

Далее экспортируем сертификат, созданный по шаблону «Кросс-сертификат» и созданный текстовый файл с именем «Policy.inf» на виртуальную машину УЦ ФБ.

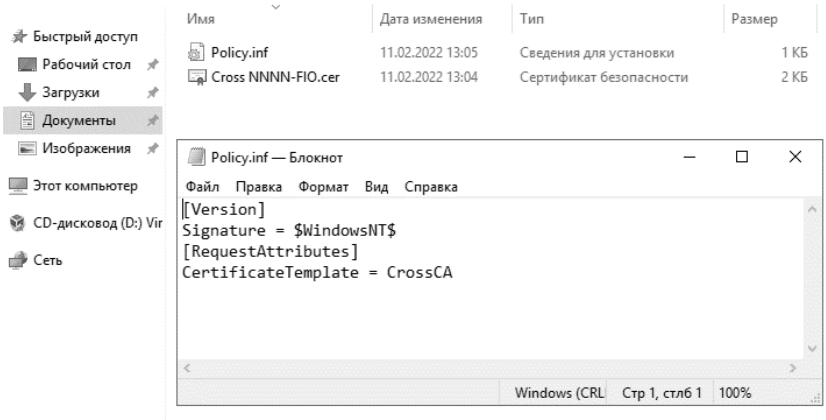

Рис. 26. Создание файла «Policy.inf»

Установим сертификат на виртуальной машине УЦ ФБ при помощи командной строки и следующей команды (рис. 27):

certreq –policy

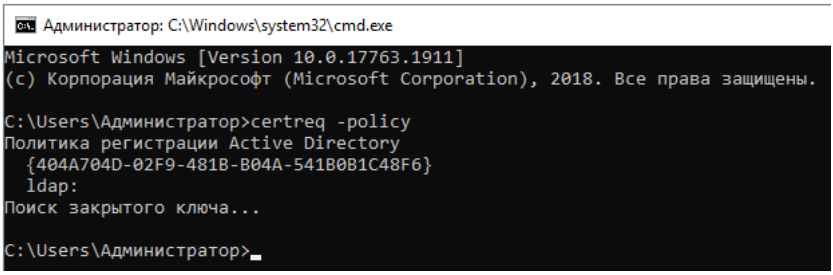

Рис. 27. Результат выполнения команды

После ввода команды выберем в диалоговом окне сертификат и файл «Policy.inf». Затем откажемся от считывания смарт-карты (рис. 28), выберем сертификат подписи (рис. 29) и укажем путь для сохранения запроса.

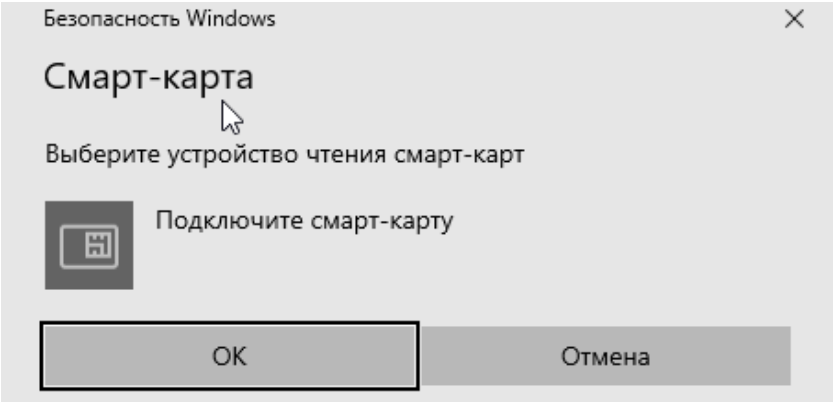

Рис. 28. Результат выполнения команды

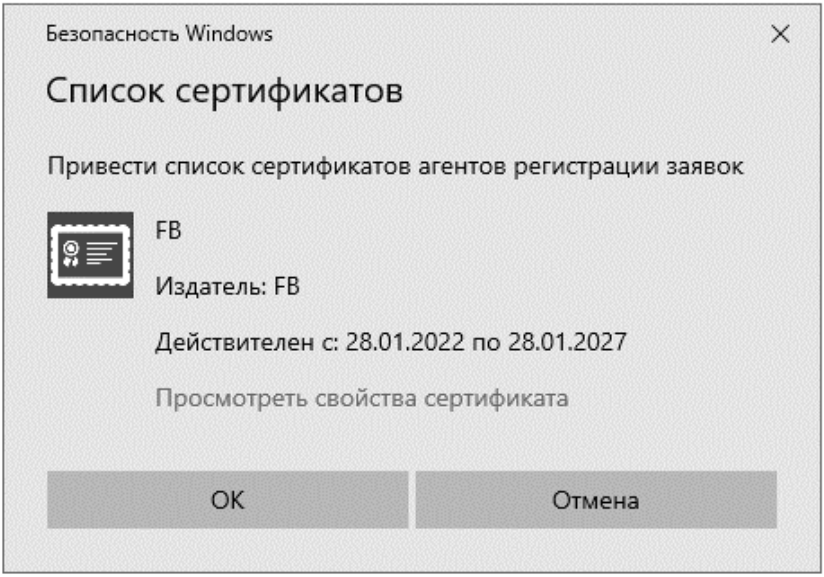

Рис. 29. Результат выполнения команды

Далее система предложит сохранить сформированный запрос. Выполним его также через командную строку (рис. 30). Для этого необходимо вызвать команду

certreq –submit path\cross.req

В данной команде path\cross.req — путь размещения и имя файла запроса для кросс-сертификата. В диалоговом окне выберем сервер CA. В результате будет получена ошибка (рис. 31).

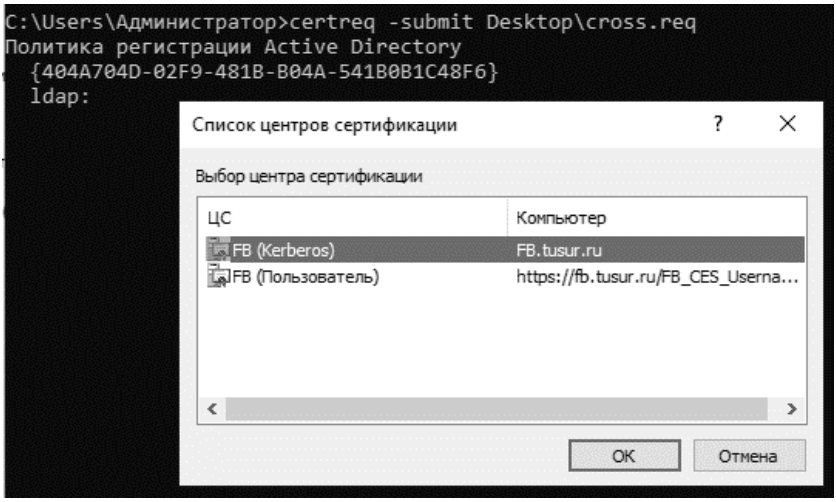

Рис. 30. Результат выполнения команды

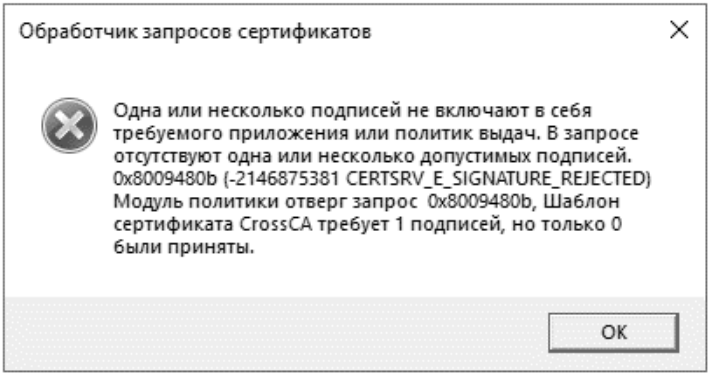

Рис. 31. Результат выполнения команды

Чтобы её исправить отменим необходимость подписи сертификата со стороны администраторов ЦС. «mmc»→ «Шаблон сертификатов» нужно найти шаблон «Перекрестный центр сертификации», зайти в его свойства в раздел «Требования выдачи» и убрать галочку на «Указанного числа авторизованных подписей».

Попытаемся снова выполнить данный запрос на сертификат (рис. 32). В этот раз система выдаст требуемый сертификат. Единственное отличие в результате будет заключаться в изменении срока действия сертификата.

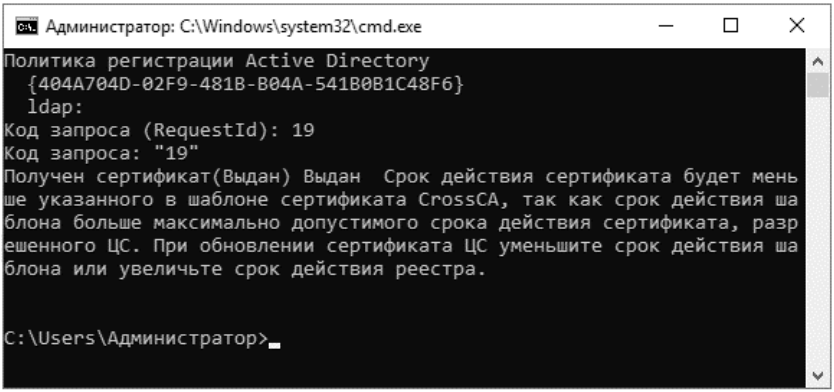

Рис. 32. Результат выполнения команды

Далее можно установить полученный сертификат. Для этого во вкладке свойств полученного сертификата нажмите на кнопку «Установить сертификат». Откроется мастер импорта сертификатов. В качестве расположения хранилища выберите «Локальный компьютер и автоматический выбор хранилища. Сертификат будет помещен в раздел «Промежуточные центры сертификаты» (рис. 33).

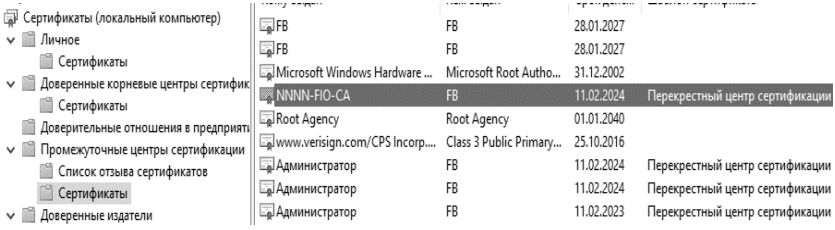

Рис. 33. Установленный сертификат

Если зайти в свойства сертификата пользователя NNNN-FIO (рис. 34), то можно увидеть, что в пути сертификации для него указано, что сертификат действителен и это подтверждено двумя удостоверяющими центрами.

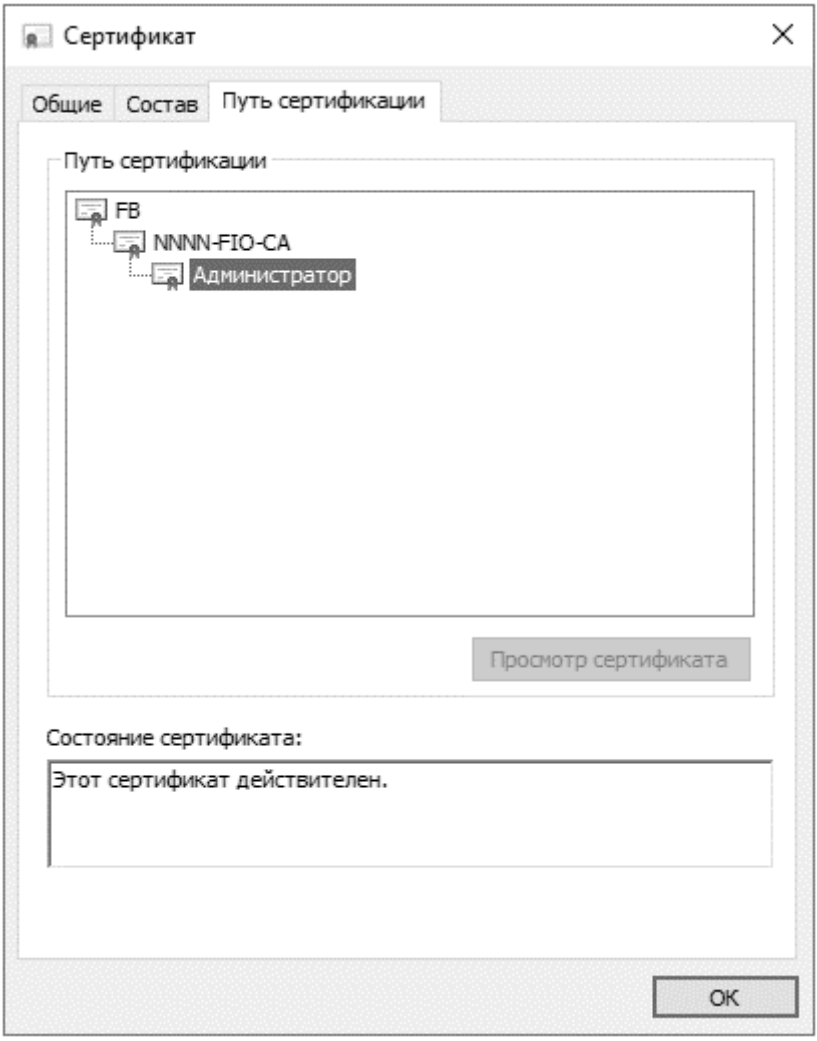

Рис. 33. Результат выполнения команды

4. Задание на лабораторную работу

1. Ознакомиться с теорией (включая лекционные материалы).
2. Создать шаблон сертификата для кросс-сертификации.
3. Провести взаимную кросс-сертификацию между настроенным Вами в предыдущих лабораторных работах удостоверяющим центром и готовым УЦ.
4. Составить по проделанной работе отчет.

5. Контрольные вопросы

1. Что такое инфраструктура открытых ключей?
2. Какие модели доверия Вам известны?
3. Что такое кросс-сертификация?
4. На какие два вида подразделяется кросс-сертификация? В чем отличие между ними?
5. Какие шаблоны сертификатов Вам известны?
6. Перечислите основные свойства сертификата.
7. Как импортировать и экспортировать сертификат?
8. Какие параметры можно установить при запросе сертификата?
9. Для чего используются списки отозванных сертификатов?
10. Опишите алгоритм получения нового списка отозванных сертификатов.

ЛАБОРАТОРНАЯ РАБОТА №7
Иерархическая модель доверия удостоверяющих центров

1. Цель работы

Целью лабораторной работы является ознакомление с одной из базовых моделей доверия, применяемой при построении архитектуры инфраструктуры открытых ключей. В данной работе будет изучена работа удостоверяющих центров при иерархической модели доверия, рассмотрены особенности работы на каждом из уровней, работа операторов на каждом из уровней сертификации.

2. Краткие теоретические сведения

Иерархия удостоверяющих центров обычно графически изображается в виде древовидной структуры с корнем наверху и ветвями, спускающимися и заканчивающимися листьями. В этом перевернутом дереве корень представляет определенный УЦ, который обычно называется корневым (или головным) и действует как главный пункт, или корень, доверия для целого домена подчиненных ему субъектов PKI. Под корнем располагаются промежуточные удостоверяющие центры. Промежуточные удостоверяющие центры представлены в древовидной структуре промежуточными узлами, от которых отходят следующие ветви. Листья, или конечные вершины дерева, соответствуют субъектам PKI, не являющимся удостоверяющими центрами, их называют конечными субъектами или просто конечными пользователями (рис. 1).

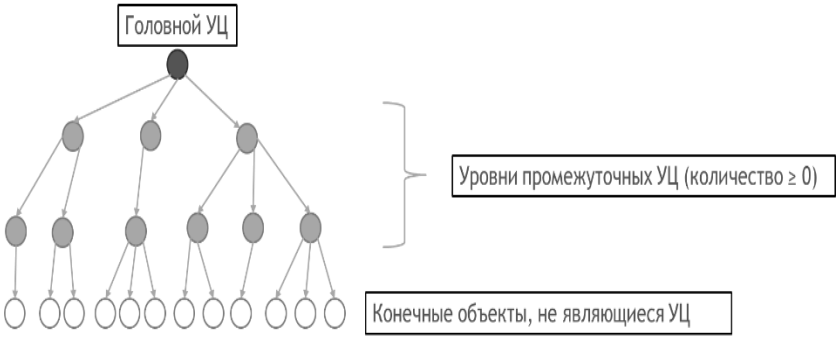

Рис. 1. Схема иерархической модели доверия удостоверяющих центров

Термин корень имеет фундаментальный смысл. Корень является не просто начальным пунктом сети, связей или архитектуры, а

начальным пунктом доверия. Все субъекты PKI (промежуточные удостоверяющие центры и конечные субъекты) владеют открытым ключом корневого (головного) УЦ и полагаются на него как на начальный и конечный пункт доверия при верификации всех сертификатов. Этот ключ является корневым, даже если в конфигурации PKI отсутствуют промежуточные удостоверяющие центры или она выглядит как-то иначе. В некоторых иерархиях УЦ верхнего уровня может сертифицировать не только удостоверяющие центры, но и конечные субъекты. Обычно в литературе, посвященной проблематике PKI, предполагается, что УЦ сертифицирует либо удостоверяющие центры, либо конечных субъектов (а не тех и других одновременно).

Кроме того, иерархическая модель позволяет минимизировать затраты при перестроении инфраструктуры в случае компрометации ключа УЦ. Действительно, если происходит компрометация ключа одного из издающих (подчиненных) УЦ, то необходимо переиздать только те сертификаты, которые были выданы этим УЦ. Более того, такая модель позволяет создавать УЦ с различными регламентами в рамках одной инфраструктуры.

3. Ход работы

3.1 Реализация иерархии удостоверяющих центров

В рамках данной лабораторной работы от Вас потребуется добавить в подчинение к УЦ ФБ, с которым организовывали взаимодействие в рамках предыдущей лабораторной работы, промежуточный удостоверяющий центр – кафедральный, на котором Вы проходите обучение.

В результате выполнения лабораторной работы должна получиться одна из ветвей схемы (рис. 2) иерархической модели подчинения Вашей специальности по отношению у удостоверяющему центру факультета.

Для того, чтобы создать подчиненный УЦ для Вашей кафедры, воспользуемся изначальной виртуальной машиной, использованной при создании Вашего персонального УЦ (NNNN-FIO). Запустите виртуальную машину «PKI lab». Для того, чтобы ввести новый (кафедральный) удостоверяющий центр в подчинение к факультетскому удостоверяющему центру необходимо ввести виртуальную машину в домен факультета.

Данная операция потребует предварительной подготовки. Иначе при добавлении компьютера в домен может быть получена следующая ошибка (рис. 3)

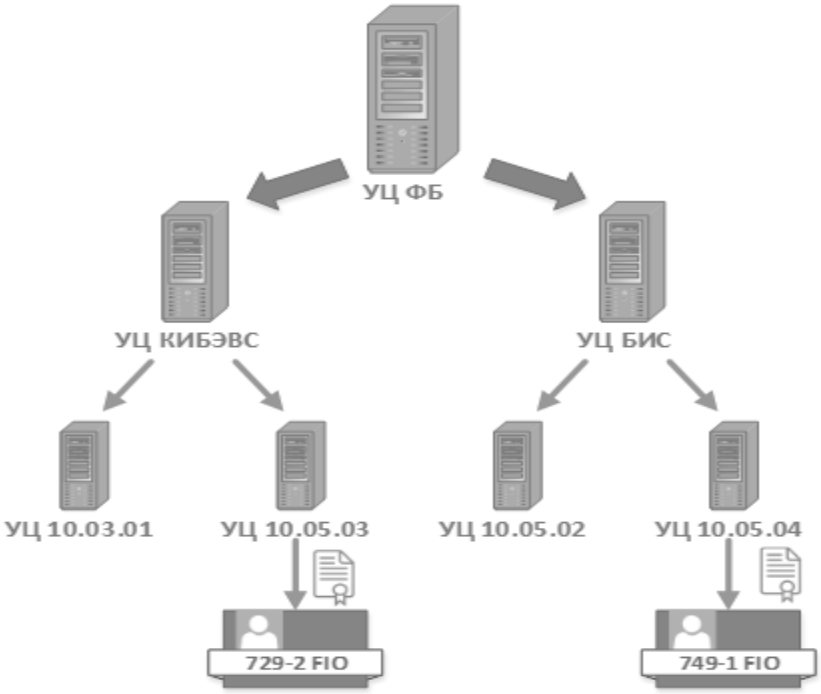

Рис. 2. Схема иерархической модели в лабораторной работе

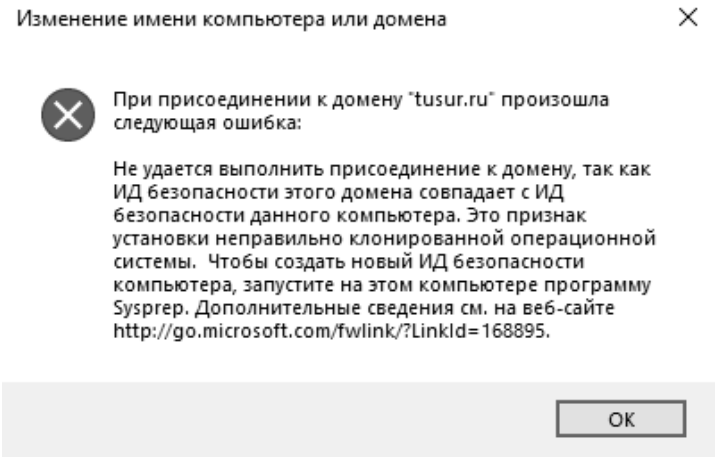

Рис. 3. Ошибка при добавлении виртуальной машины в домен

Данная ошибка связана с тем, что в рамках первой работы с удостоверяющими центрами мы создали клон этой же виртуальной машины. Поэтому виртуальная машина, на которой установлен домен, воспринимает подключаемую виртуальную машину как саму себя. Это связано с тем, что идентификаторы безопасности (SID) у них идентичны. Для кросс-сертификации данная проблема не является критичной.

Для того, чтобы исправить данную проблему, воспользуемся утилитой Sysprep. Запуск ее осуществляется из директории (рис. 4), в которой расположена утилита следующей командой:

sysprep /oobe /generalize

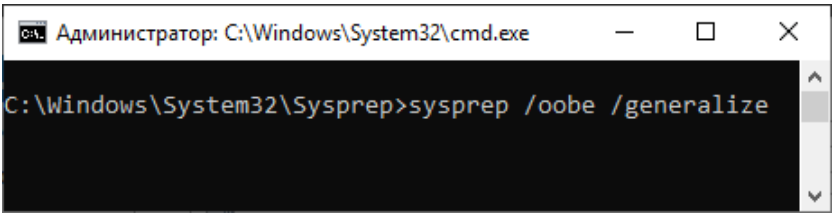

Рис. 4. Вызов утилиты в командной строке с параметрами

В данной команде заданы следующие ключевые параметры:

/generalize – режим подготовки системы к созданию образа с удалением всех идентификаторов, журналов и точек восстановления;

/oobe – перезагружает компьютер в режиме экрана приветствия, позволяя администратору создавать новые учетные записи, переименовывать ПК и так далее.

В результате у второй виртуальной машины изменится SID, и она выключится. Запустите ее заново. После запуска потребуется заново выбрать настройки региона и задать пароль администратора.

Следующим шагом потребуется внести изменения в параметры сетевых адаптеров обоих виртуальных машин. В свойствах у IP версии 4 укажите для удостоверяющих центров факультета и кафедры IP-адреса 192.168.0.1 и 192.168.0.2 соответственно (рис. 5).

Для внесения данных изменений откройте «Свойства сетевого подключения» (Пуск – Панель управления – Сеть и Интернет – Центр управления сетями и общим доступом – Изменение параметров адаптера), вызовите контекстное меню подключения и выберите «Свойства». Выделите «Протокол Интернета версии 4 (TCP/IPv4)».

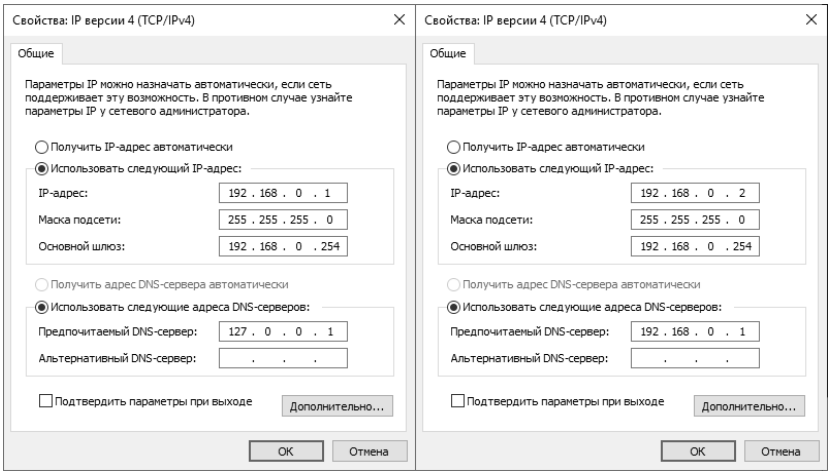

Рис. 5. Настройка IP-адресов адаптеров виртуальных машин

Создайте на виртуальной машине УЦ ФБ учетную запись для управления подчиненным удостоверяющим центром. Для этого запустите оснастку «Пользователи и компьютеры Active Directory» через меню «Средства» диспетчера серверов (рис. 6).

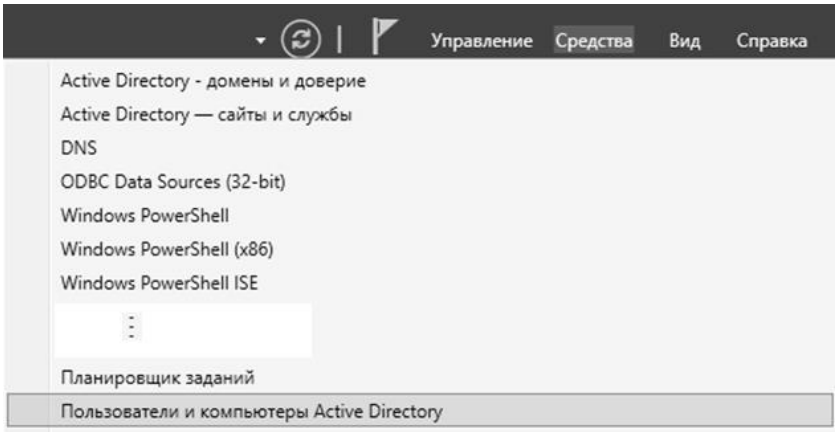

Рис. 6. Вызов оснастки «Пользователи и компьютеры Active Directory»

В открывшемся окне выберите домен «tusur.ru» и вызовите контекстное меню. В нем выберите пункт «Создать», а в предложенном списке вариантов «Пользователь».

В качестве имени пользователя можете указать привычную связку NNNN_FIO, соответствующие номеру Вашей группы и Вашим инициалам (рис. 7).

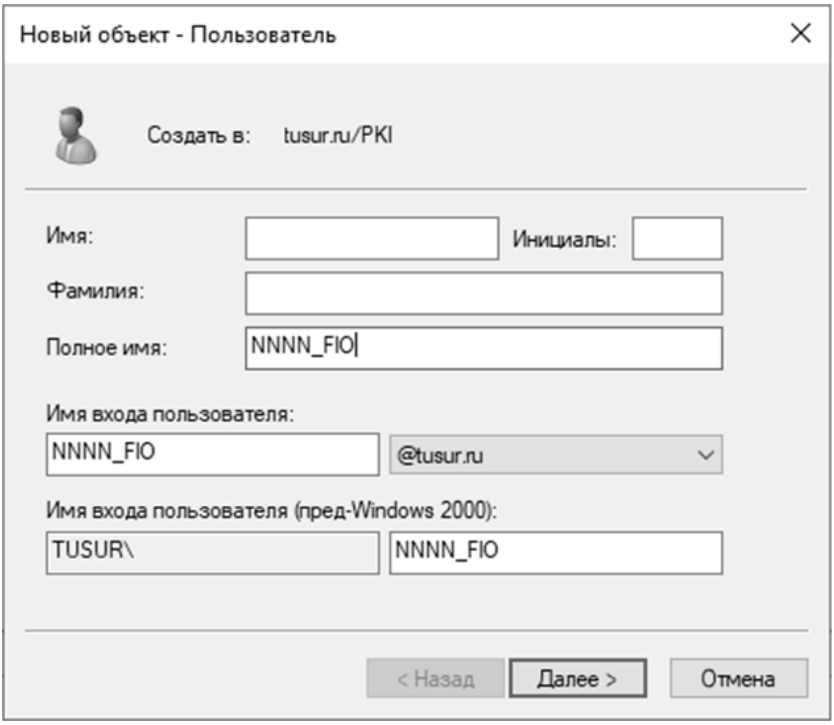

Рис. 7. Параметры создаваемого пользователя

Далее можно перейти к присоединению второй виртуальной машины к домену. Для этого необходимо в свойствах ее системы (Пуск – Панель управления – Система и безопасность – Система – Дополнительные параметры системы) выбрать вкладку «Имя компьютера» и нажать на кнопку «Изменить».

Задайте в качестве имени компьютера название кафедры (рис. 8) и укажите, что компьютер является частью домена tusur.ru. После нажатия на кнопку «ОК» потребуется указать логин и пароль пользователя. Укажите данные созданного Вами пользователя (рис. 9).

В результате система выдаст сообщение об успешном подключении к домену данной виртуальной машины (рис. 10).

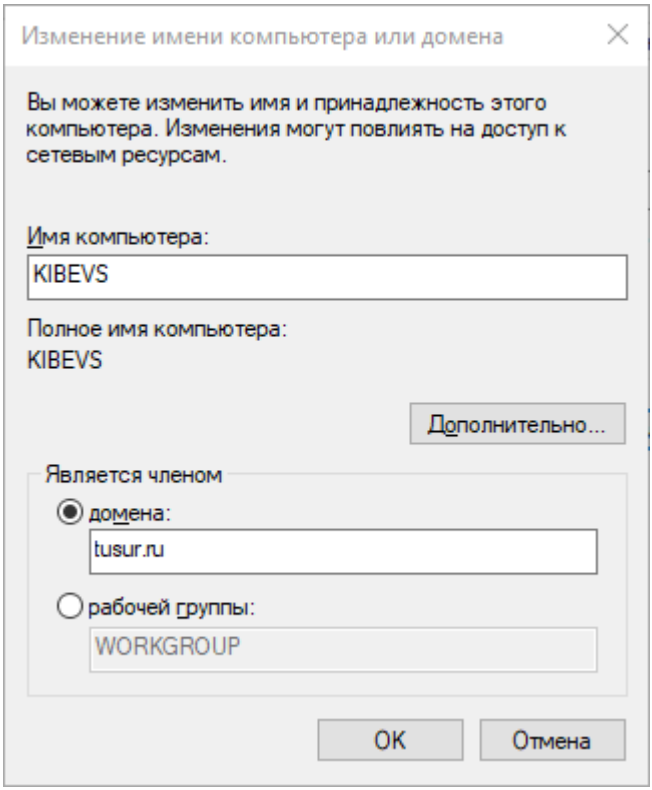

Рис. 8. Подключение виртуальной машины к домену

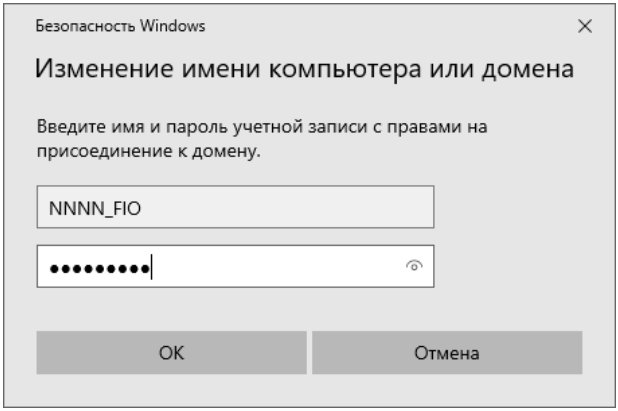

Рис. 9. Ввод учетных данных для подключения к домену

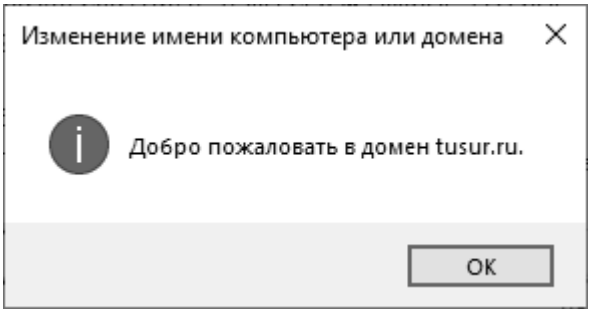

Рис. 10. Уведомление об успешного включении виртуальной машины в домен

Выдадим права подчиненному серверу на изготовление сертификатов. Для этого на виртуальной машине УЦ ФБ снова откройте оснастку «Пользователи и компьютеры Active Directory» и во вкладке «tusur.ru» выбираем раздел «Users» (рис. 11). Находим там пользователя созданного нами пользователя, под чьим именем мы вошли на виртуальной машине кафедрального УЦ.

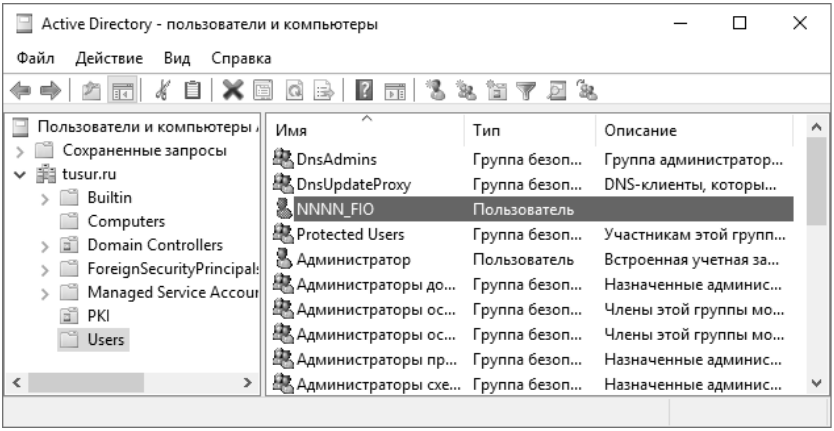

Рис. 11. Выбор созданного пользователя в оснастке

Зайдите в свойства данного пользователя и перейдите во вкладку «Член групп». Нажмите на кнопку «Добавить». В открывшемся окне в поле «Введите имена выбираемых объектов» укажите «Издатели сертификатов» (рис. 12). Аналогично можете сделать пользователя администратором домена.

Далее вернемся к виртуальной машине с кафедральным удостоверяющим центром. Запустите «Диспетчер серверов» и выберите пункт «Добавить роли и компонент».

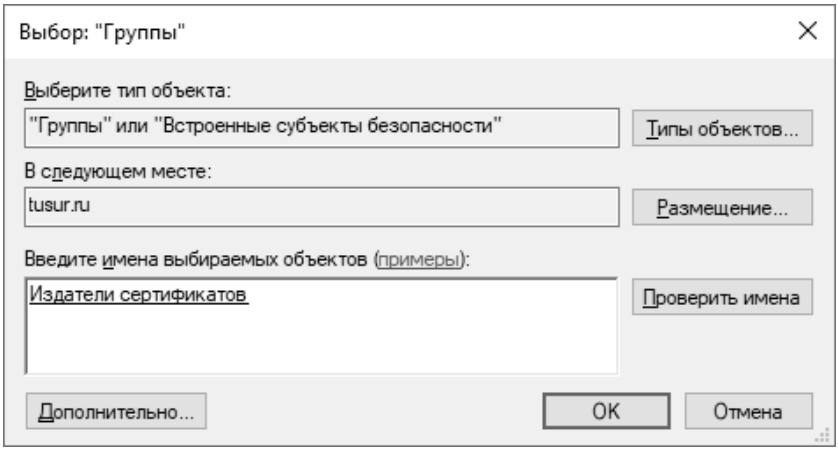

Рис. 12. Добавление пользователю группы «Издатели сертификатов»

В открывшемся мастере добавления ролей и компонентов для текущего сервера выберите роль «Службы сертификатов Active Directory» с компонентами «Центр сертификации» и «Служба регистрации в центре сертификации через Интернет».

После окончания установки компонентов нажмите на ссылку «Настроить службы сертификатов Active Directory». В открывшемся конфигураторе выберите оба установленных компонента. В качестве варианта установки центра сертификации выберите «ЦС предприятия», а на следующем шаге «Подчиненный ЦС» (рис. 13).

Дальнейшая настройка осуществляется аналогично корневому центру сертификации. Создайте новый закрытый ключ для подчиненного центра сертификации. Параметры генерации ключа можете оставить стандартными.

На следующем шаге необходимо указать имя подчиненного центра сертификации. С целью упрощения понимания имени центров сертификации в рамках лабораторной работы рекомендуется использовать на данном шаге наименование кафедры.

Далее появится окно, в котором необходимо выбрать корневой центр сертификации, к которому будет отправлен запрос на сертификат (рис. 14).

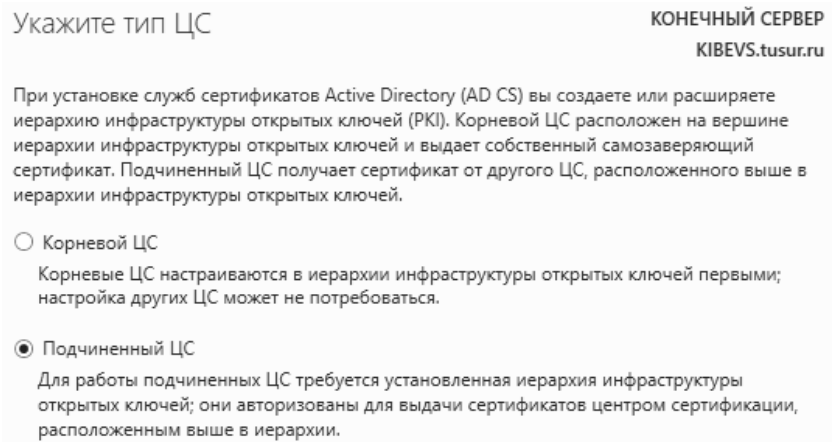

Рис. 13. Добавление пользователю группы «Издатели сертификатов»

Выберите пункт» Отправить запрос сертификата в родительский ЦС». В противном случае потребуется копировать файл на другую виртуальную машину и вручную проводить обработку запроса, а после вручную копировать полученный сертификат на подчиненном удостоверяющем центре. Далее нажмите на кнопку «Выбрать» и в открывшемся окне выберите корневой центр сертификации (рис. 15).

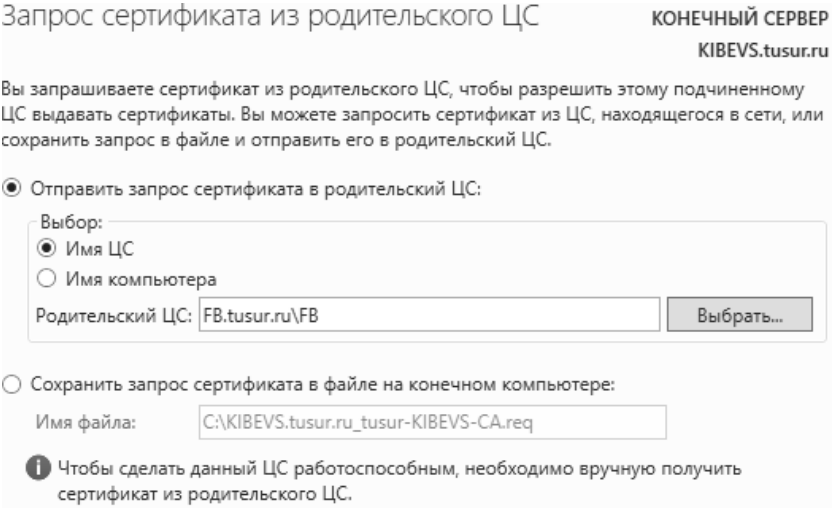

Рис. 14. Запрос сертификата из родительского ЦС

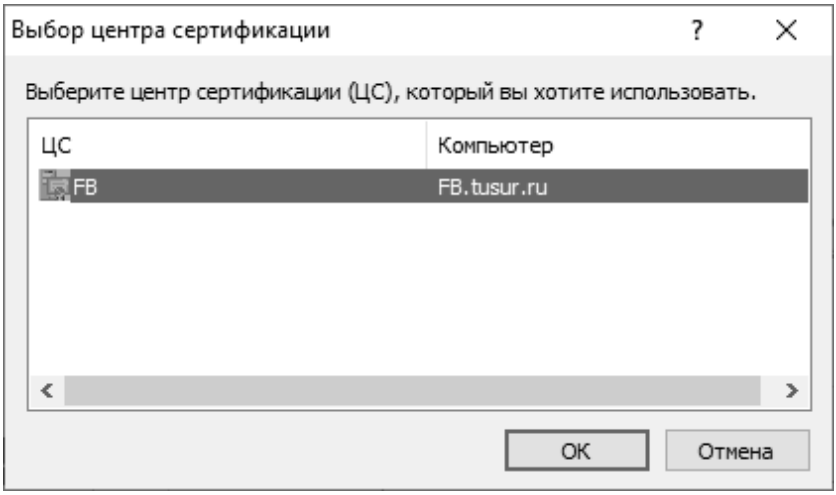

Рис. 15. Выбор родительского центра сертификации

В следующих разделах оставьте параметры по умолчанию и нажмите на кнопку «Настроить».

После окончания настройки проверьте работоспособность локального центра сертификации. Запустите Internet Explorer и в адресной строке укажите путь к своему ЦС. По умолчанию это **http://192.168.0.2/certsrv**. В качестве примера показан вход по адресу **http://kibevs.tusur.ru/certsrv** (рис. 16-17).

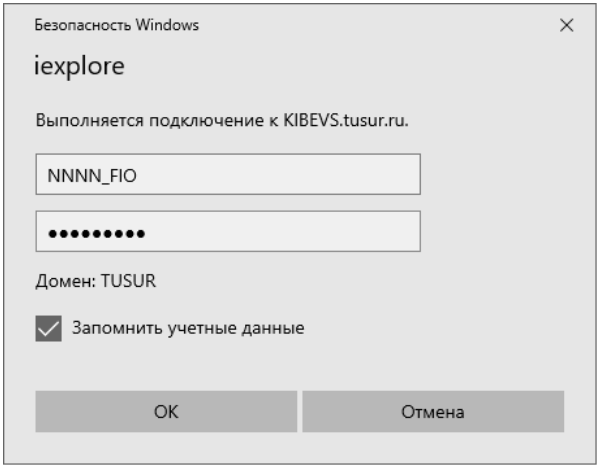

Рис. 16. Ввод учетных данных для входа на подчиненный ЦС

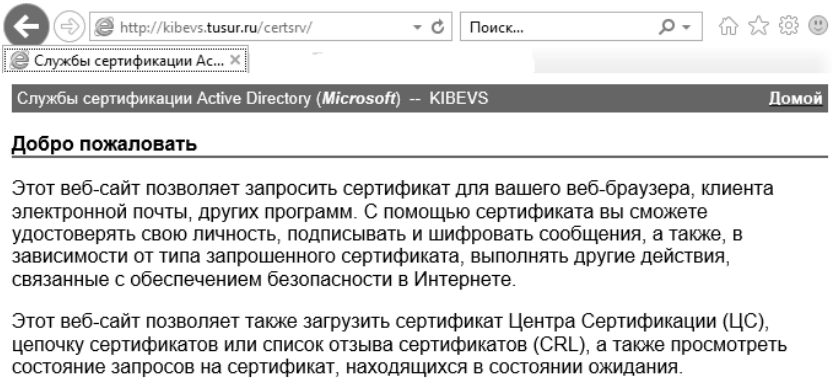

Рис. 17. Подчиненный центр сертификации

Далее проверим возможность подключения подчиненного центра сертификации к корневому. Для этого в адресной строке пропишите путь к нему и войдите под текущей учетной записью (рис. 18).

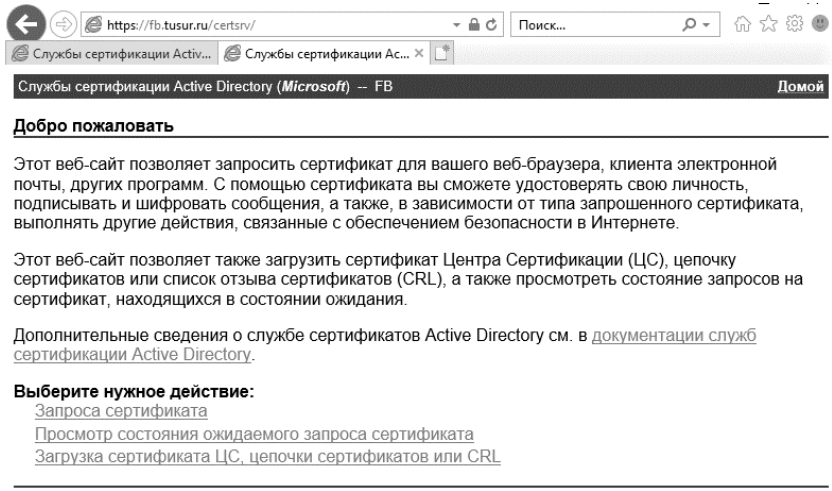

Рис. 18. Корневой центр сертификации

Перейдем к виртуальной машине с корневым центром сертификации (УЦ ФБ). На данном этапе необходимо проверить, что подчиненному сертификату был выдан соответствующий сертификат. Для этого запустите оснастку «Центр сертификации». В разделе выданные сертификаты выделите последний выданный сертификат (рис. 19). Зайдите в свойства сертификата (рис. 20).

Код запроса	Имя запросившего	Шаблон сертификата
3	TUSUR\FB$	Контроллер домена (DomainController)
4	TUSUR\FB$	ЦС Exchange (CAExchange)
7	TUSUR\Администра...	Кросс-сертификат (1.3.6.1.4.1.311.21.8.6686...
15	TUSUR\Администра...	Перекрестный центр сертификации (1.3.6....
18	TUSUR\Администра...	Пользователь (User)
19	TUSUR\Администра...	Перекрестный центр сертификации (1.3.6....
20	TUSUR\Администра...	Перекрестный центр сертификации (1.3.6....
21	TUSUR\NNNN_FIO	Подчиненный центр сертификации (SubCA)

Рис. 19. Список выданных сертификатов

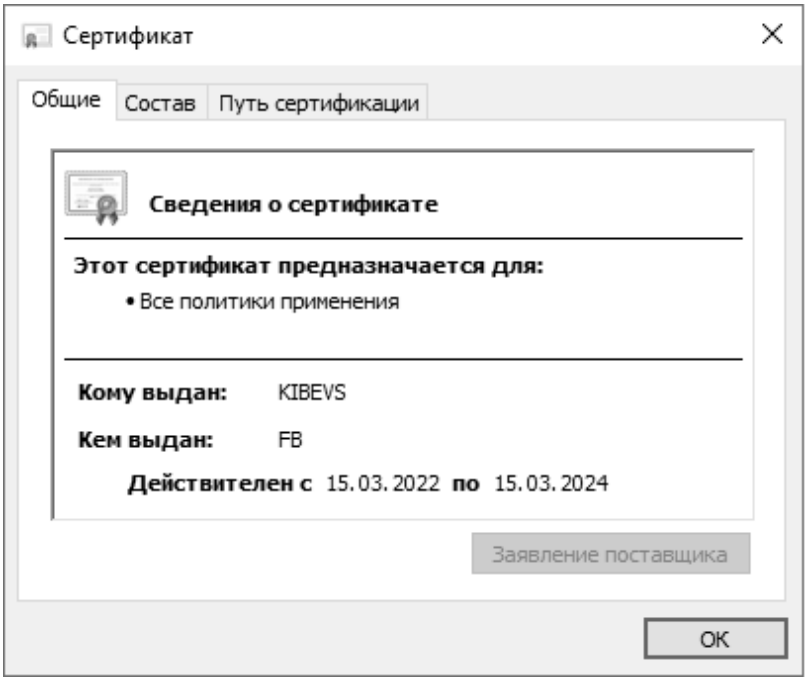

Рис. 20. Свойства сертификата подчиненного ЦС

Для того, чтобы подчиненный центр сертификации мог также выдавать сертификаты, как и корневой (УЦ ФБ) завершим его настройку в соответствии с указаниями по предыдущим работам. Иначе при попытке выдачи сертификата будет получена ошибка (рис. 21)

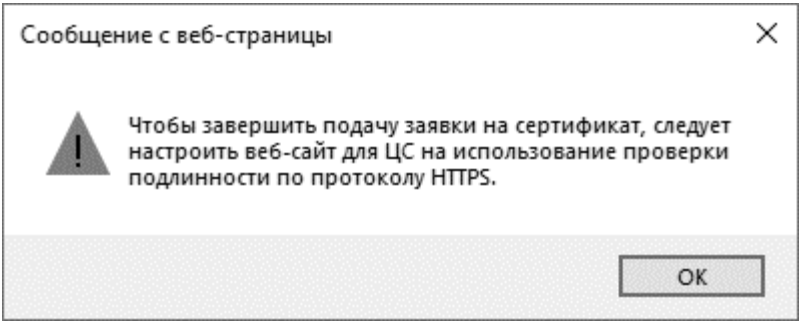

Рис. 21. Ошибка запроса сертификата

Для этого установим последний необходимый компонент «Веб-служба регистрации сертификатов». Для него необходимо выбрать корневой ЦС, к которому будет прикреплена данная служба.

Далее рассмотрим взаимодействие с удостоверяющими центрами с нижнего уровня иерархии, который будет представлен в методическом руководстве на примере виртуальной машины с ОС Windows 10. В качестве данного уровня иерархии может быть использована любая другая версия операционной системы. Единственное требование к виртуальной машине заключается в настройке сетевого подключения (рис. 22), позволяющее подключиться к первым двум машинам.

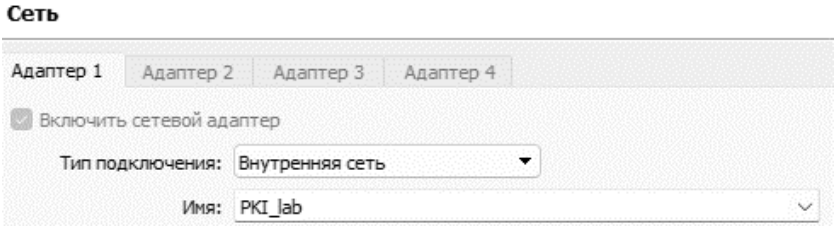

Рис. 22. Пример настройки сетевого адаптера виртуальной машины

Запустите третью виртуальную машину и установите на ней КриптоАРМ в режиме настраиваемой установки (рис. 23-24).

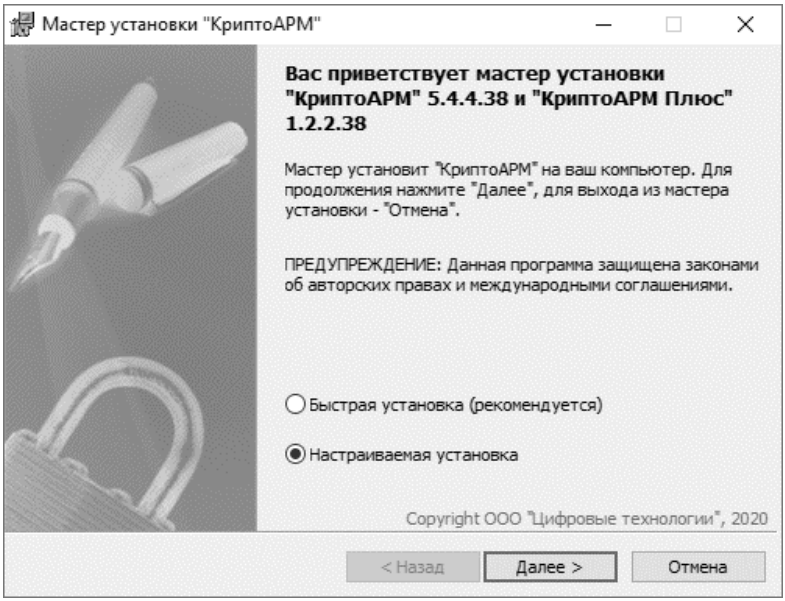

Рис. 23. Запуск установки КриптоАРМ

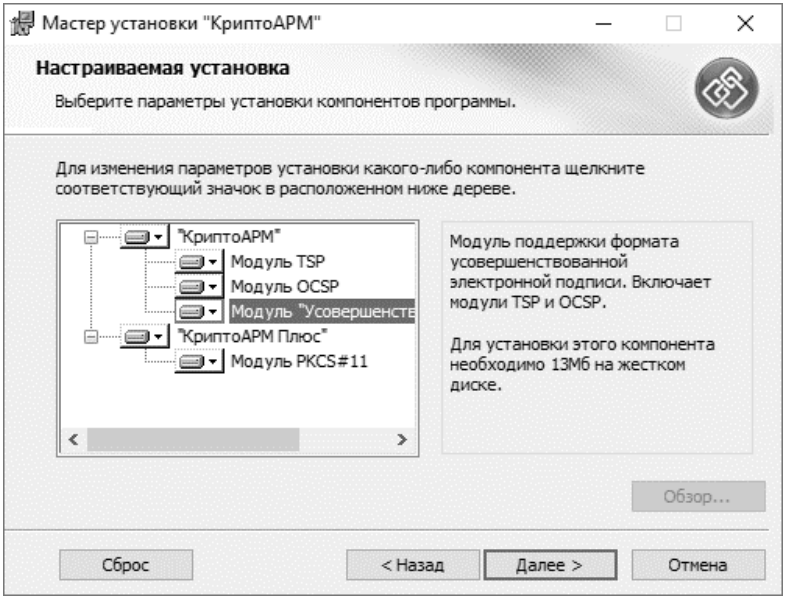

Рис. 24. Выбор установки всех доступных модулей

Для полного соответствия получаемой иерархии схеме на рисунке 2 включим третью виртуальную машину в домен tusur.ru. Для этого потребуется изменить параметры сетевого адаптера (рис. 25) и отключить брандмауэр.

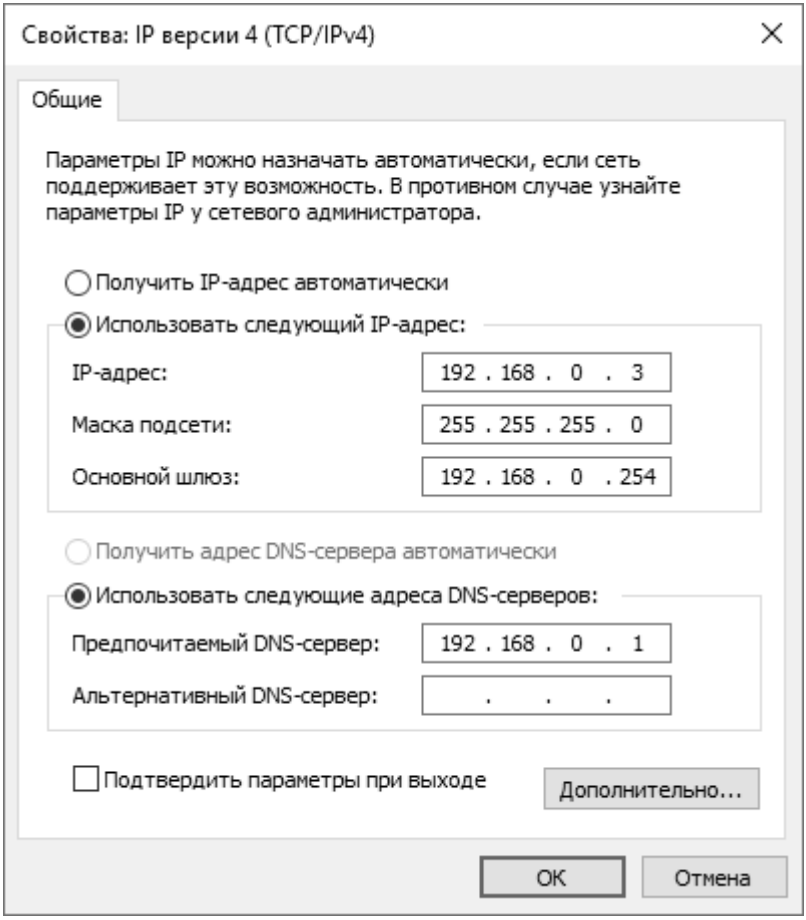

Рис. 25. Изменение параметров сетевого адаптера третьего уровня иерархии

Обратите внимание, что в случае присвоения компьютеру имени как на рис. 26, система выдаст предупреждение о нежелательности использования подобных имен. Поэтому можете вместо этого использовать в лабораторной работе свои инициалы в формате FIO.

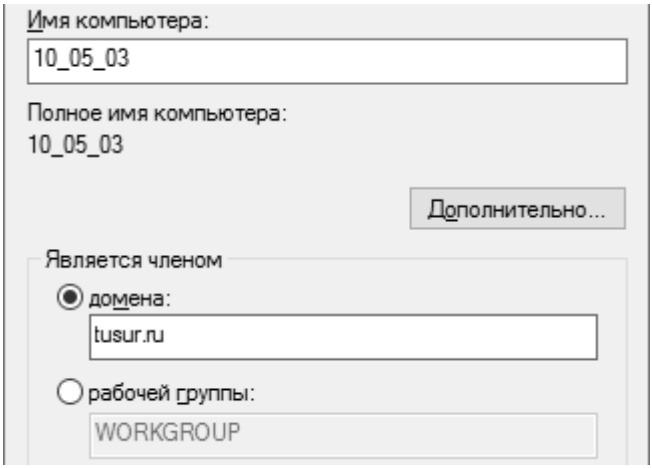

Рис. 26. Добавление компьютера в домен tusur.ru

После перезагрузки виртуальной машины зайдите под доменной учетной записью. Запустите Internet Explorer и в адресной строке укажите путь к подчиненному ЦС. По умолчанию это **http://192.168.0.2/certsrv**. От Вас потребуется ввести логин и пароль (рис. 27)

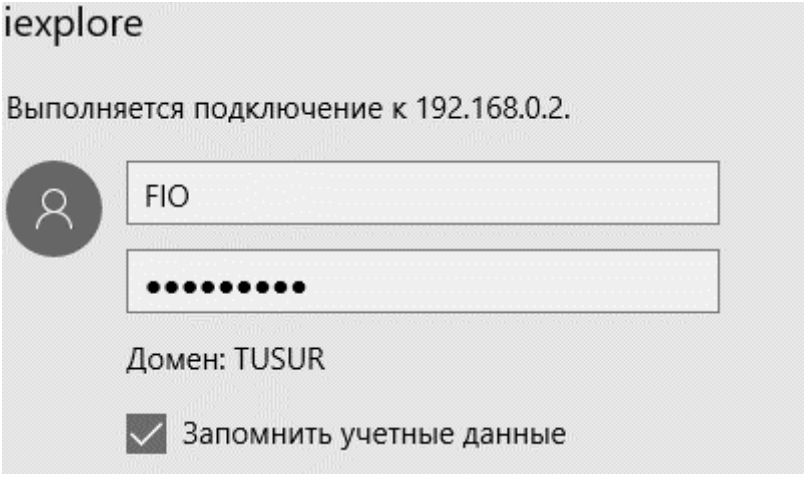

Рис. 27. Подключение к подчиненному центру сертификации

В результате успешной авторизации на виртуальной машине нижнего уровня отобразится веб-интерфейс подчиненного центра сертификации (рис. 28).

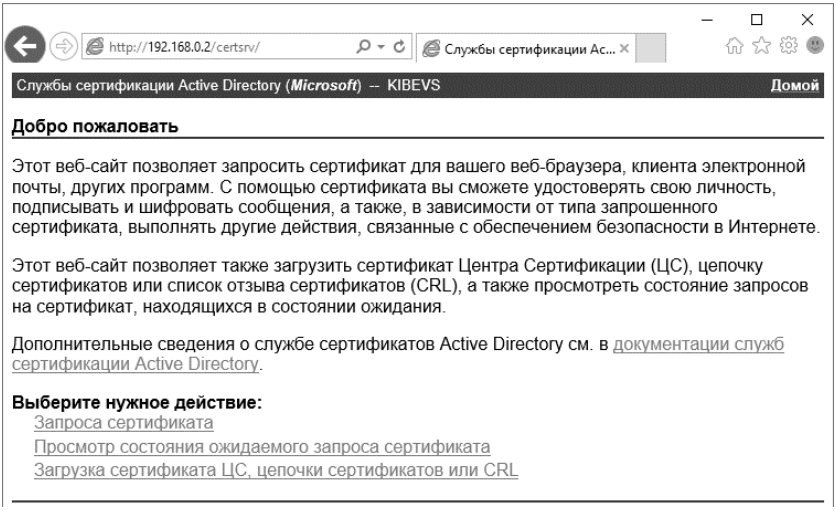

Рис. 28. Подчиненный центр сертификации

Далее необходимо получить сертификат от подчиненного центра сертификации. Запросите стандартный сертификат пользователя. Для этого последовательно вызываются функции «Запрос сертификата», «Сертификат пользователя» и «Выдать» (рис. 29).

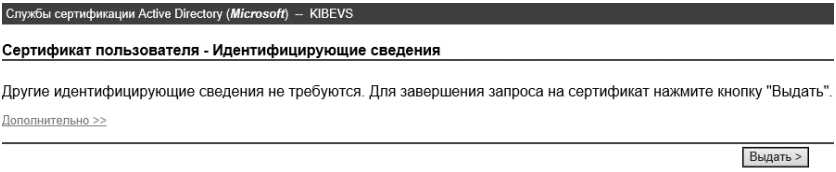

Рис. 29. Выдача сертификата

В результате проделанных действий будет получен сертификат (рис. 30). Установите сертификат нажатием на соответствующую команду. Далее Вы можете просмотреть содержание сертификата через соответствующую оснастку. В общих свойствах сертификата можно увидеть, что выдан этот сертификат был подчиненным центром сертификации – KIBEVS, а получателем является нижний уровень иерархии – FIO(рис. 31).

Службы сертификации Active Directory (*Microsoft*) -- KIBEVS

Сертификат выдан

Запрошенный вами сертификат был вам выдан.

Установить этот сертификат

☐ Сохранить ответ

Рис. 30. Получение сертификата

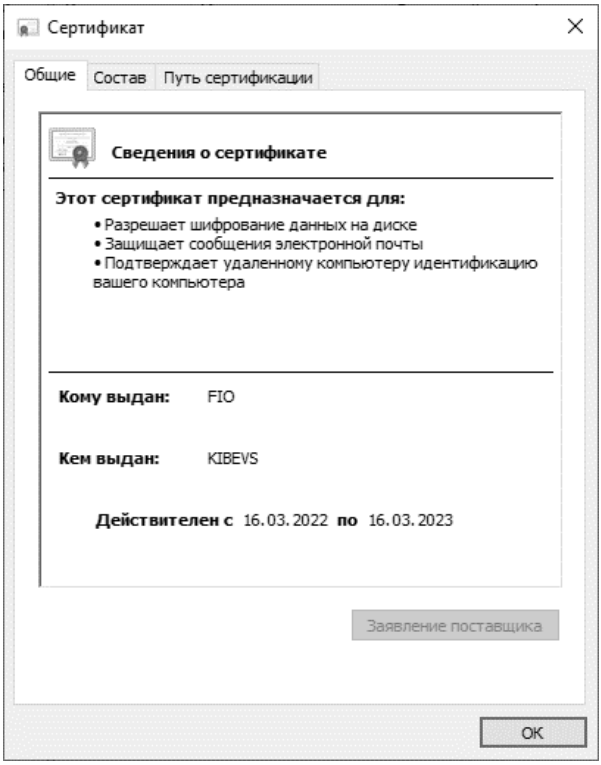

Рис. 31. Общие сведения сертификата

Более интересной будет вкладка «Путь сертификации» (рис. 32), в которой можно увидеть полное дерево иерархии от корневого центра сертификации до текущего уровня.

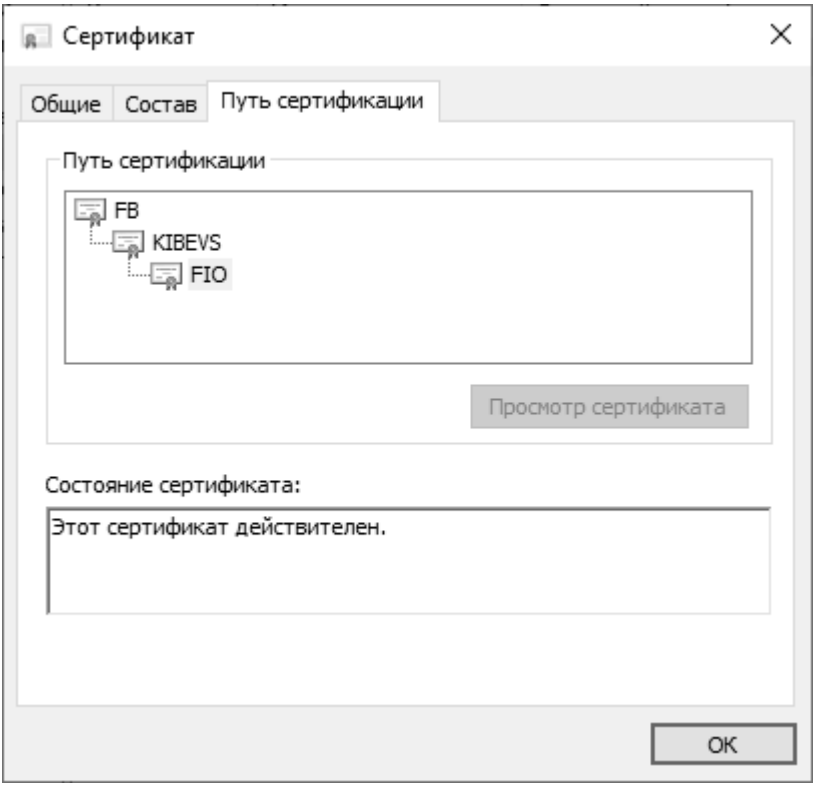

Рис. 32. Путь сертификации

3.2 Практическое изучение иерархической модели доверия

Вернемся к работе с КриптоАРМ. Для этого создайте на рабочем столе текстовый документ с любым непустым содержанием. После этого запустите КриптоАРМ и нажмите кнопку «Подписать» (рис. 33).

В результате будет запущен мастер создания электронной подписи (рис. 34), которому потребуется последовательно сообщить настройки для нового профиля подписи (в дальнейшем его можно будет выбирать для автоматизации процесса).

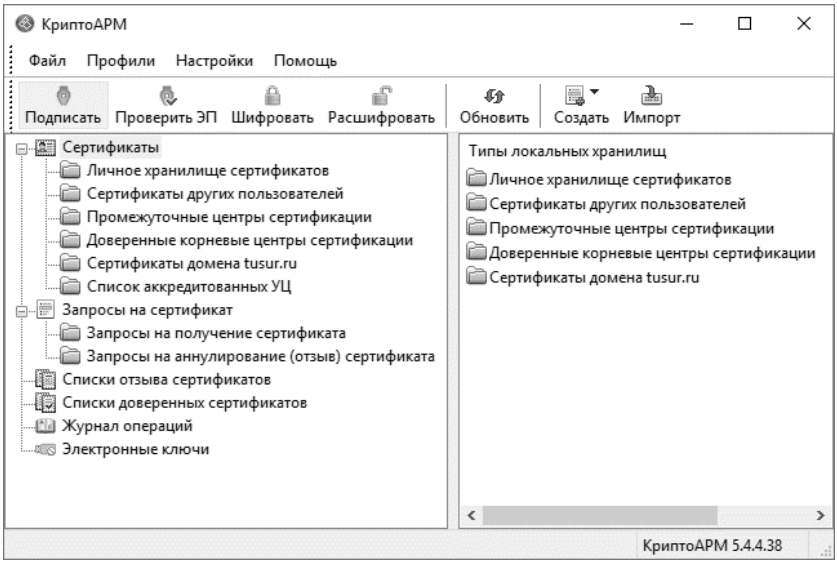

Рис. 33. Интерфейс программы КриптоАРМ

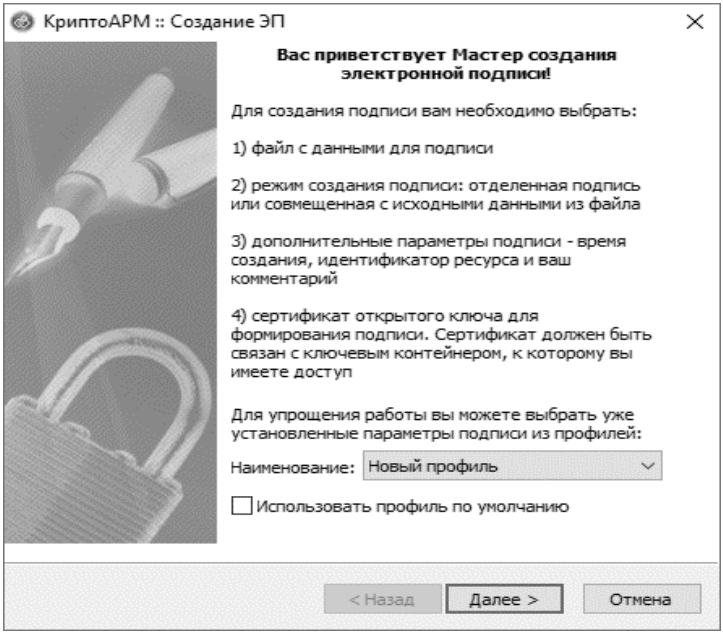

Рис. 34. Мастер создания электронной подписи

Выберите ранее созданный файл (рис. 35) нажатием на кнопку «Добавить файл». В результате будет открыт «Проводник» для поиска необходимого файла. В качестве примера показан выбор файла «Документ.txt» на рабочем столе, созданный ранее. Текст на рисунке был указан произвольный. Не обязательно указывать в своей работе именно его.

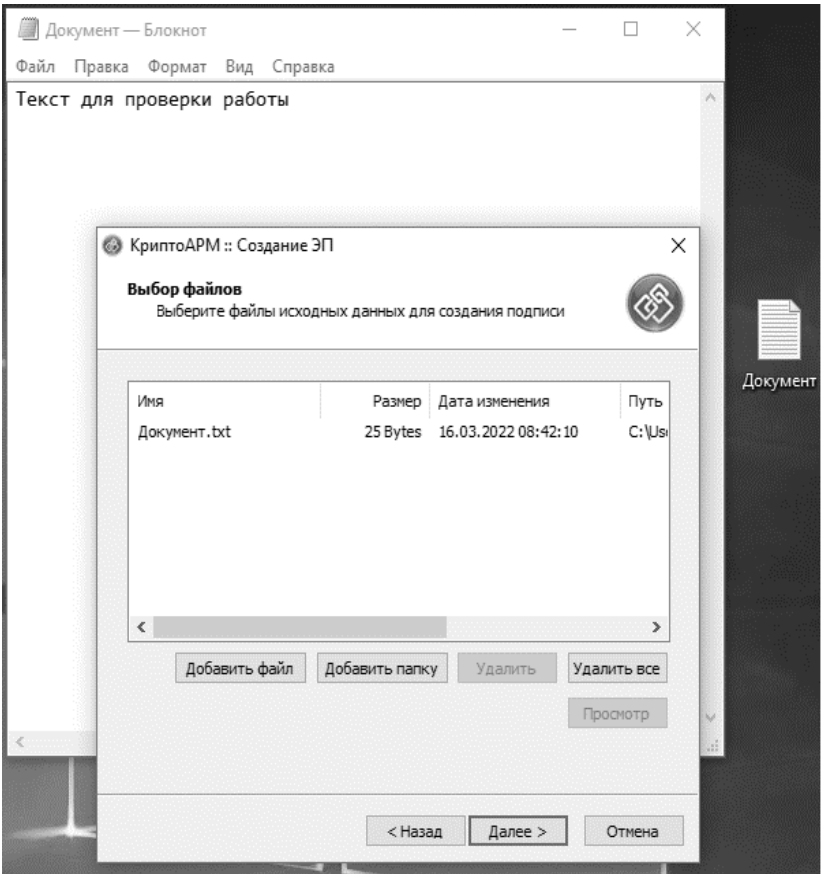

Рис. 35. Выбор файлов для проставления на них электронной подписи

В разделе «Свойства подписи» для пункта «Использование подписи» выберите вариант «Подписано», а в поле «Включить в подпись» – «Все сертификаты пути сертификации» (рис. 36). Остальные параметры на данной вкладке можно оставить по умолчанию.

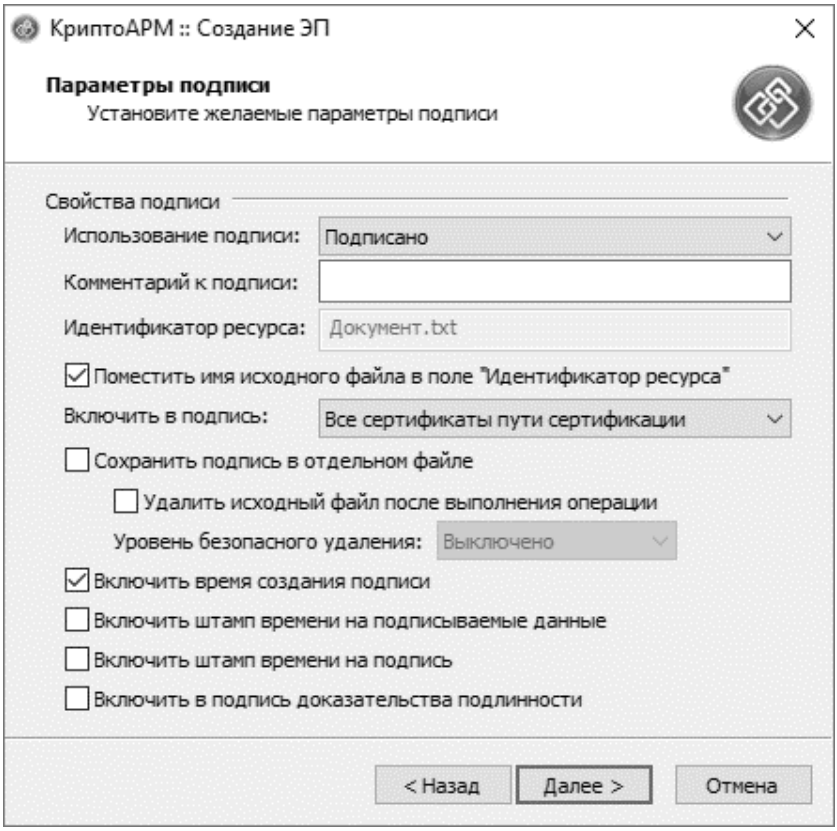

Рис. 36. Свойства создаваемой электронной подписи

Далее от пользователя потребуется указать сертификат, с помощью которого можно проставить электронную подпись на выбранный документ. Этот сертификат мы ранее получили от подчиненного удостоверяющего центра (рис. 30).

Нажмите на кнопку «Выбрать» (рис. 37) для перехода к обзору содержимого хранилища сертификатов (рис. 38). Здесь мы можем найти ранее добавленный в хранилище сертификат, полученный от подчиненного центра сертификации. В случае, если необходимого сертификата в списке не будет – его можно добавить путем нажатия на кнопку «Импорт» и поиском по проводнику. В результате в меню выбора сертификата будет отображена основная информация по

выбранному сертификату. Также здесь можно просмотреть содержание сертификата.

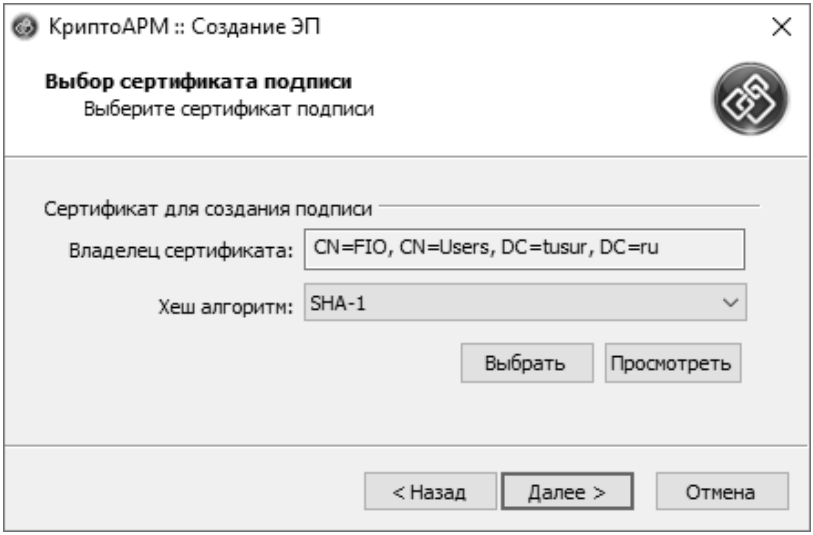

Рис. 37. Выбор сертификата для проставления электронной подписи

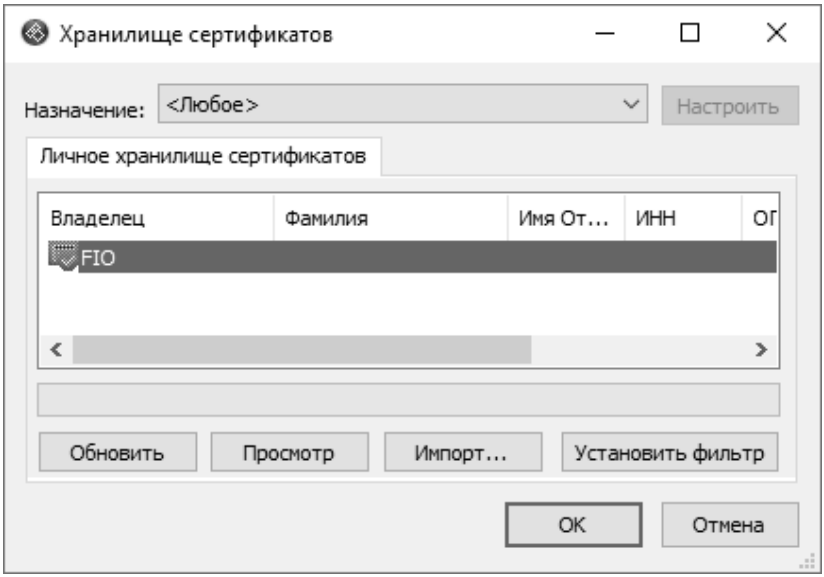

Рис. 38. Выбор сертификата из хранилища

В результате выполнения описанных действий будет произведена электронная подпись выбранного документа. Об этом нам будет выведено соответствующее уведомление (рис. 39), а в директории с подписанным файлом появится файл электронной подписи (рис. 40).

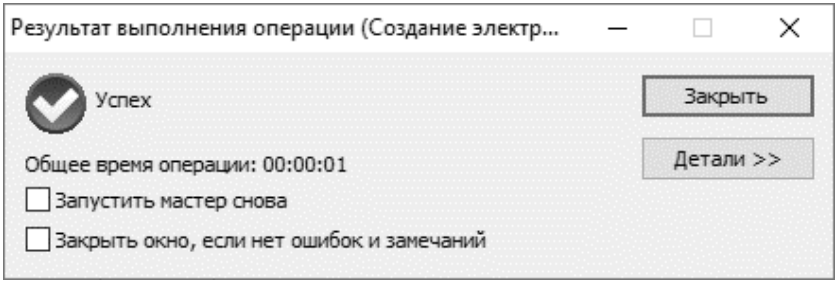

Рис. 39. Уведомление об успешном проставлении электронной подписи

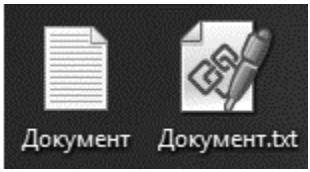

Рис. 40. Файл электронной подписи рядом с подписанным документом

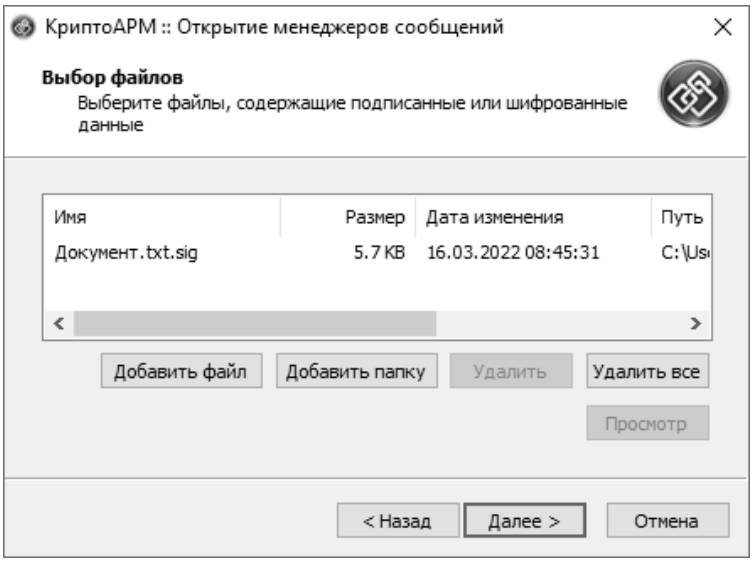

Рис. 41. Открытие полученного файла электронной подписи

Данный файл подписи можно открыть с помощью КриптоАРМ и просмотреть его содержание (рис. 41). Для этого необходимо выбрать файл (в данном варианте – Документ.txt.sig) и нажать кнопку «Просмотр».

В результате выполнения данного действия откроется меню управления подписанными данными (рис. 42). В данном окне можно выполнить ряд операций над подписанным документом, но для нас в рамках лабораторной работы будет интересен пункт «Просмотреть».

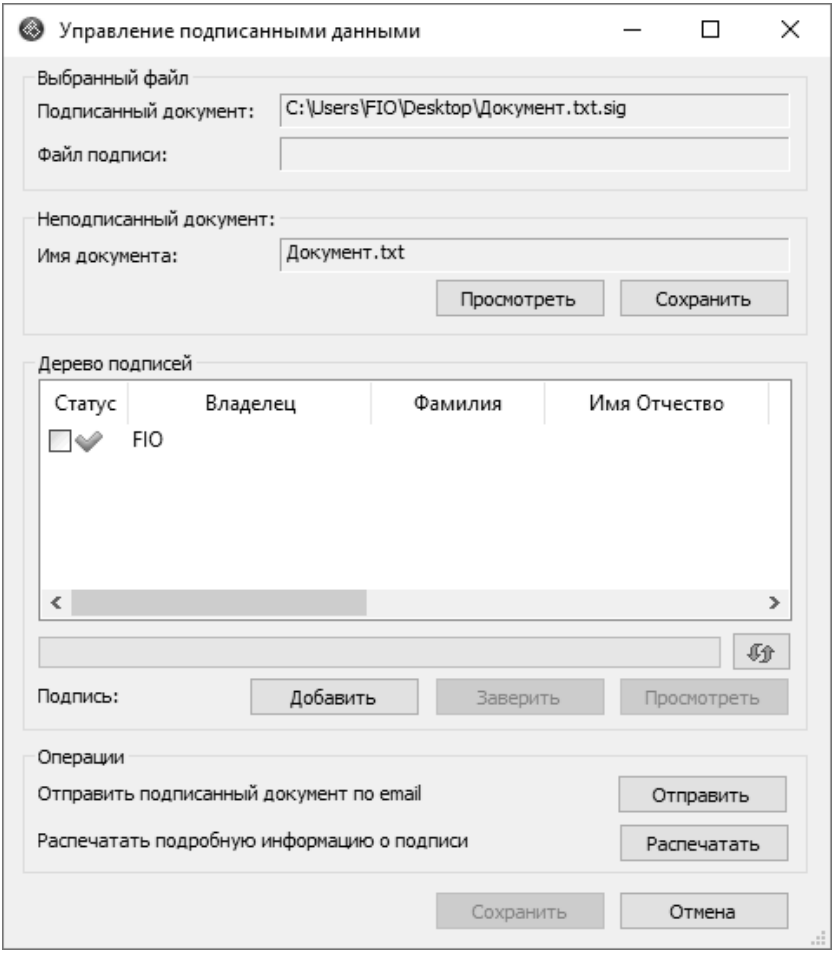

Рис. 42. Открытие полученного файла электронной подписи

В открывшемся окне будет возможно изучить содержание трех вкладок:

- Подпись (рис. 43). В данном разделе отображается информация, указанная нами на этапе создания подписи (рис. 36). Кроме того указан алгоритмы, с помощью которых была сформирована электронная подпись и произведено хеширование данных.

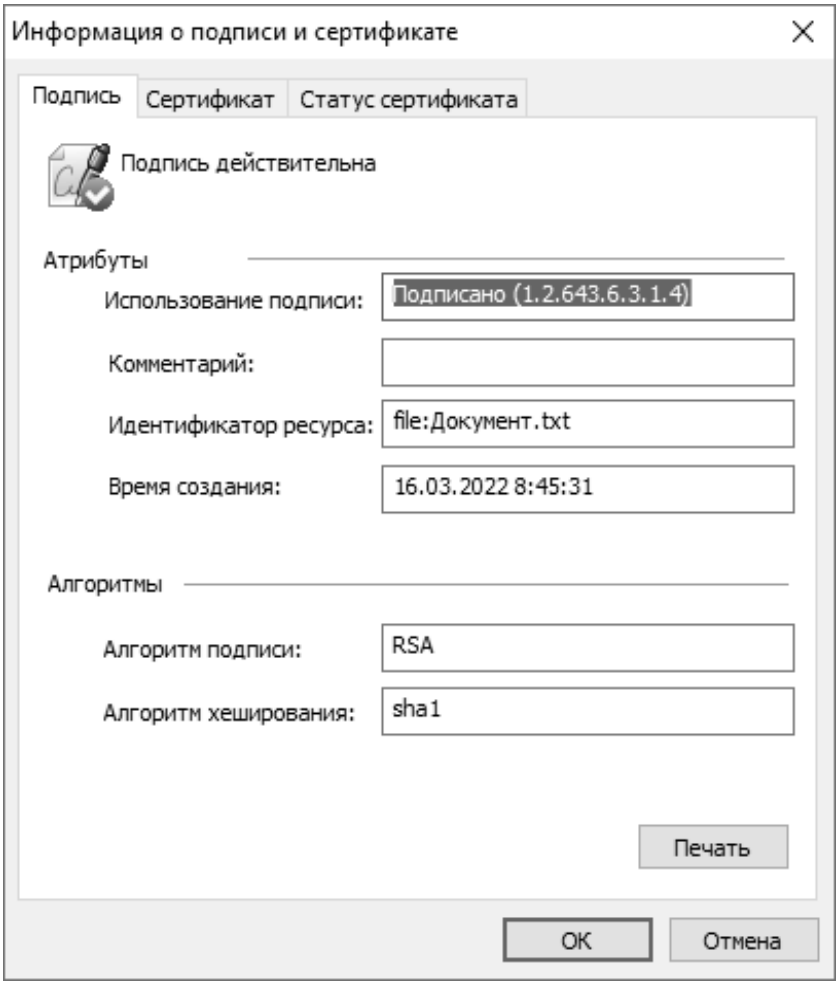

Рис. 43. Открытие полученного файла электронной подписи

- Сертификат (рис. 44). В данной вкладке можно увидеть всю информацию о владельце сертификата и подчиненного центре сертификации, который является его издателем. Также здесь указаны сведения по срокам действия сертификата и закрытого ключа. По нажатию кнопки «Просмотреть» будет открыт сам сертификат.

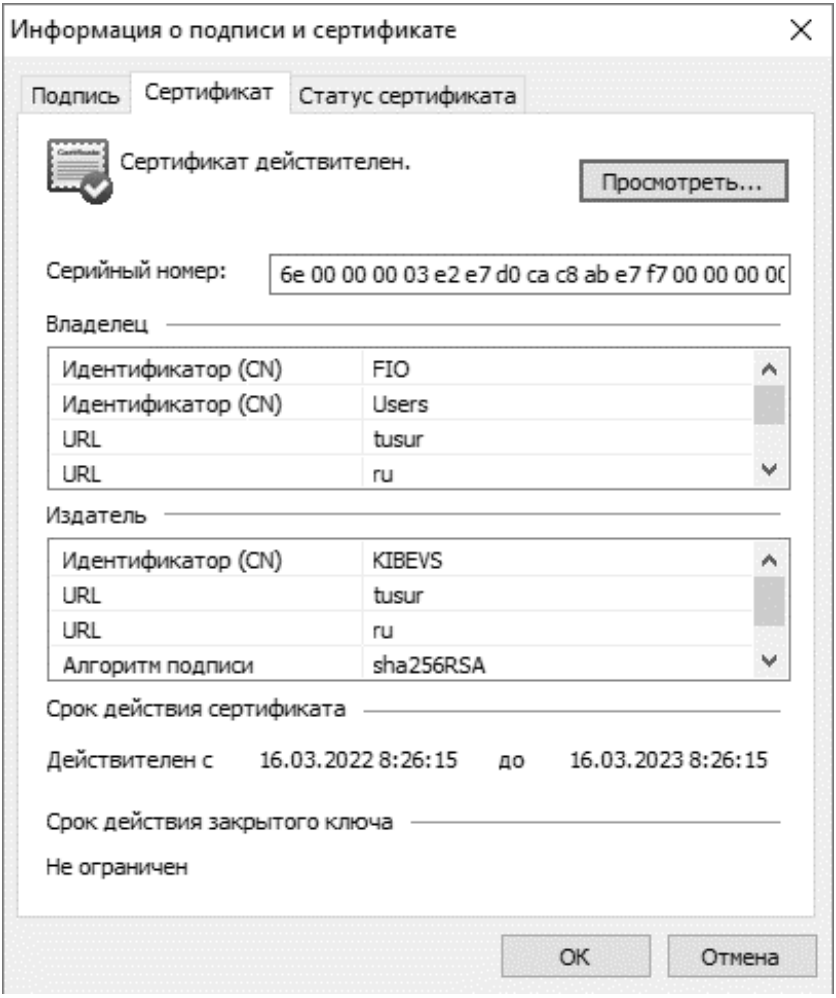

Рис. 44. Просмотр данных сертификата подписи

- Статус сертификата (рис. 45). Здесь мы можем увидеть информацию о действительности использованного сертификата и полную цепочку, аналогичную той, что была

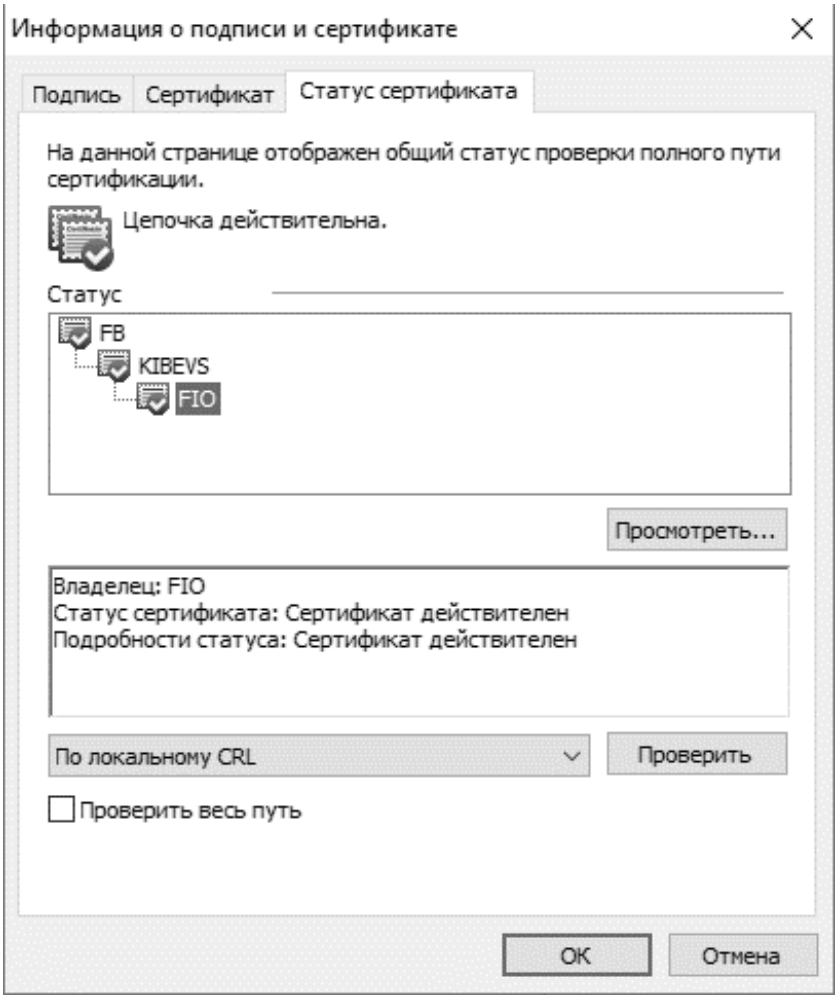

Рис. 45. Проверка статуса сертификата

Далее рассмотрим, как будет выглядеть работа уровней иерархической архитектуры при отказе работы ее компонентов.

В качестве примера рассмотрит отзыв сертификата, выданного подчиненному удостоверяющему центру. Для этого перейдите в корневой удостоверяющий центр, выберите в оснастке «Центр сертификации» вкладку «Выданные сертификаты». Среди сертификатов выберите необходимый и в контекстном меню для него выберите задачу «Отзыв сертификата» (рис. 46).

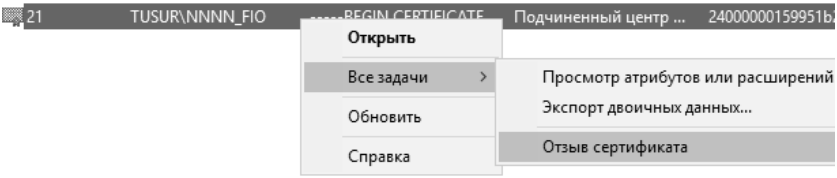

Рис. 46. Запуск процедуры отзыва сертификата

Появится окно отзыва сертификатов (рис. 47), в котором необходимо указать причины, дату и время для отзыва сертификата. Для данного примера необходимо выбрать причину «Приостановка действий». Далее нам потребуется восстановить действие сертификата, а остальные варианты данную процедуру совершить не позволят. Проверьте, что сертификат был отозван в другой вкладке ЦС (рис.48)

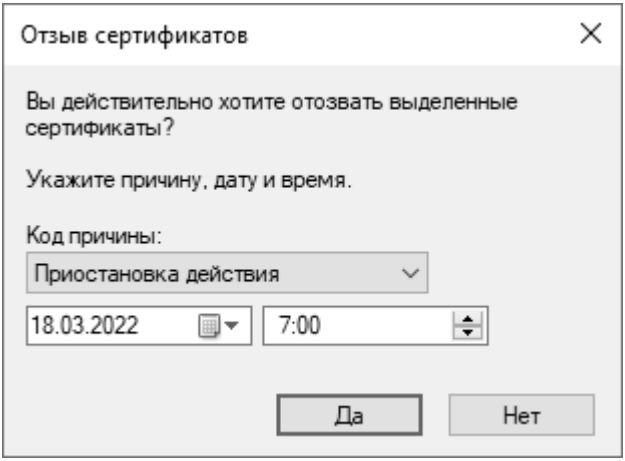

Рис. 47. Параметры отзыва сертификата

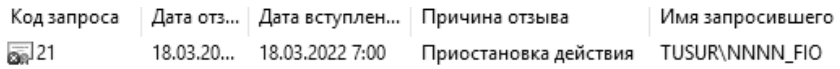

Рис. 48. Отозванный сертификат

Во вкладке «Отозванные сертификаты» присутствует только что отозванный сертификат, но информация об этом еще не опубликована. Чтобы это исправить нажмите правой кнопкой мыши в любом месте в данном разделе и выберите задачу «Публикация» (рис. 49).

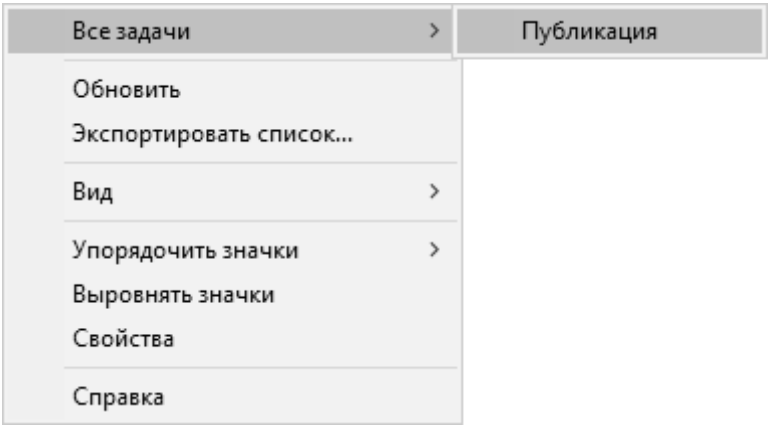

Рис. 49. Вызов процедуры публикации списка отозванных сертификатов

Появится окно выбора типа публикуемого списка отозванных сертификатов. Выберите «Новый базовый CRL» (рис. 50).

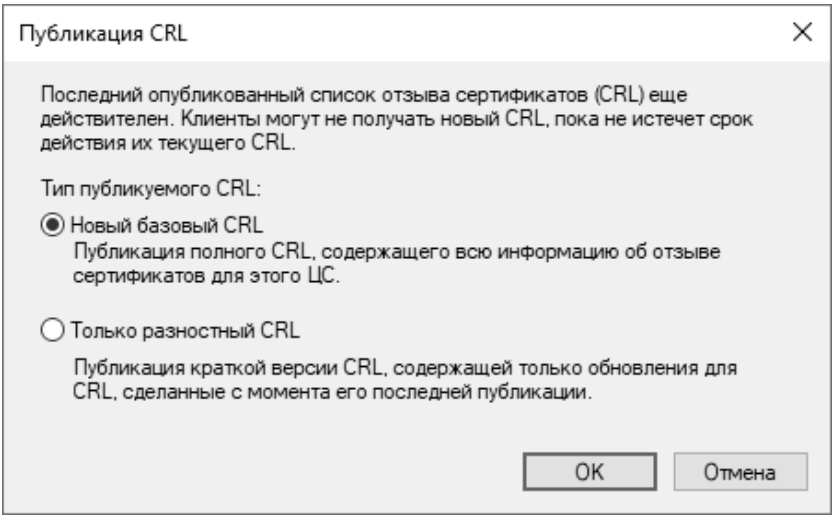

Рис. 50. Вызов процедуры публикации списка отозванных сертификатов

Перейдите на виртуальную машину нижнего уровня иерархии и откройте ранее созданную электронную подпись. Статус подписи сменился на знак вопроса, а во вкладке «Статус сертификата» для нижнего уровня иерархии для все параметров указано «Статус неизвестен» (рис. 51).

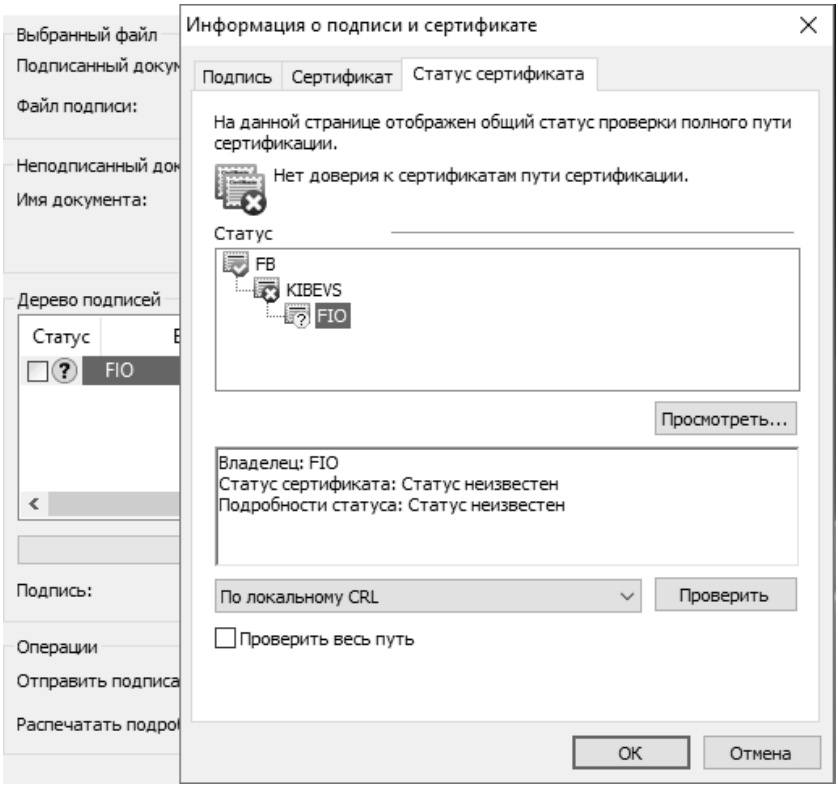

Рис. 51. Статус электронной подписи после отзыва сертификата

Данный результат связан с тем, что у подчиненного центра сертификации был отозван сертификат (рис. 52), что является промежуточным уровнем между корневым удостоверяющим центром и нижним уровнем.

Отмените отзыв сертификата. Для этого перейдите на корневом УЦ во вкладку «Отозванные сертификаты» и в контекстном меню выберите соответствующий пункт для нужного сертификата (рис. 53).

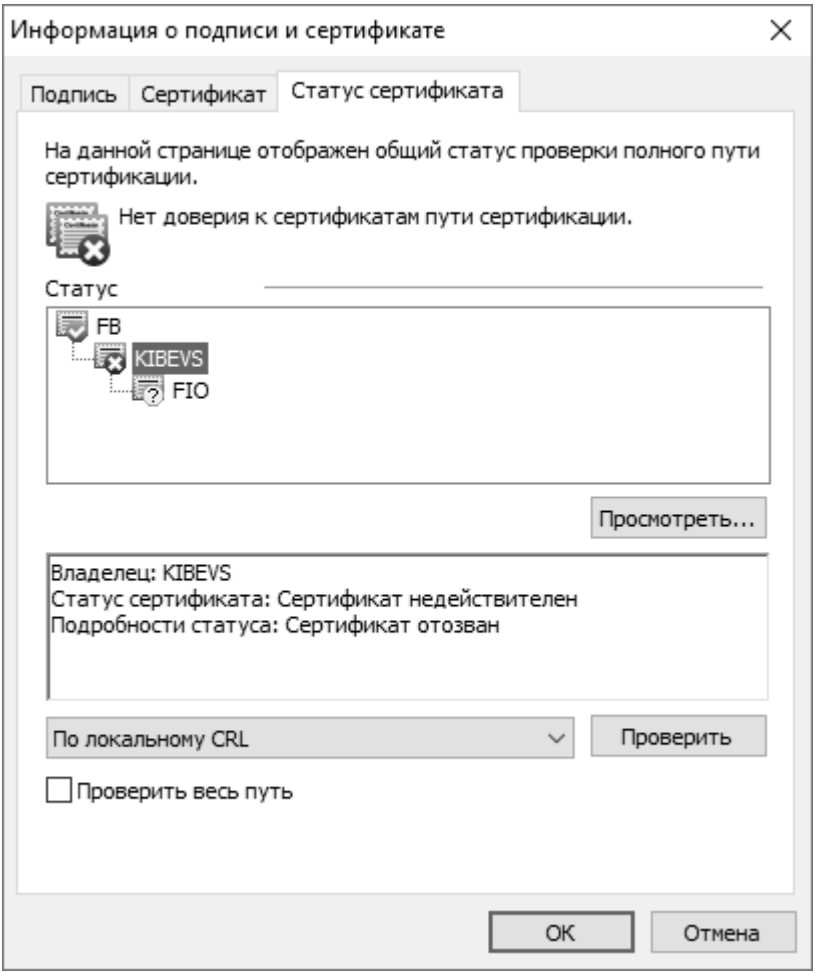

Рис. 52. Статус сертификата подчиненного центра сертификации

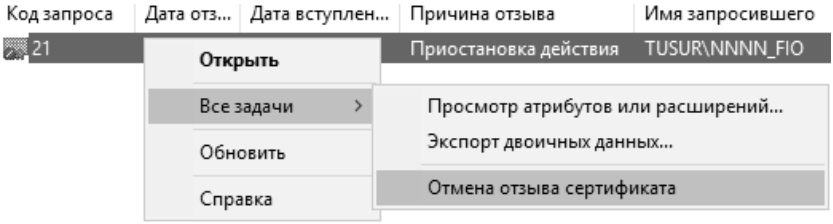

Рис. 53. Отмена отзыва сертификата

Далее снова потребуется провести процедуру публикации списка отозванных сертификатов. Проверьте, что сертификат снова отображается во вкладке «Выданные сертификаты», а в свойствах электронной подписи восстановилось доверие к цепочке сертификации.

4. Задание на лабораторную работу

1. Ознакомиться с теорией (включая лекционные материалы).
2. Реализовать иерархическую архитектуру, состоящую из двух удостоверяющих центров и клиентской машины.
3. Подписать на клиентской машине документ с помощью, сертификата, полученного от подчиненного удостоверяющего центра.
4. Проверить состояние электронной подписи после отзыва сертификата корневым удостоверяющим центром.
5. Составить по проделанной работе отчет.

5. Контрольные вопросы

1. Объясните разницу между строгой и нестрогой иерархиями удостоверяющих центров.
2. Какие отличия между корневым и подчиненным удостоверяющими центрами?
3. Поясните понятие «путь сертификации».
4. Какие этапы включены в обработку пути?
5. Опишите алгоритм отзыва сертификата.
6. Какие причины можно указать при отзыве сертификата?
7. Опишите алгоритм восстановления отозванного сертификата.
8. Действие любого отозванного сертификата может быть возобновлено?
9. Для чего необходимо публиковать списки отозванных сертификатов после восстановления отозванного сертификата?
10. Какие существуют варианты проверки действия сертификата?

ЛАБОРАТОРНАЯ РАБОТА №8
Применение криптопровайдеров

1. Цель работы

Целью лабораторной работы является получение практических навыков по установке, настройке и применению криптопровайдеров в различных программах.

2. Краткие теоретические сведения

Криптопровайдер – средство криптографической защиты информации (СКЗИ), программный продукт, для авторизации и обеспечения юридической значимости электронного документооборота между участниками взаимодействия, посредством использования процедур формирования и проверки электронной подписи (ЭП), а также обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты.

Под криптовайдером понимается некий независимый модуль, который позволяет осуществлять криптографические операции в операционных системах Microsoft, управление которым происходит с помощью функций CryptoAPI. Проще говоря, это посредник между операционной системой, которая может управлять им с помощью стандартных функций CryptoAPI, и исполнителем криптографических операций (это может быть как программа, так и аппаратный комплекс).

CryptoAPI (Cryptographic Application Programming Interface) — интерфейс программирования приложений, который обеспечивает разработчиков Windows-приложений стандартным набором функций для работы с криптопровайдером. Входит в состав операционных систем Microsoft. Большинство функций CryptoAPI поддерживается, начиная с Windows 2000. CryptoAPI поддерживает работу с асимметричными и симметричными ключами, то есть позволяет шифровать и расшифровывать данные, а также работать с электронными сертификатами. Набор поддерживаемых криптографических алгоритмов зависит от конкретного криптопровайдера.

Интерфейс Microsoft CryptoAPl содержит как функции, осуществляющие базовые криптографические преобразования, так и функции, реализующие преобразования более высокого уровня - работу с сертификатами X.509, работу с криптографическими сообщениями PKCS#7 и другие функции, поддерживающие так называемую инфраструктуру открытых ключей. Данный интерфейс является

криптографическим ядром прикладного уровня современных операционных систем Microsoft.

Задачи CryptoAPI:

- надежное сокрытие данных;
- возможность передачи сокрытых данных третьим лицам;
- надежная система проверки достоверности пришедшей от третьих лиц информации;
- расшифровывание полученных конфиденциальных данных;
- работа с "идентификационными удостоверениями" третьих лиц;
- обеспечение работы с признанными криптографическими стандартами;
- возможность расширения и работы с пока еще неизвестными алгоритмами.

Реализация всех алгоритмов полностью выведена из состава CryptoAPI и реализуется в независимых динамических библиотеках - «криптопровайдерах». CryptoAPI предоставляет конечному пользователю унифицированный интерфейс работы с функциями криптопровайдера.

Любой криптопровайдер должен экспортировать набор обязательных функций, которые формируют системный программный интерфейс CryptoAPI, при этом каждая из этих функций соответствует некоторой функции CryptoAPI. Также криптопровайдер должен обеспечивать:

- реализацию стандартного интерфейса криптопровайдера;
- работу с ключами шифрования, предназначенными для обеспечения работы алгоритмов, специфичных для данного криптопровайдера;
- невозможность вмешательства третьих лиц в схемы работы алгоритмов.

Приложения не работают напрямую с криптопровайдером. Вместо этого они вызывают функции CryptoAPI из библиотек Advapi32.dll и Crypt32.dll. Операционная система фильтрует вызовы этих функций и вызывает соответствующие функции CryptoAPI, которые непосредственно работают с криптопровайдером.

Минимальный состав криптопровайдера — одна DLL. Обычно эта библиотека хранится в папке \WINDOWS\system32\. Обязательным является контроль целостности этой DLL. Кроме стандартных функций CryptoAPI, криптопровайдер обычно поддерживает ряд собственных

функций. Если собственные функции не реализованы, то DLL действует, по сути, как промежуточный слой между операционной системой и исполнителем криптографических операций.

Одним из основных объектов является ключевой контейнер. В контейнере может существовать не более одной пары ключей подписи, одной пары ключей обмена и одного симметричного ключа. Если поддерживается несколько алгоритмов симметричного шифрования, то симметричных ключей может быть несколько, по одному ключу каждого алгоритма.

Пары ключей и симметричные ключи могут находиться только в контейнере. Только открытый ключ пары может находиться вне контейнера.

Закрытые (private) ключи пар ключей экспортируются только в зашифрованном виде. Некоторые криптопровайдеры принципиально не позволяют экспортировать закрытые ключи, даже в зашифрованном виде. Симметричные ключи при экспорте также обязательно шифруются на открытом ключе получателя или ключе согласования. Для вычисления хеш-функций создаются объекты хеширования. Для создания объектов хеширования создавать контейнер не нужно.

3. Ход работы

3.1 Подготовка к изучению криптопровайдеров

Перед тем, как приступить к работе с криптопровайдерами, проведем небольшую подготовительную работу. Подготовка к работе включает в себя два обязательных этапа:

- сохранение состояния используемой виртуальной машины;
- анализ текущего набора доступных криптографических алгоритмов.

Определить набор доступных алгоритмов криптографических преобразований можно основываясь на доступных в операционной системе криптопровайдерах. Если Вы уже выполняли работы по удостоверяющим центрам, то сталкивались с выбором из набора необходимого криптопровайдера (рис. 1).

Рис. 1. Выбор криптопровайдера для генерации ключей на УЦ

Предлагаемые наборы криптопровайдеров определены в соответствующей вкладке свойств шаблона каждого сертификата. Запустите оснастку «Шаблоны сертификатов» и откройте свойства сертификата «Пользователь» (рис. 2). Здесь будут выбраны те же поставщики, которые мы увидели в списке доступных для генерации ключей.

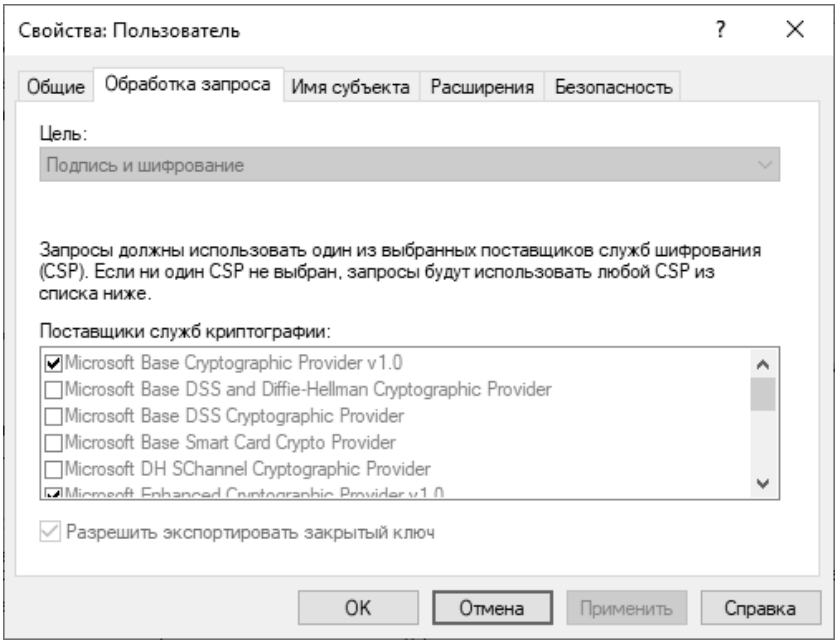

Рис. 2. Поставщики служб криптографии шаблона сертификата «Пользователь»

Для стандартных шаблонов заранее определены криптопровайдеры. Но для шаблонов, которые Вы создаете на их основе, можно будет указать собственный набор криптопровайдеров. Этому будет посвящена часть выполняемых работ с каждым из рассматриваемых СКЗИ – созданию шаблона сертификата со службами, поставляемыми данным поставщиком криптографических функций, и выдаче сертификатов по данным шаблонам.

Следует учесть, что изучаемые в работе криптопровайдеры, хоть и предоставляют возможность работы с одними и теми же криптографическими алгоритмами, не тождественны между собой. В первую очередь это связано с тем, что реализуемые ими ГОСТы не определяют параметры криптографических алгоритмов. Это дает

возможность разработчикам СКЗИ самостоятельно их задавать. Из этого не следует, что СКЗИ разных производителей обязательно будут совместимы.

Первоначально на отечественном рынке криптопровайдеров возникла ситуация, при которой было невозможно взаимодействие пользователей разных СКЗИ. Однако, в дальнейшем компания Крипто-Про выступила с инициативой об унификации параметров и форматов, используемых при реализации алгоритмов ГОСТ, к которому присоединились ведущие разработчики СКЗИ.

С целью предотвращения сбоев в работе виртуальной машины, на которой будет проводиться изучение возможностей криптопровайдеров, рекомендуется перед началом работы с ними создать снимок текущего состояния виртуальной машины (рис. 3).

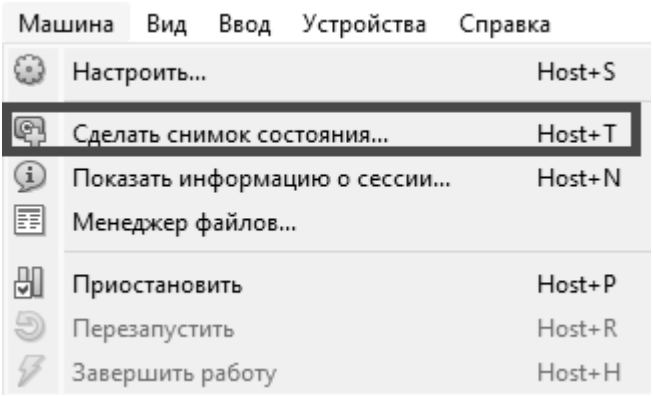

Рис. 3. Выбор криптопровайдера для генерации ключей на УЦ

3.2 Средство криптографической защиты информации «Signal-COM CSP»

3.2.1 Краткие сведения о СКЗИ

Первый криптопровайдер, с которым необходимо познакомиться в рамках данной лабораторной работы, это продукт компании «Сигнал-КОМ»». Криптопровайдер Signal-COM CSP поддерживает российские криптографические алгоритмы и обеспечивает к ним доступ из пользовательских приложений через стандартный криптографический интерфейс компании Microsoft — CryptoAPI 2.0.

Согласно информации, взятой с их сайта, данный криптопровайдер выполнен в соответствии с технологией Cryptographic Service Provider (CSP), благодаря чему российские алгоритмы

шифрования и ЭП могут использоваться во многих популярных и широко распространенных приложениях:

- Удостоверяющий Центр Microsoft Certification Authority;
- Приложения Microsoft Office (MS Outlook, MS Word, MS Excel, MS Power Point, MS Info Path);
- почтовый клиент Microsoft Outlook Express;
- приложение контроля целостности программного обеспечения Microsoft Authenticode;
- программа для защиты файлов КриптоАРМ (разработчик — ООО «Цифровые технологии»);
- почтовый клиент The Bat! (разработчик — компания «RITLABS»);
- система защиты конфиденциальной информации на персональном компьютере Secret Disk NG (разработчик — компания «ALADDIN Software Security R.D.») и др.

В состав СКЗИ также входит модуль Signal-COM TLS, разработанный в соответствии с криптографическим интерфейсом Microsoft — Security Support Provider Interface (SSPI). Signal-COM TLS является расширением стандартного провайдера MS Schannel и позволяет использовать протокол TLS с российскими криптографическими алгоритмами в стандартных приложениях Microsoft:

- Internet Information Server,
- Internet Explorer.

Криптографические ключи, используемые в СКЗИ «Signal-COM CSP», подразделяются на сеансовые и парные (с открытым ключом). Сеансовые ключи используются в симметричных (одноключевых) алгоритмах для зашифрования и расшифрования данных. Они создаются на определенный сеанс работы с СКЗИ «Signal-COM CSP» и уничтожаются после его завершения.

Парные ключи используются в алгоритмах с открытым ключом для формирования цифровых подписей и зашифрования сеансовых ключей. Они состоят из закрытого ключа, который должен быть известен только его владельцу, и открытого ключа, который в виде сертификата (см. ниже) может и должен распространяться свободно (помещаться в открытые справочники, передаваться по почте и т.д.). С помощью парного закрытого ключа осуществляется формирование цифровой подписи владельца ключа и расшифрование сеансовых ключей. Парный открытый ключ используется для проверки цифровой подписи, сформированной закрытым ключом, и для зашифрования

сеансовых ключей, которые, в свою очередь, используются для зашифрования сообщения в адрес владельца закрытого ключа.

Парные ключи условно подразделяются на ключи подписи и ключи обмена (ключи зашифрования сеансовых ключей), хотя и те, и другие могут использоваться для формирования цифровой подписи и зашифрования сеансовых ключей. Для обеспечения высокого уровня безопасности рекомендуется использовать одну пару ключей для формирования цифровых подписей и другую пару ключей - для зашифрования сеансовых ключей.

3.2.2 Установка и настройка СКЗИ

Перейдем к изучению средства криптографической защиты информации «Signal-COM CSP». Запустите программу установки СКЗИ (рис. 4).

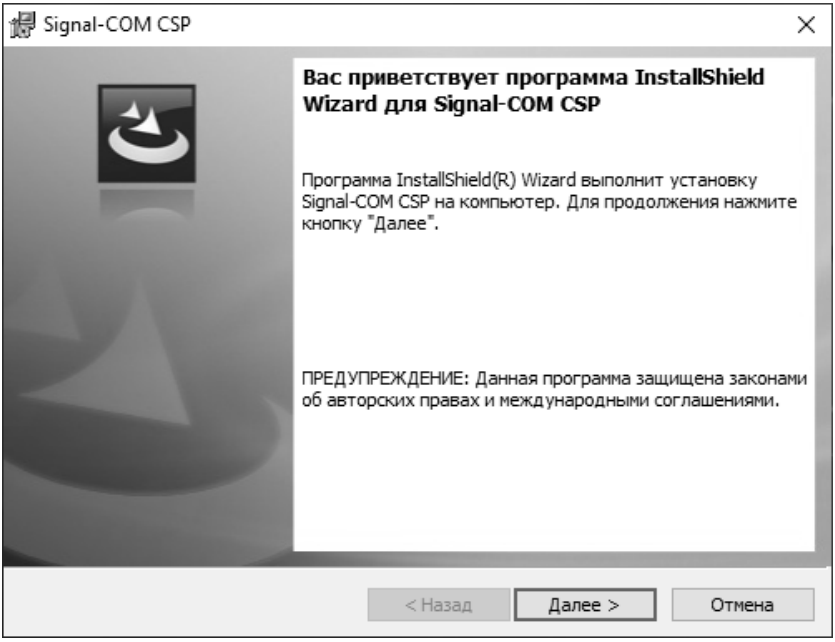

Рис. 4. Запуск мастера установки СКЗИ «Signal-COM CSP»

Примите условия лицензионного соглашения и перейдите к следующему шагу установки. Укажите имя и организацию для пользователя, от чьего имени будет происходить дальнейшая работа. Изучение принципов работы криптопровайдера будет осуществляться

на примере демонстрационной версии – поэтому поле ключа оставьте пустым (рис. 5).

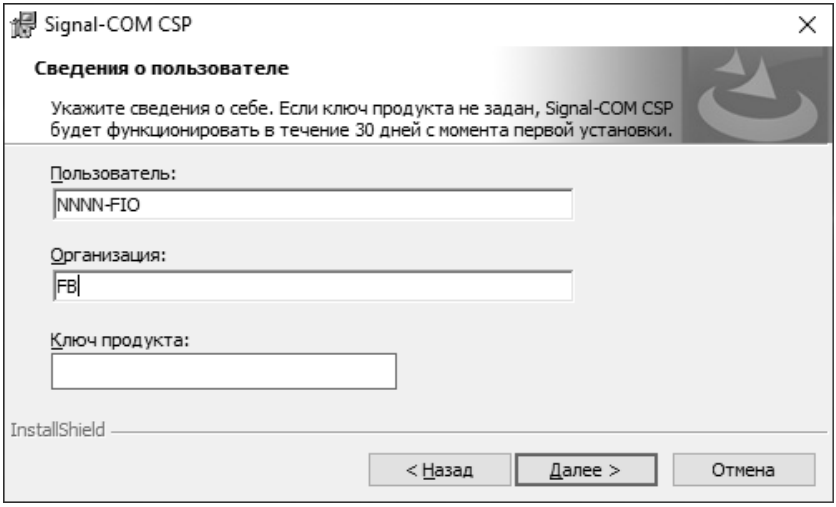

Рис. 5. Ввод сведений о пользователе

Далее потребуется выбрать необходимые компоненты для работы криптопровайдера. Выберите установки обоих модулей.

Модуль Signal-COM CSP (рис. 6) обеспечивает совместимость с криптографическими приложениями, построенными на базе СКЗИ различных российских компаний:

- в части параметров криптографических алгоритмов электронной подписи (ГОСТ Р 34.10-2012), хэширования (ГОСТ Р 34.11-2012) и шифрования (ГОСТ 28147-89);
- в части правил кодирования ГОСТ Р ИСО/МЭК 8825-1-2003, используемых при обмене защищенными сообщениями в соответствии со стандартом S/MIME и в сертификатах формата X.509.

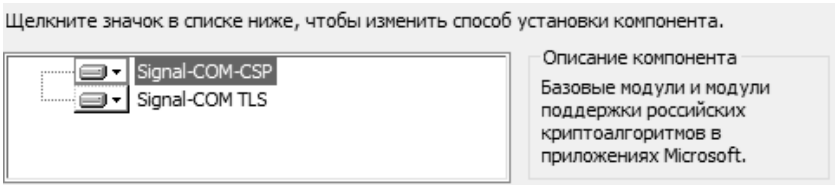

Рис. 6. Выбор модуля «Signal-COM CSP»

В модуле Signal-COM TLS (рис. 7) реализована поддержка российских криптографических алгоритмов в соответствии с рекомендацией IETF «GOST 28147-89 Cipher Suites for Transport Layer Security (TLS)» для совместимости с приложениями, обеспечивающими защиту трафика по протоколу TLS с использованием криптографических решений российских компаний.

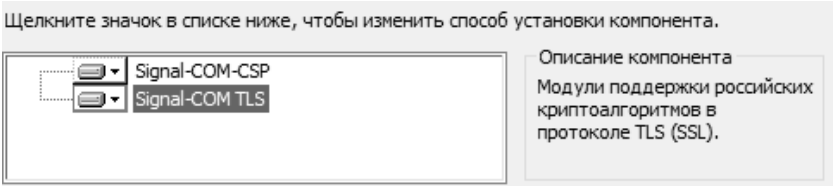

Рис. 7. Выбор модуля «Signal-COM TLS»

Далее от пользователя потребуется инициализировать датчик случайных чисел. Данную процедуру можно выполнить двумя способами: с использованием существующего ключевого контейнера или с помощью специальной процедуры, которая требует нажатий клавиатуры или перемещений курсора мыши (рис. 8).

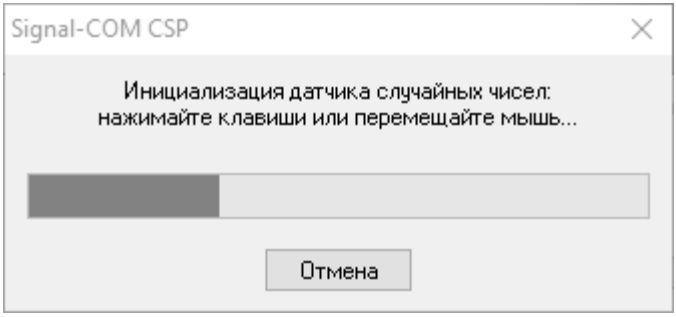

Рис. 8. Сбор энтропии для инициализации датчика случайных чисел

По окончанию установки перезагрузите виртуальную машину.

3.2.3 Применение функций криптопровайдера в приложениях

В меню пуск появились пункты, относящиеся к установленному криптопровайдеру (рис. 9). Запустите приложение «Администратор», чтобы ознакомиться с базовым интерфейсом программы (рис. 10).

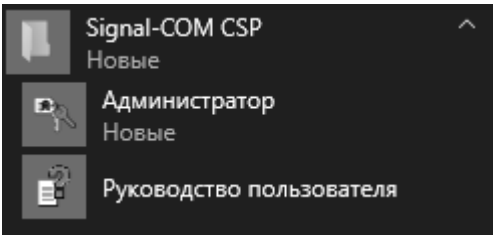

Рис. 9. Папка криптопровайдера в меню «Пуск»

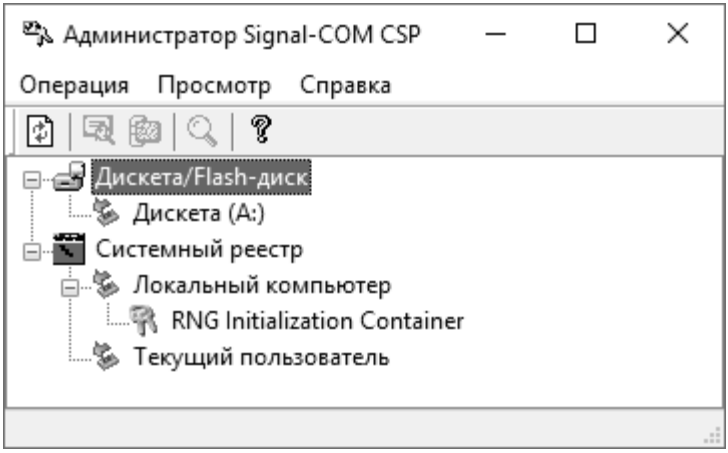

Рис. 10. Окно администратора криптопровайдера «Signal-COM CSP»

В данный момент в данном окне нет элементов, которые могли бы быть интересны для изучения. Чтобы исправить данную ситуацию – необходимо добавить ключевые контейнеры на имеющиеся носители. В данной работе будет рассматриваться использование дискеты.

Перейдем к изучению функций, которые стали доступны после установки данного криптопровайдера. В качестве примера рассмотрим работу центра сертификации. Запустите консоль управления Microsoft и добавьте в нее оснастку «Шаблоны сертификатов». Выделите шаблон «Пользователь» и в контекстном меню выберите операцию «Скопировать шаблон».

Задайте имя шаблона «Сигнал-КОМ» и перейдите во вкладку «Шифрование». В отличие от исходного шаблона здесь можно изменить набор доступных поставщиков криптографических услуг (рис. 11).

Для того, чтобы отобразились необходимые нам поставщики, потребуется изменить значение поля «Минимальный размер ключа», по которому фильтруются отображаемые поставщики.

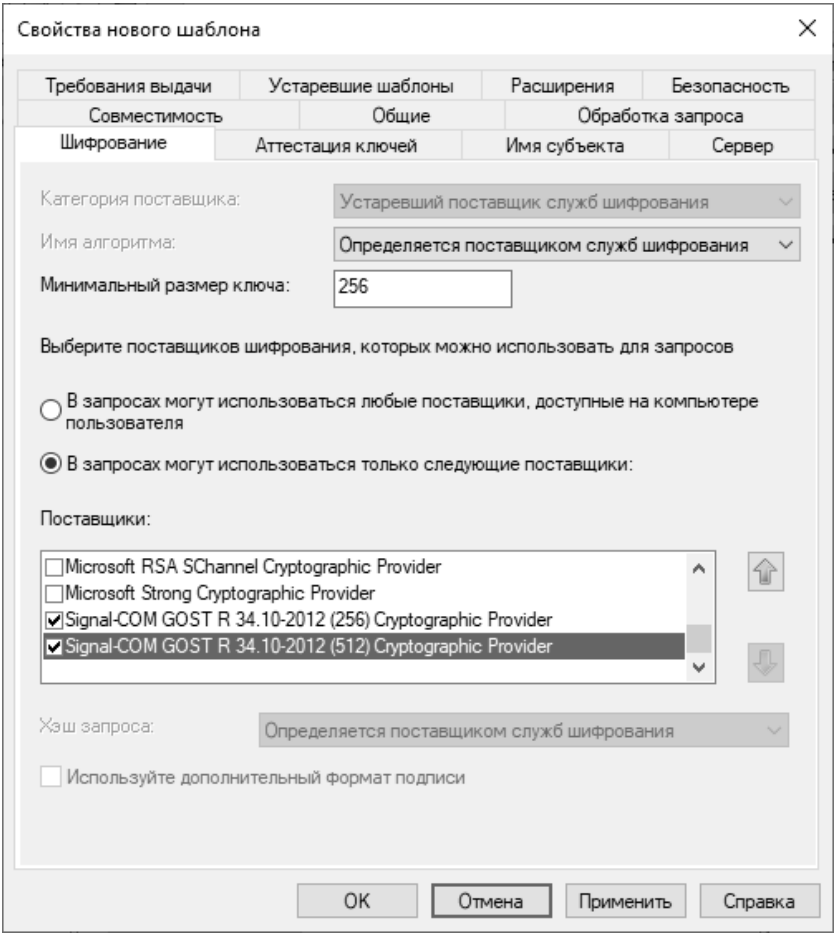

Рис. 11. Вкладка «Шифрование» свойств создаваемого шаблона сертификата

Добавьте оснастку «Центр сертификации» и сделайте доступным к выдаче новый шаблон сертификатов. После проделанных операций откройте в Internet Explorer центр сертификации и выберите расширенный запрос сертификата (рис. 12).

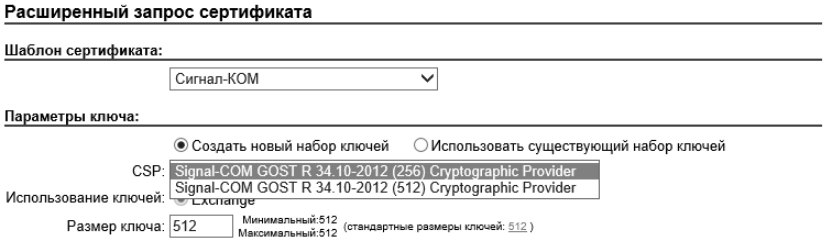

Рис. 12. Выбор криптопровайдера для созданного шаблона сертификатов

Выберите один из вариантов криптопровайдера и выдайте сертификат. Чтобы упростить восприятие создаваемых ключевых контейнеров рекомендуется использовать заданное пользователем имя. В качестве примера (рис. 13) может быть использовано имя NNNN_FIO, соответствующее номеру группы исполнителя (NNNN) и его инициалы на английском языке (FIO).

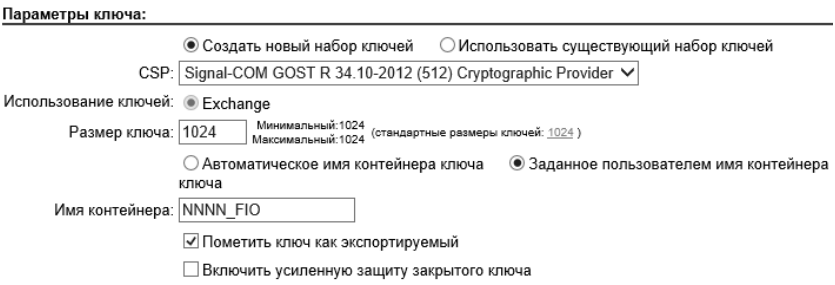

Рис. 12. Параметры ключа выдаваемого сертификата

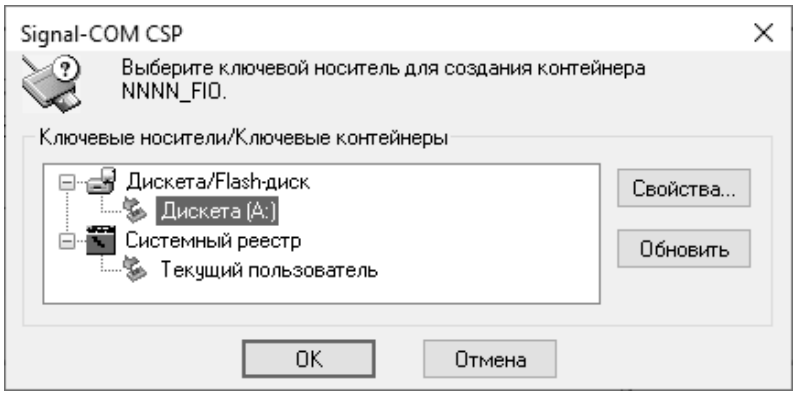

Рис. 13. Выбор ключевого носителя для создания контейнера

После нажатия кнопки «Выдать» появится окно для выбора носителя, на который будет помещен создаваемый контейнер NNNN_FIO (рис. 12). Для примера выберем дискету. Для обеспечения безопасности информации в ключевом контейнере используйте пароль для доступа к нему (рис. 14-15).

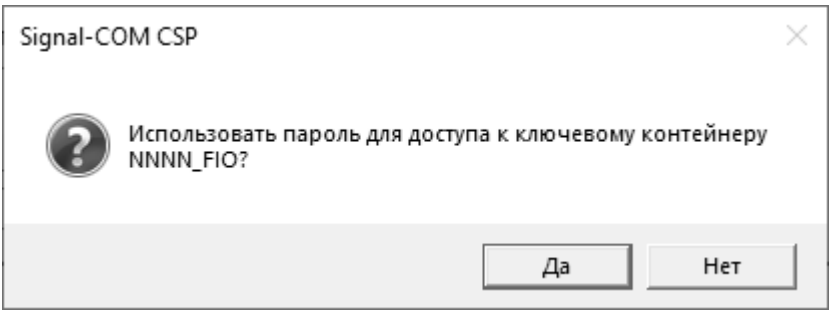

Рис. 14. Согласие с использованием пароля для защиты контейнера

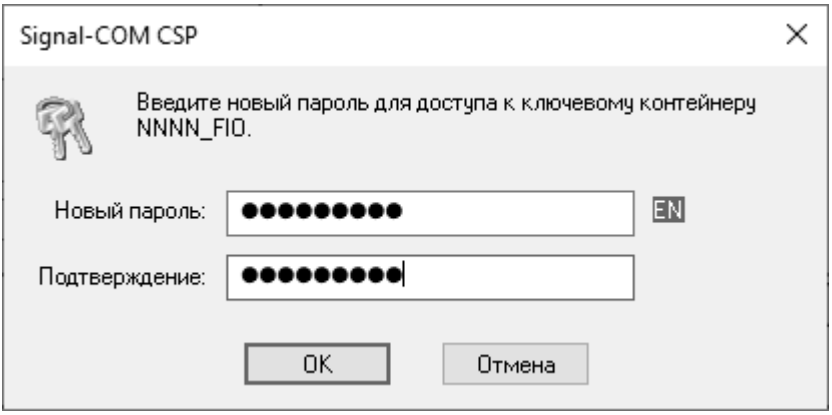

Рис. 15. Ввод пароля для доступа к ключевому контейнеру

После система снова инициализирует датчик случайных чисел. Будет отображено сообщение об успешной выдаче запрошенного сертификата. Теперь можно снова вернуться к окну администратора криптопровайдера (рис. 16).

Как можно заметить, на дискете появился контейнер, который мы запрашивали. Если он не отобразился сразу, то можно обновить отображение с помощью соответствующей кнопки.

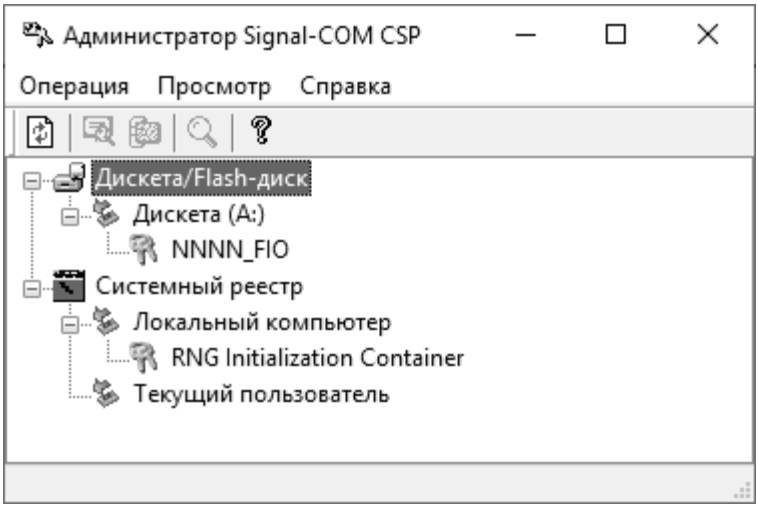

Рис. 16. Наличие ключевого контейнера на дискете

Можете открыть проводник и ознакомиться с содержанием данного контейнера (рис. 17). Очевидно, что использование дискеты или flash-диска не является безопасным с точки зрения обеспечения целостности хранимых на носителе данных. В связи с этим лучше на практике использовать для подобных операций смарт-карты и usb-токенов.

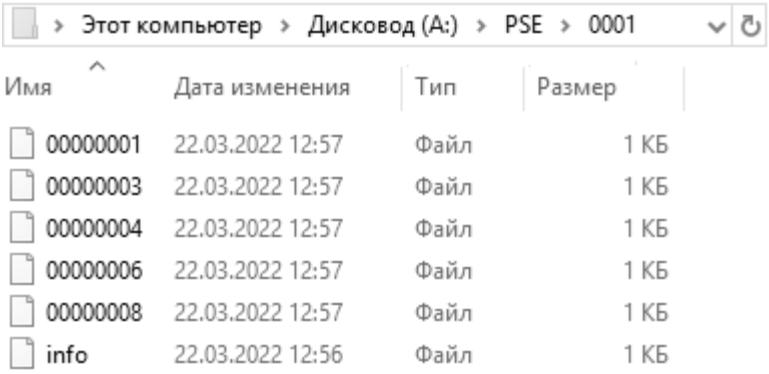

Рис. 17. Просмотр содержимого ключевого контейнера на дискете

Вернитесь к центру сертификации и нажмите на кнопку «Установить сертификат». В результате в контейнере будет создан еще

1 файл. Выделите ключевой контейнер в окне администратора и вызовите команду «Сертификат», а для нее выберите вариант «Просмотр». От Вас потребуется указать пароль для доступа к контейнеру (рис. 18).

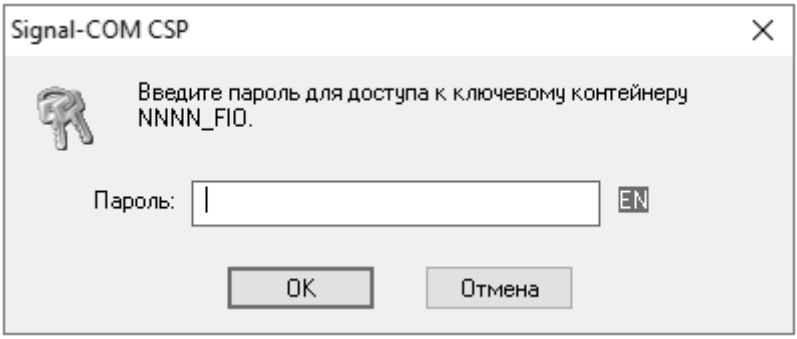

Рис. 18. Запрос пароля для доступа к ключевому контейнеру

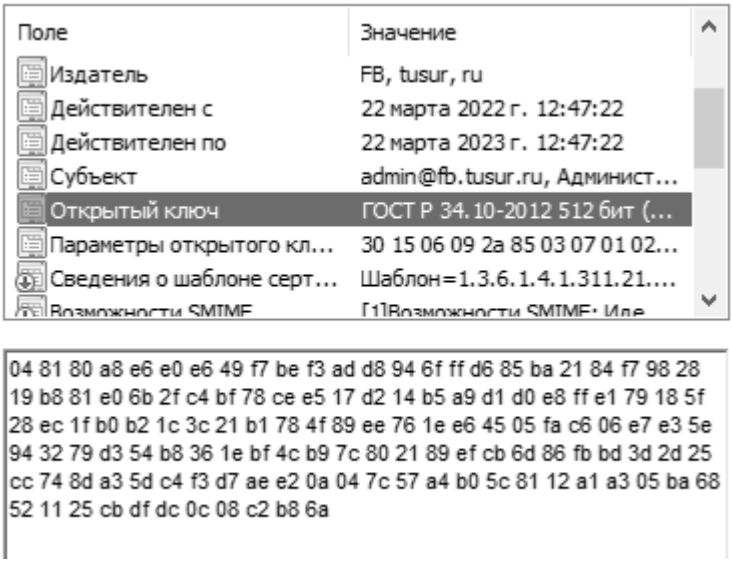

Рис. 19. Сведения об открытом ключе выданного сертификата

В свойствах выданного шаблона просмотрите сведения об открытом ключе (рис. 19).

3.3 Средство криптографической защиты информации «КриптоПро CSP»

3.3.1 Краткие сведения о СКЗИ

КриптоПро CSP —криптопровайдер, включающий в себя возможности работы с:

- классическими токенами и другие пассивными хранилищами секретных ключей;
- неизвлекаемыми ключами на токенах с защищенным обменом сообщениями;
- ключами в облаке.

Главное преимущество заключается в том, что работа со всеми ключевыми носителями, включая ключи в облаке, единообразна. Интерфейс доступа к ним одинаков, и работа с ключом в облаке будет происходить точно таким же образом, как и с классическим ключевым носителем.

Назначение КриптоПро CSP:

- Формирование и проверка электронной подписи.
- Обеспечение конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты.
- Обеспечение аутентичности, конфиденциальности и имитозащиты соединений по протоколам TLS, и IPsec.
- Контроль целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений доверенного функционирования.

В КриптоПро CSP наряду с российскими реализованы зарубежные криптографические алгоритмы:

- Электронная подпись – ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018), ECDSA, RSA;
- Хэш-функции – ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018), SHA-1, SHA-2;
- Шифрование – ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018), ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018), ГОСТ 28147-89, AES (128/192/256), 3DES, 3DES-112, DES, RC2, RC4.

КриптоПро CSP позволяет быстро и безопасно использовать российские криптографические алгоритмы в следующих стандартных приложениях:

- Офисный пакет Microsoft Office;

- Почтовый сервер Microsoft Exchange и клиент Microsoft Outlook;
- Продукты Adobe;
- Браузеры Яндекс.Браузер, Спутник, Internet Explorer, Chromium GOST;
- Средство формирования и проверки подписи приложений Microsoft Authenticode;
- Веб-серверы Microsoft IIS, nginx, Apache;
- Средства удаленных рабочих столов Microsoft Remote Desktop Services;
- Microsoft Active Directory.

3.3.2 Установка и настройка СКЗИ

Восстановите исходное состояние виртуальной машины (до установки криптопровайдера Signal-COM CSP). Далее запустите мастер установки криптопровайдера. Выберите установку по умолчанию (рис. 20). Отличие в дополнительных опциях заключается в выборе уровня безопасности: КС1, КС2 или КС3.

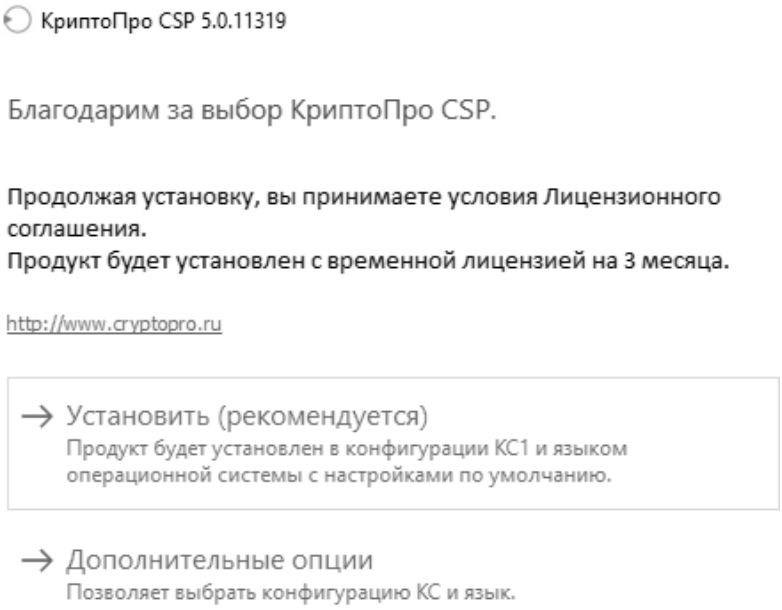

Рис. 20. Запуск установки криптопровайдера

3.3.3 Применение функций криптопровайдера в приложениях

В меню пуск появились пункты, относящиеся к установленному криптопровайдеру (рис. 21). Запустите утилиту «Инструменты КриптоПро» (рис. 22). В данный момент в приложении нет никаких данных, с которыми мы могли бы осуществить какие-то операции.

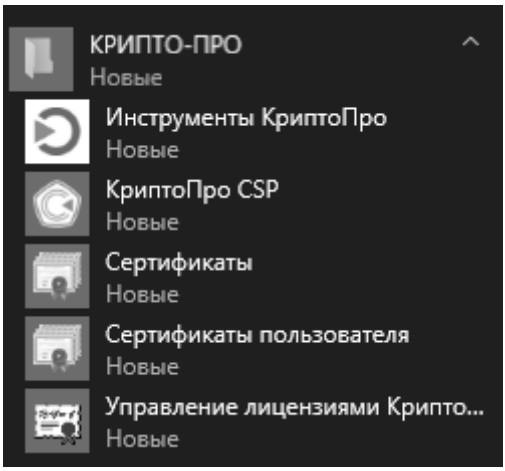

Рис. 21. Папка криптопровайдера в меню «Пуск»

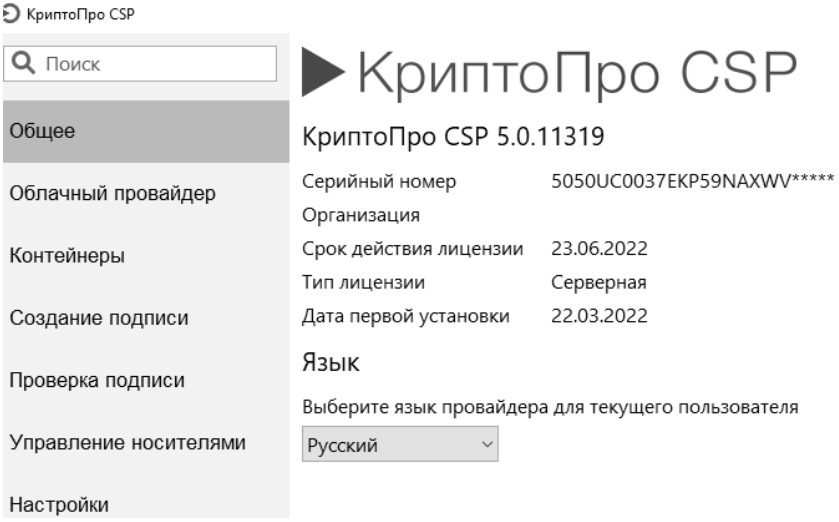

Рис. 22. Инструменты КриптоПро

По аналогии с тем, как мы изучали возможности другого криптопровайдера, создадим новый шаблон для КриптоПро. Единственным отличием от свойств предыдущего шаблона сделайте возможность выбирать любого поставщика шифрования, доступного на компьютере пользователя (рис. 23). Сделайте шаблон доступным для выдачи через оснастку «Центр сертификации».

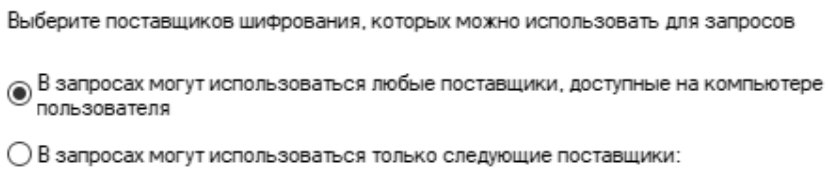

Рис. 23. Выбор поставщика криптографических функций для шаблона

Далее перейдите на страницу центра сертификации и запросите новый сертификат по созданному шаблону (рис. 24). Выберите поставщиком шифрования криптопровайдер от КриптоПро.

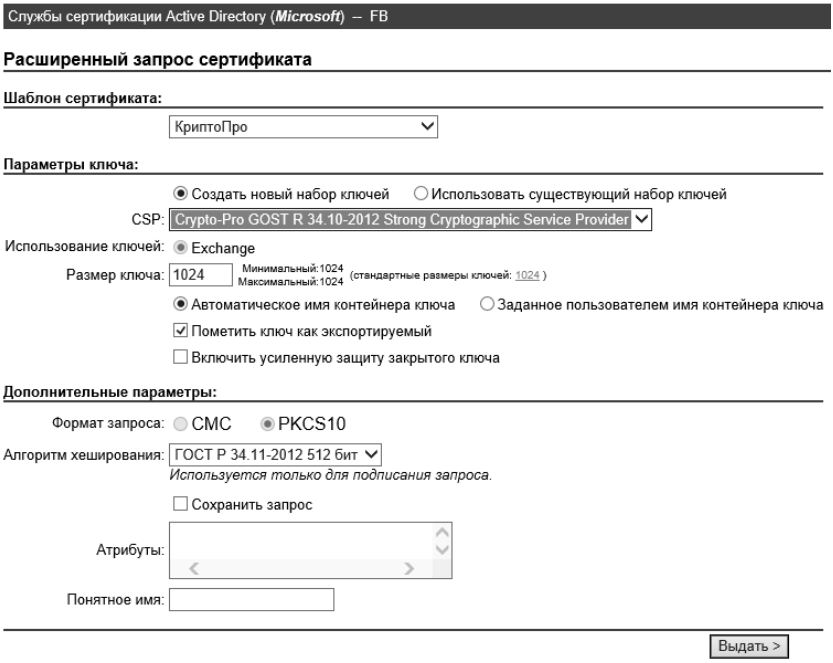

Рис. 24. Запрос сертификата по шаблону с криптопровайдером КриптоПро

Система запросит выбрать ключевой носитель для создаваемого контейнера (рис. 25). В данный момент для Вас доступны только 2 варианта: реестр и директория. Для выбора облачного токена необходимо предварительно настроить доступ к облаку. Установите контейнер в реестр.

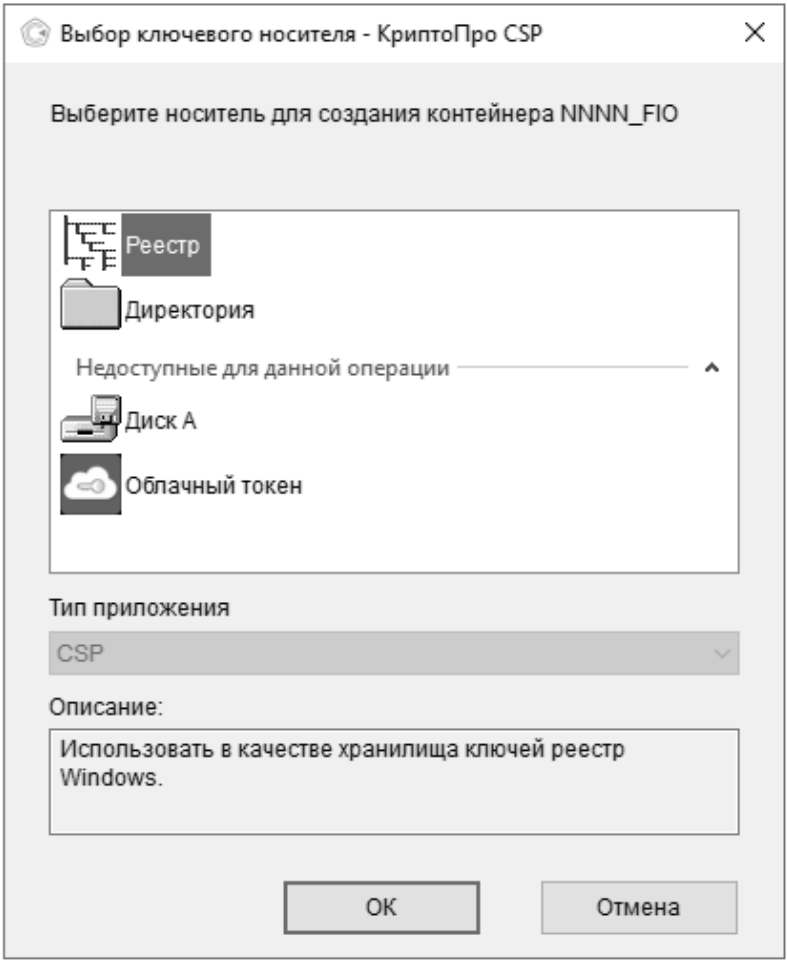

Рис. 25. Выбор носителя для ключевого контейнера

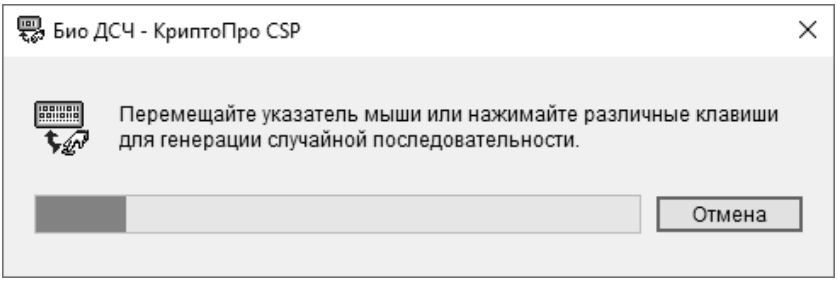

Рис. 26. Генерация случайной последовательности

Следующим шагом система попросить задать пароль для доступа к ключевому контейнеру (рис. 27). После будет выведено сообщение об успешности выполненной операции (рис. 28).

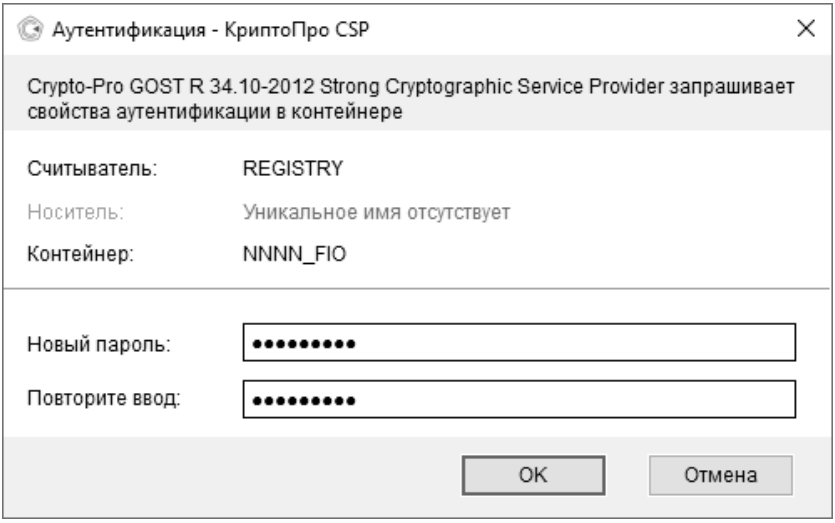

Рис. 27. Создание пароля для доступа к ключевому контейнеру

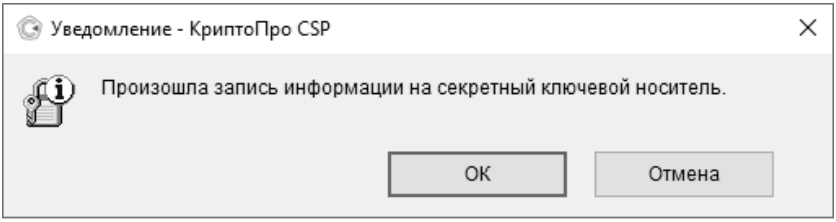

Рис. 28. Уведомление об успешной записи информации в контейнер

Просмотрите полученный сертификат. Убедитесь, что открытый ключ был создан по выбранному Вами алгоритму (рис. 29).

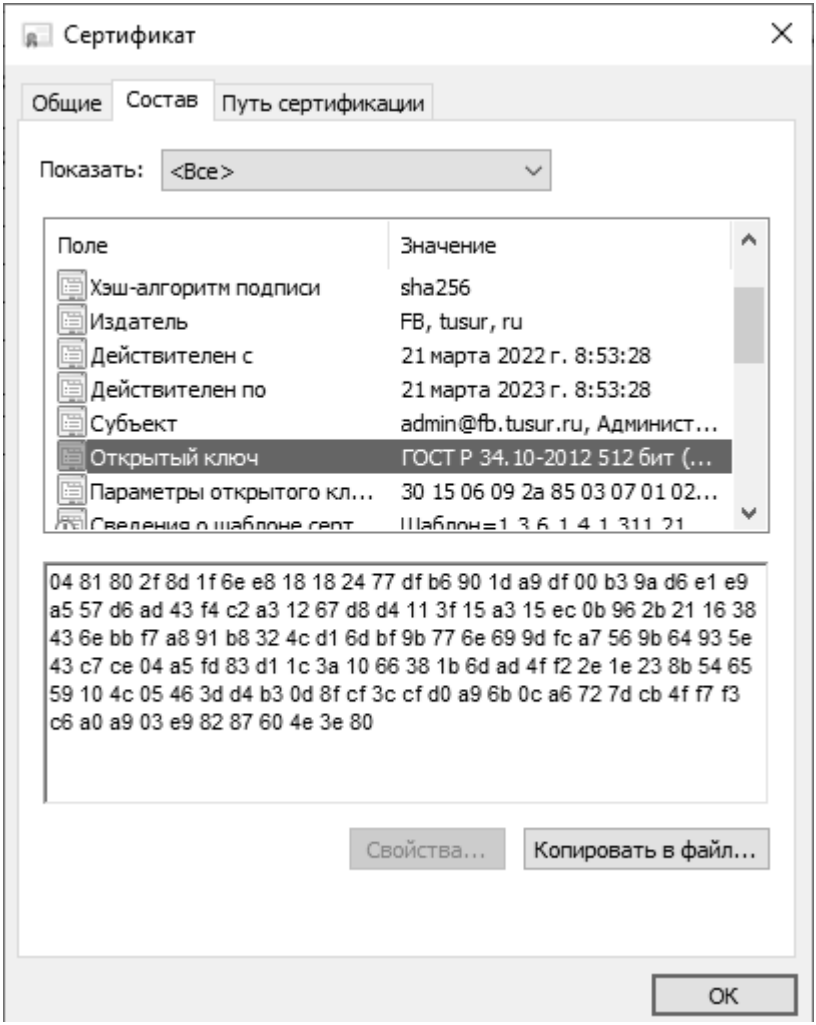

Рис. 29. Сведения об открытом ключе выданного сертификата

Вернемся к приложению «Инструменты КриптоПро». Теперь во вкладке «Контейнеры» можно увидеть только что созданный нами ключевой контейнер (рис. 30).

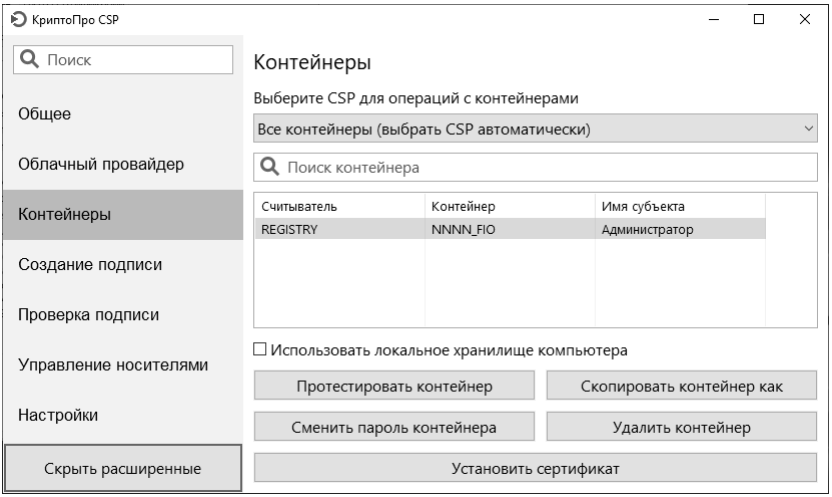

Рис. 30. Ключевой контейнер в приложении

Выделите созданный контейнер и нажмите на кнопку «Протестировать контейнер». После ввода правильного пароля от контейнера отобразится окно с результатом тестирования (рис. 31). Ознакомьтесь со сведениями, представленными отчетом о проверке.

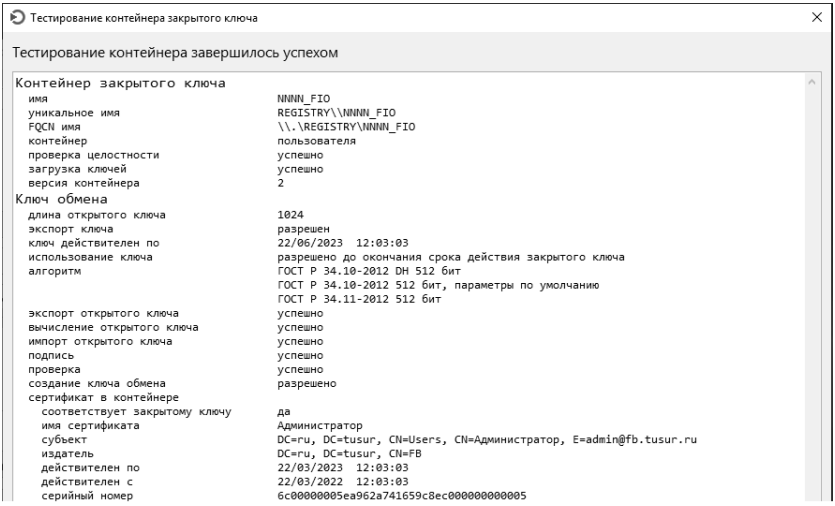

Рис. 31. Фрагмент результата тестирования ключевого контейнера

Перейдите в раздел «Создание подписи». Создайте текстовый документ произвольного содержания и выберите его для подписи в данном окне (рис. 32).

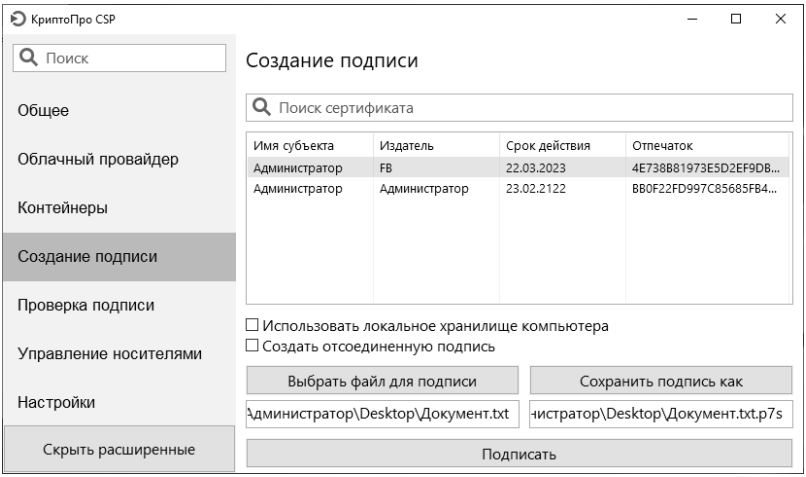

Рис. 32. Подпись документа с помощью сертификата

После нажатия кнопки «Подписать» потребуется вновь ввести пароль для доступа к ключевому контейнеру, соответствующему выбранному сертификату (рис. 33).

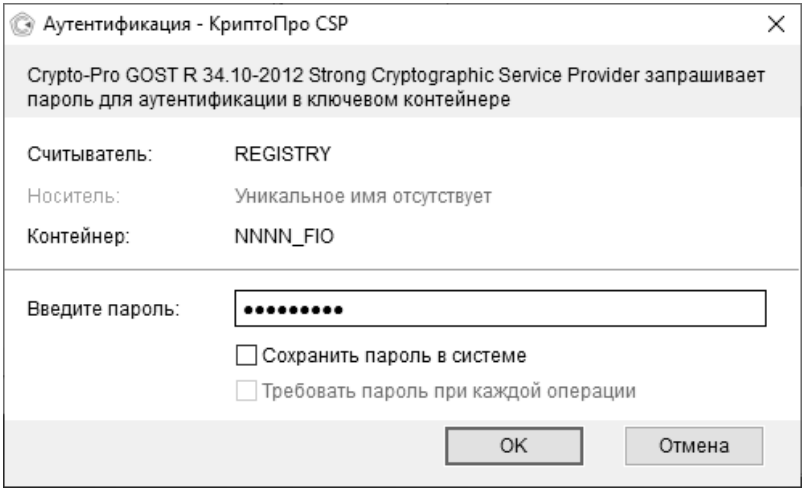

Рис. 33. Аутентификация в ключевой контейнер

Об успешности выполненной операции будет уведомлено соответствующим сообщением под кнопкой «Подписать» (рис. 34) .

Рис. 34. Сообщение об успешности процедуры подписи

Проверить подпись можно в соседнем разделе (рис. 35). Выберите полученную только что подпись и нажмите на кнопку «Проверить подпись».

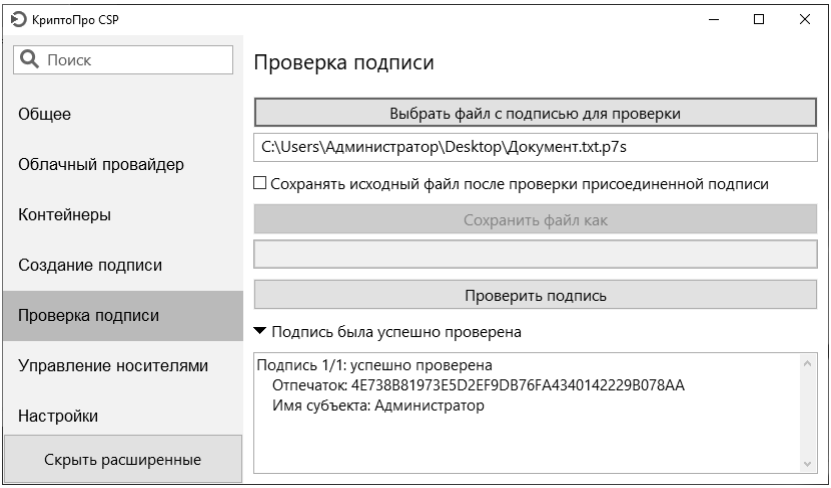

Рис. 35. Проверка подписи на выбранном файле

Отзовите данный сертификат и проверьте подпись на документе снова. Система должна сообщить о том, что сертификат был отозван и доверять данной подписи нельзя (рис. 36).

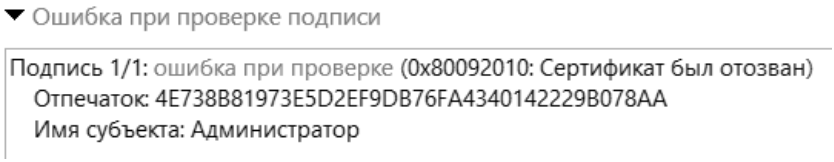

Рис. 36. Сообщение об ошибке проверки подписи, вызванной отзывом сертификата

4. Задание на лабораторную работу

1. Ознакомиться с теорией (включая лекционные материалы).
2. Установить и настроить криптопровайдер Signal-COM CSP.
3. Создать шаблон сертификата, использующий установленный криптопровайдер, и выдать на его основе сертификат.
4. Установить и настроить криптопровайдер КриптоПро CSP.
5. Создать шаблон сертификата, использующий установленный криптопровайдер, и выдать на его основе сертификат.
6. Подписать файл с использованием созданного сертификата.
7. Отозвать сертификат и проверить подписанный с его помощью файл.
8. Составить по проделанной работе отчет.

5. Контрольные вопросы

1. Что такое криптопровайдер?
2. Что такое CryptoAPI?
3. Какие задачи выполняет CryptoAPI?
4. Какие функции обеспечивают криптопровайдеры?
5. В каком формате криптопровайдеры хранятся на компьютере?
6. Что такое ключевой контейнер?
7. Почему не рекомендуется устанавливать несколько криптопровайдеров на одном устройстве?
8. Какие виды носителей могут быть использованы для хранения ключевого контейнера в СКЗИ Signal-COM CSP?
9. Какие виды носителей могут быть использованы для хранения ключевого контейнера в СКЗИ КриптоПро CSP?
10. Зачем необходим сбор энтропии при инициализации работы датчика случайных чисел?