МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

федеральное государственное автономное образовательное учреждение высшего образования

«Санкт–Петербургский государственный университет  
аэрокосмического приборостроения»

ФАКУЛЬТЕТ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

ОТЧЕТ   
ЗАЩИЩЕН С ОЦЕНКОЙ

РУКОВОДИТЕЛЬ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| преподаватель |  |  |  | И. В. Козлов |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |

|  |
| --- |
| ОТЧЕТ ПО ЛАБОРАТОРНЫМ РАБОТАМ  по дисциплине МДК 02.02. Программное обеспечение компьютерных сетей |
|  |
|  |
|  |
|  |

РАБОТУ ВЫПОЛНИЛИ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТЫ ГР. № | С342 |  |  |  | Б. И. Глаголевский,  Е. Ю. Барабаш |
|  |  |  | подпись, дата |  | инициалы, фамилия |

# ОГЛАВЛЕНИЕ

[ОГЛАВЛЕНИЕ 2](#_Toc189302337)

[Защита учетной записи. 3](#_Toc189302338)

[Результат работы 32](#_Toc189302339)

[Шифрование BitLocker 33](#_Toc189302340)

[Включение TPM в Hyper-V manager 35](#_Toc189302341)

[Отсоединение образа от машины 38](#_Toc189302342)

[Включение групповой политики для BitLocker 40](#_Toc189302343)

[Включение BitLocker 41](#_Toc189302344)

[Шифрование папки 52](#_Toc189302345)

# Защита учетной записи.

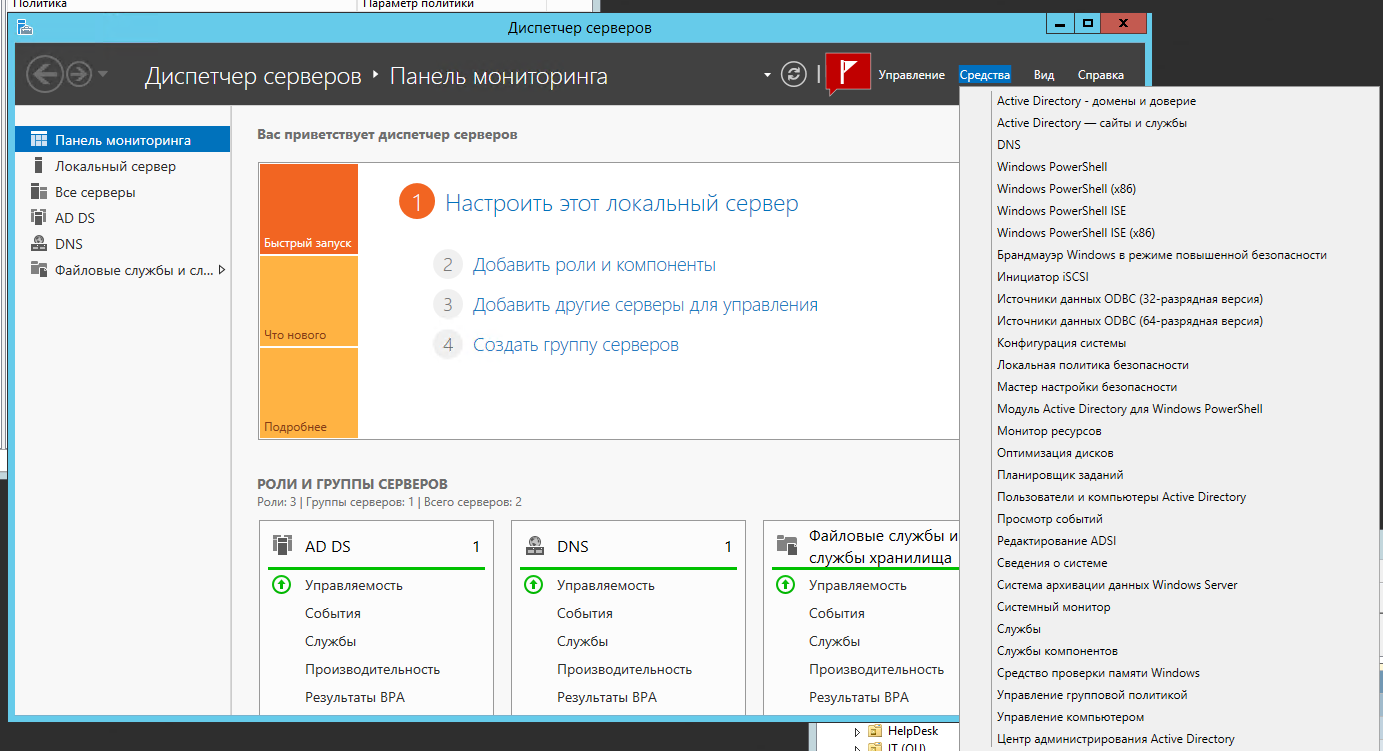


Рисунок 1. Как открыть “Управление групповой политикой” на Windows Server 2012.

Групповая политика позволяет управлять параметрами пользователя и компьютера на компьютерах под управлением операционных систем Windows Server и Windows Client. Помимо использования групповой политики для определения конфигураций для групп пользователей и клиентских компьютеров, можно также использовать групповую политику для управления серверами, настраивая множество параметров операционной и безопасности для конкретного сервера.

На “Рисунке 1” можно увидеть, как открыть данную службу.

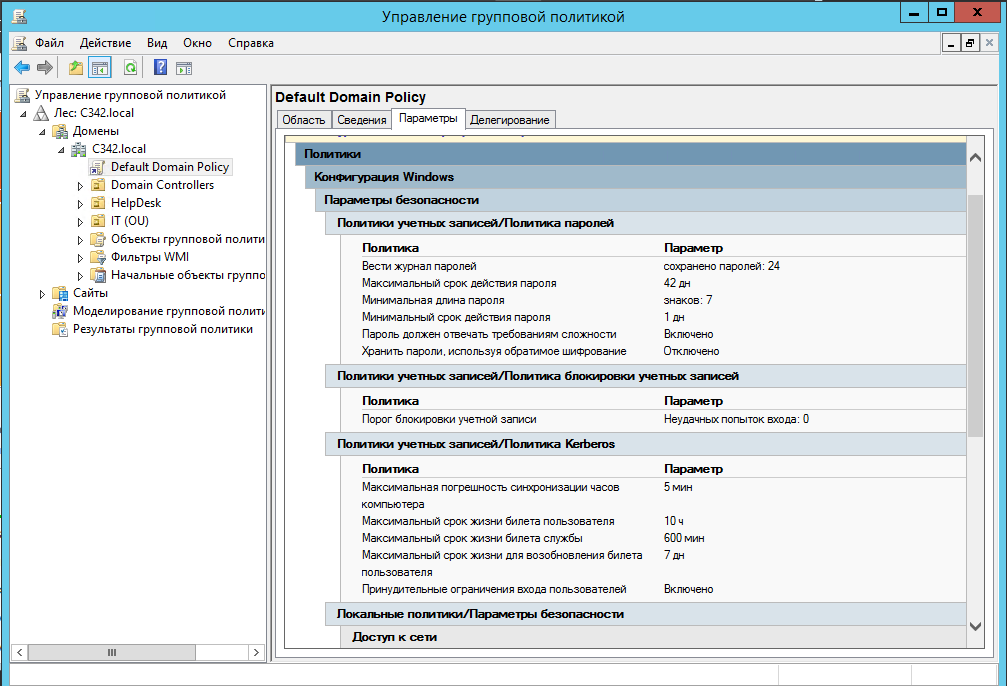


Рисунок 2 – Управление групповой политикой

На данном этапе необходимо перейти в “Default Domain Policy” по адресу “Управление групповой политикой” \” Лес C342.local” \” Домены” \” C342.local” \” Default Domain Policy”.

Это нужно, чтобы впоследствии перейти в “Редактор управления групповыми политиками”. Нажмите “Политики учетных записей/Политика паролей” правой кнопкой мыши.

**Политика паролей** — это набор правил, направленных на повышение безопасности компьютера путём поощрения пользователей к использованию надёжных паролей и их правильному использованию.

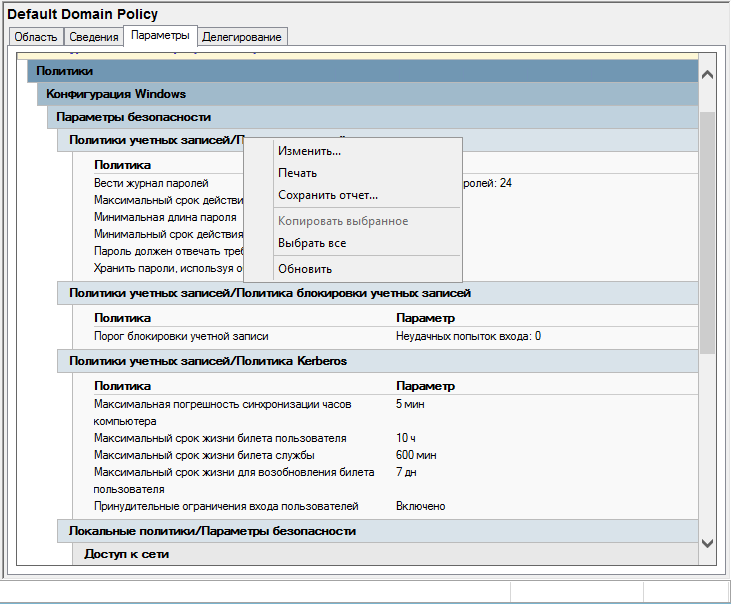


Рисунок 3 -Вход в редактор управления групповыми политиками

На этом этапе необходимо нажать кнопку “Изменить”.

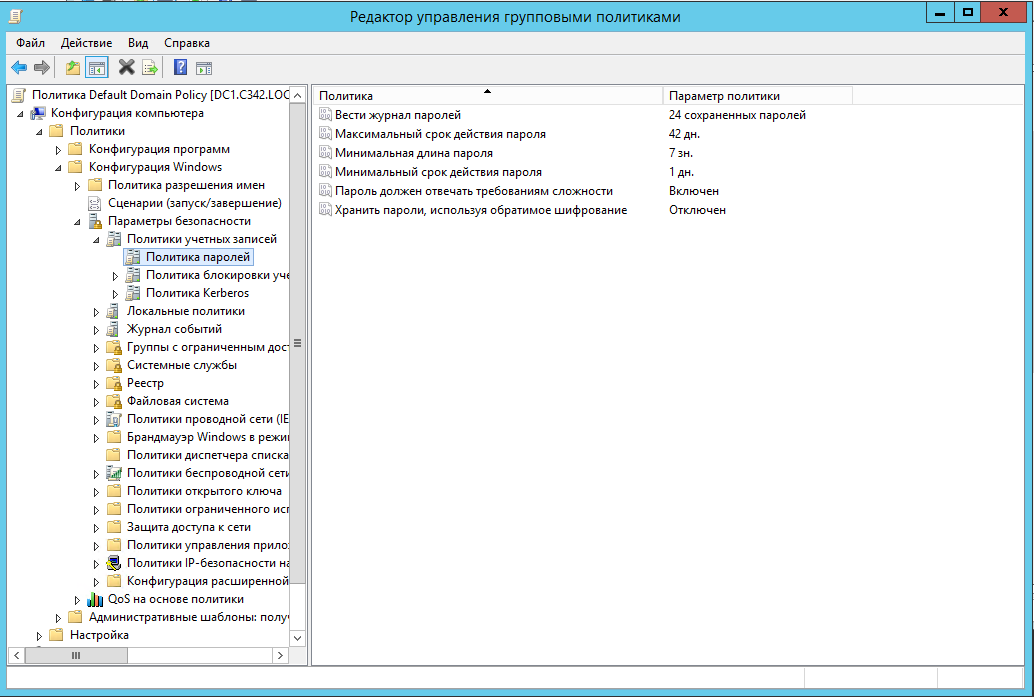


Рисунок 4 – Редактор управления групповыми политиками

На “Рисунок 4” показан путь к политике паролей домена, а также можно заметить, что политика паролей имеет следующие поля: вести журнал паролей, максимальный срок действия пароля, минимальная длина пароля, минимальный срок действия пароля, пароль должен отвечать требованиям сложности, хранить пароли, используя обратное шифрование.

Путь к политике паролей имеет следующий путь.

“Конфигурация компьютера” -> “Политики” -> “Конфигурация Windows” -> “Параметры безопасности” -> “Политики учетных записей” -> “Политики паролей”.

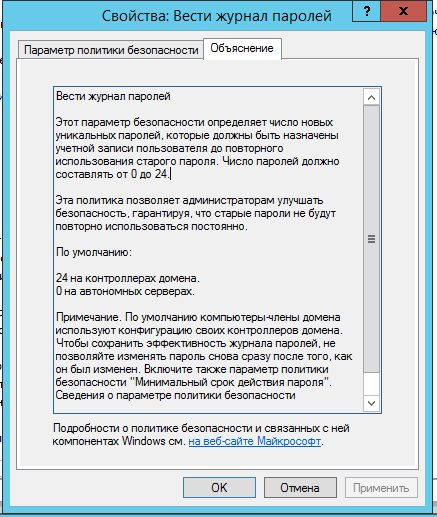


Рисунок 5 – Свойства политики “Вести журнал паролей”

На “Рисунок 5” показана справка по политике “Вести журнал паролей”. На этом окне написано, что этот параметр безопасности определяет число новых уникальных паролей, которые должны быть назначены учетной записи пользователя до повторного использования старого пароля. Число паролей должно составлять от 0 до 24. На данном этапе необходимо перейти по вкладку “Параметр политики безопасности”.

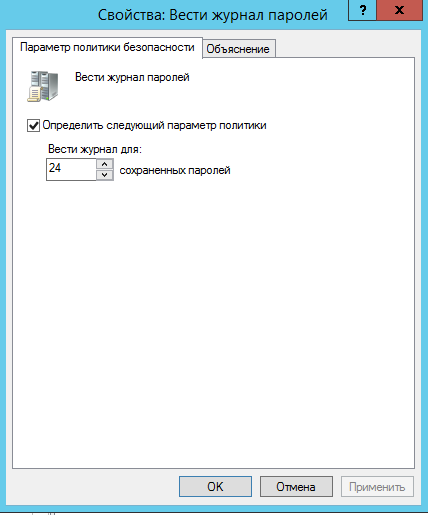


Рисунок 6 – Изменение параметра политики безопасности

На данном этапе нужно изменить 24 на 12.

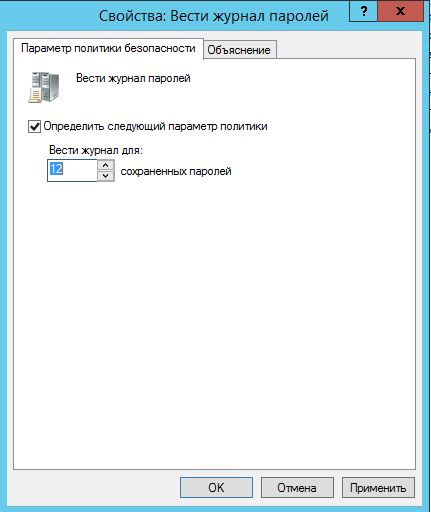


Рисунок 7 – Изменение числа сохраненных паролей

На данном этапе необходимо нажать кнопку “ОК”.

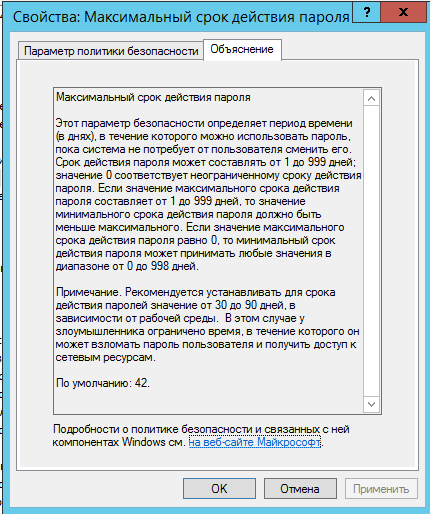


Рисунок 8 – Параметр “Максимальный срок действия пароля”

На “Рисунок 8” можно, вычитав из справочной информации, понять, что этот параметр безопасности определяет период времени в днях, в течение которого можно использовать пароль. 0 – это неограниченный срок действия, а также существует интервал от 1 до 999 дней. Рекомендуется устанавливать срок от 30 до 90 дней.

Далее необходимо нажать на вкладку “Параметр политики безопасности”

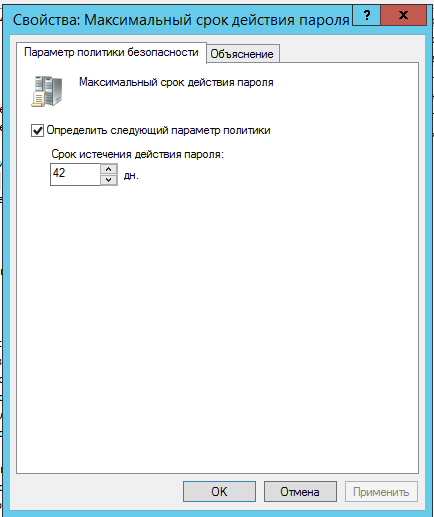


Рисунок 9 – Изменение параметра безопасности

На данном этапе необходимо изменить поле “Срок истечения действия пароля” и нажать “Применить”, а потом нажать “ОК”.

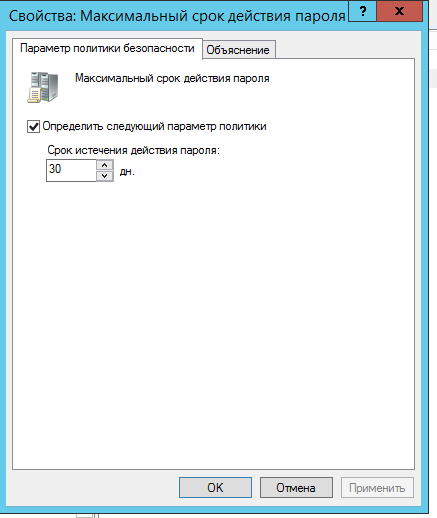


Рисунок 9.1 – Применение параметра

На данном этапе необходимо нажать кнопку “ОК”

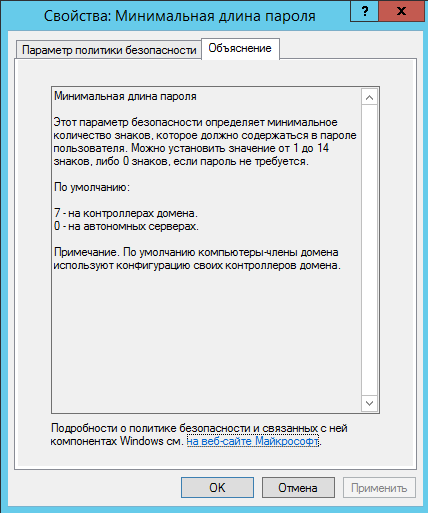


Рисунок 10 – параметр “Минимальная длина пароля”

На “Рисунок 10” можно увидеть справочную информацию по параметру “Минимальная длина пароля”. Этот параметр безопасности определяет минимальное количество знаков, которые должно содержаться в пароле пользователя. Можно устанавливать от 1 до 14 знаков, либо 0 знаков, если пароль **не требуется**.

Далее необходимо нажать на вкладку “Параметр политики безопасности”.

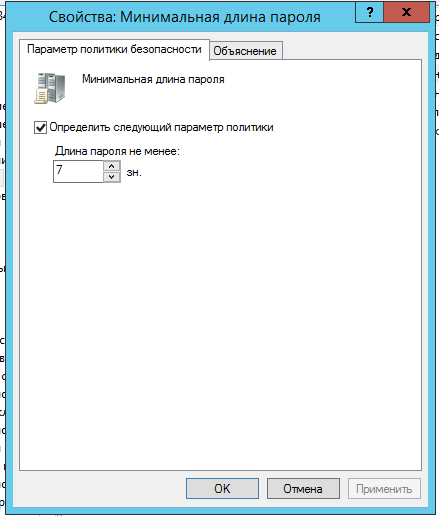


Рисунок 11 – Изменение параметра безопасности

На данном этапе нужно изменить длину пароля с 7 на 5, далее нажать на кнопку “Применить”, а в конце нажать на кнопку “ОК”.

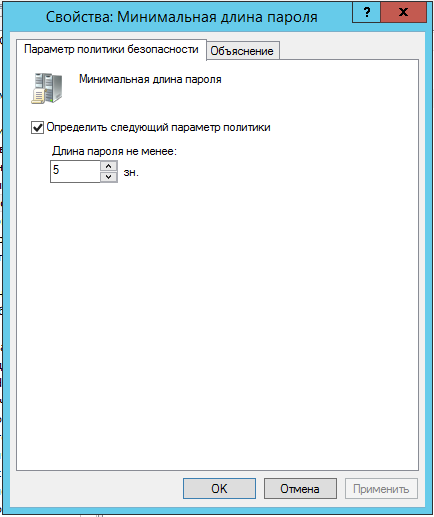


Рисунок 11.1 – применение параметра

На данном этапе необходимо нажать на кнопку “ОК”.



Рисунок 12 – Параметр безопасности “Минимальный срок действия пароля”

На “Рисунок 12” можно наблюдать справочную информацию по параметру безопасности “Минимальный срок действия пароля”. В этой справочной информации написано, что это параметр безопасности определяет период времени, в течение которого необходимо использовать пароль, прежде чем пользователь сможет его **изменить.** Можно установить значение от 1 до 998, либо разрешить изменять пароль сразу, установив значение 0 дней.

Далее необходимо нажать на вкладку “Параметр политики безопасности”.

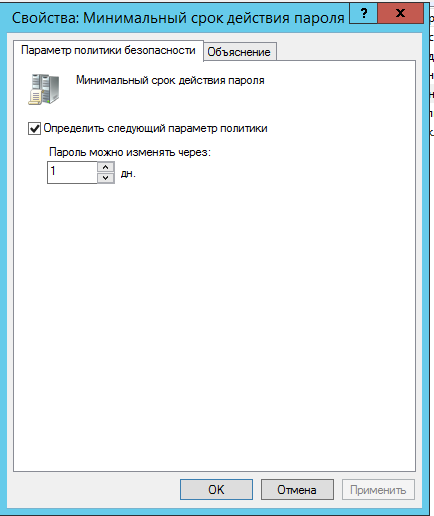


Рисунок 13 – Изменение параметра безопасности

На данном этапе необходимо изменить значение в поле “Пароль можно изменять через” с 1 на 2, затем нажать применить, а далее нажать “ОК”.



Рисунок 13.1 – Применение параметра

На данном этапе необходимо нажать на кнопку “ОК”

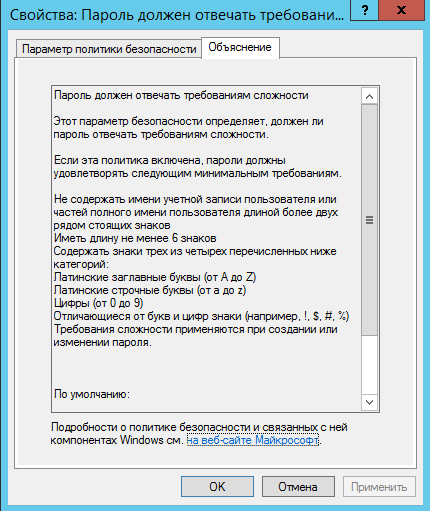


Рисунок 14 – параметр безопасности “Пароль должен отвечать требованиям сложности”

На “Рисунок 14” можно видеть справочную информацию по параметру безопасности “Пароль должен отвечать требованиям сложности”, в ней написано, что параметр определяет, должен ли пароль отвечать требованиям сложности. Если эта политика включена, пароли должны удовлетворить следующими минимальными требованиями: не содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков; иметь длину не более 6 знаков; содержать знаки трех из четырех перечисленных ниже категорий; Латинские буквы заглавные и строчные; цифры; специальные знаки.

Далее необходимо нажать на вкладку “Параметр политики безопасности”.

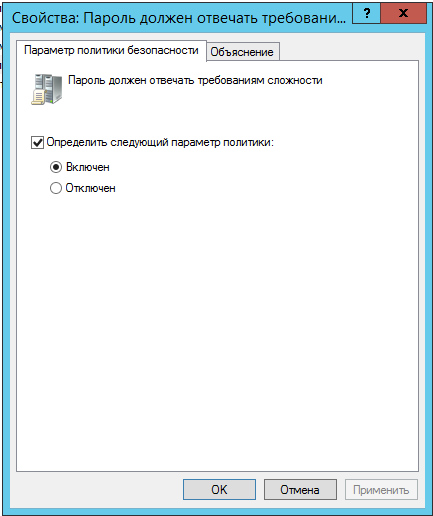


Рисунок 15 - Изменение параметра безопасности

На данном этапе можно отключить параметр безопасности, нажав на соответствующий флаг, затем необходимо нажать “Применить”, а потом нажать кнопку “ОК”.

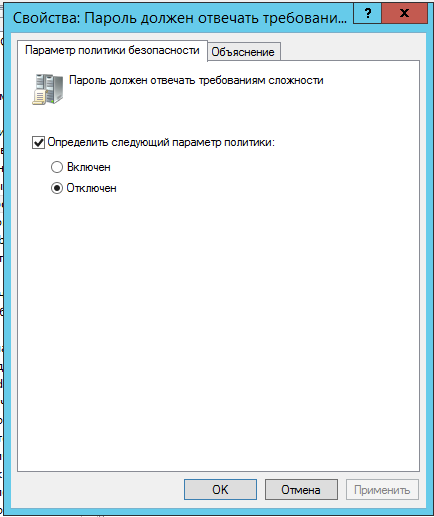


Рисунок 15.1 – Применение параметра

На данном этапе необходимо нажать на кнопку “ОК”

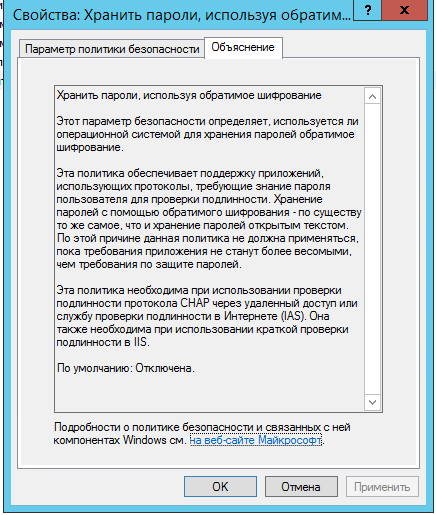


Рисунок 16 – параметр безопасности “Хранить пароли, используя обратимое шифрование”

На “Рисунок 16” можно наблюдать справочную информацию по параметру безопасности “Хранить пароли, используя обратимое шифрование”. В ней написано, что этот параметр безопасности определяет, используется ли операционной системой для хранения паролей обратимое шифрование.

Далее необходимо нажать на вкладку “Параметр политики безопасности”.

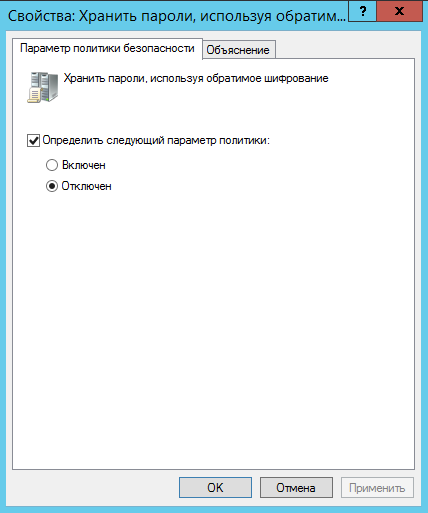


Рисунок 17 – Изменение параметра безопасности

На данном этапе необходимо выбрать флаг “Включен”, нажать кнопку “Приметь”, а далее нажать кнопку “ОК”.

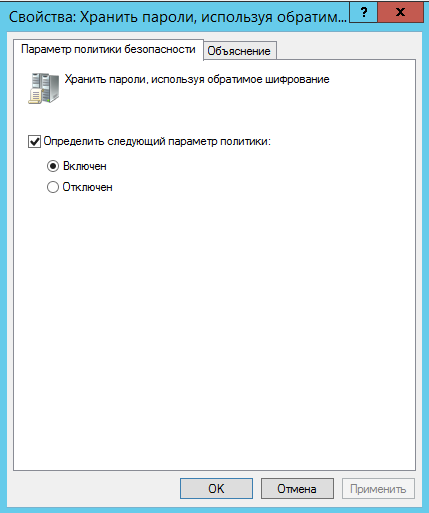


Рисунок 17.1 – Применение параметра

На данном этапе необходимо нажать кнопку “ОК”.

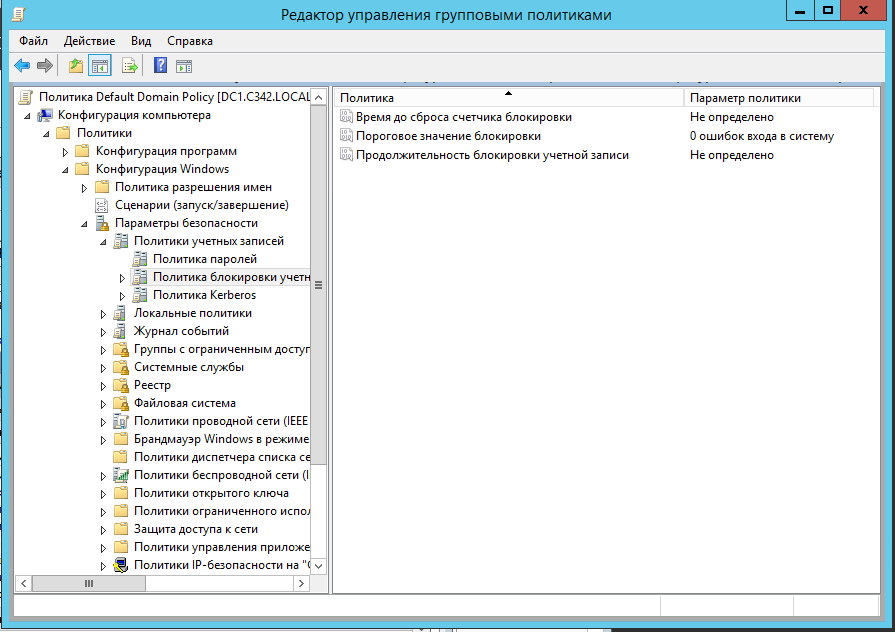


Рисунок 18 – Политика блокировки учетной записи

На данном этапе нужно перейти из “Политики паролей” в “Политику блокировки учетной записи”. В этой политике можно изменять пороговое значений неправильный попыток до блокировки учетной записи, а также продолжительность этой блокировки.

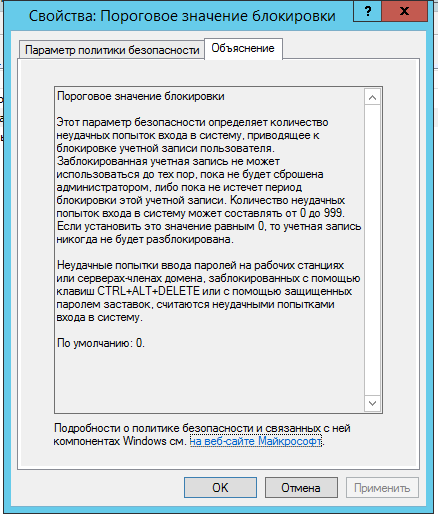


Рисунок 19 – параметр безопасности “Пороговое значение блокировки”

На “Рисунок 19” можно наблюдать справочную информацию о параметре безопасности “Пороговое значение блокировки”. Он определяет количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя. Заблокированная учетная запись не может использоваться до тех пор, пока не будет сброшена администратором, либо пока не истечет период блокировки учетной записи.

Далее необходимо перейти во вкладку “Параметр политики безопасности”.

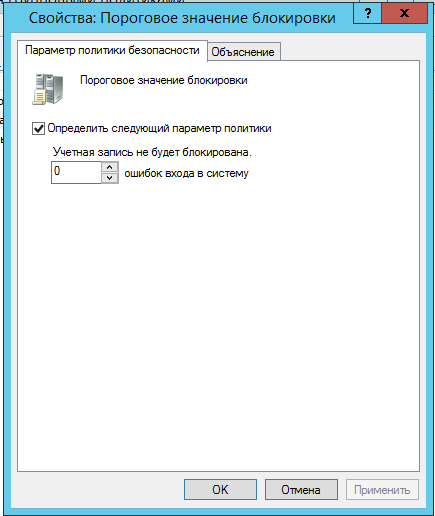


Рисунок 20 – изменение параметра безопасности

В поле “ошибок входа в систему” нужно установить 3, а затем нажать на кнопку “Применить”.

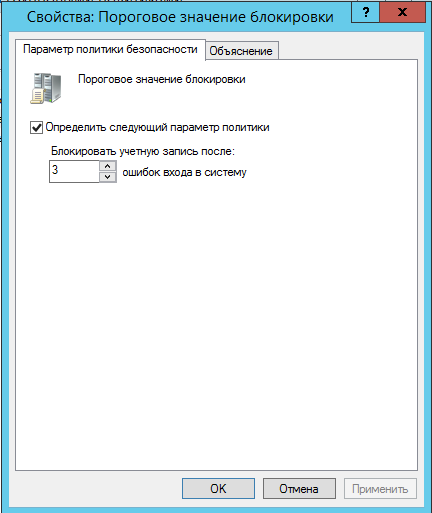


Рисунок 20.1 – Применение изменений

На данном этапе нужно нажать кнопку “ОК”.

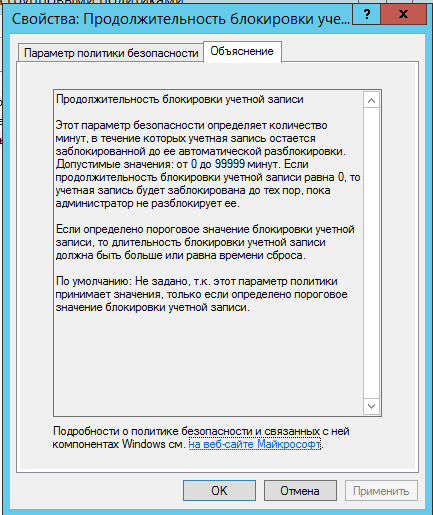


Рисунок 21 – параметр безопасности “Продолжительность блокировки учетной записи”.

На “Рисунок 21” можно наблюдать справочную информацию о параметре безопасности “Продолжительность блокировки учетной записи”. Этот параметр определяет количество минут, в течение которых учетная запись остается заблокированной до ее автоматической разблокировки. Значение от 0 до 99999 минут.

Далее необходимо перейти во вкладку “Параметр политики безопасности”.

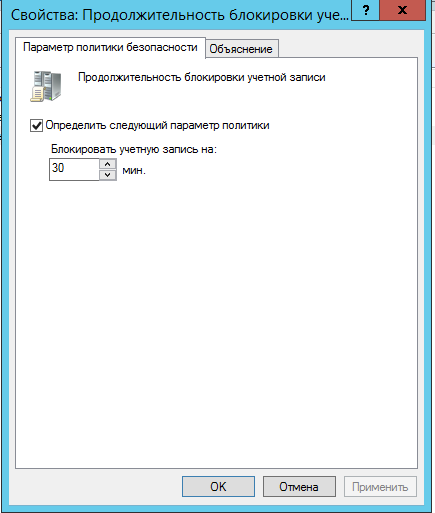


Рисунок 22 – Изменение параметра безопасности

На данном этапе необходимо изменить значение в поле “Блокировать учетную запись на” на 5 минут, а зачем нажать кнопку “Приметь”.

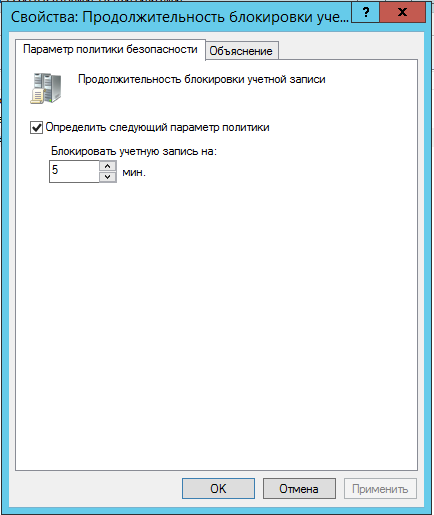


Рисунок 22.1 – Применение параметров

На данном этапе нужно нажать кнопку “ОК”.

# Результат работы

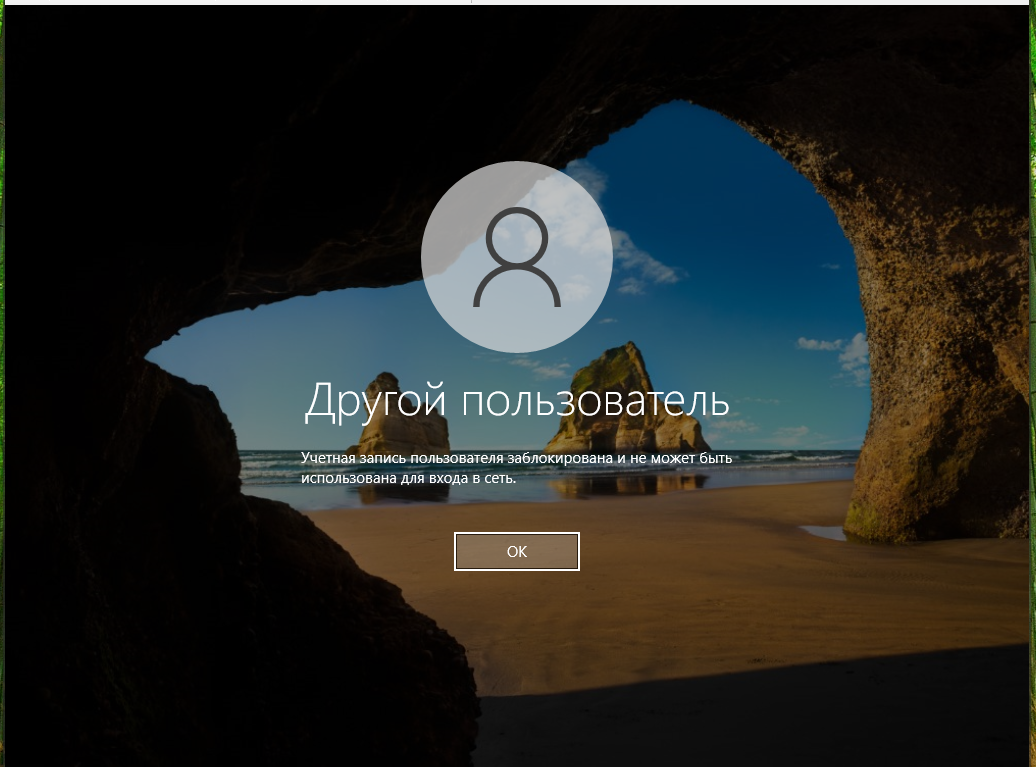


Рисунок 23 – учетная запись заблокирована

После ввода 3 попыток во вход в учетную запись AD заблокировал учетную запись на 5 минут. Для этого был создан новый пользователь в AD.

# Шифрование BitLocker

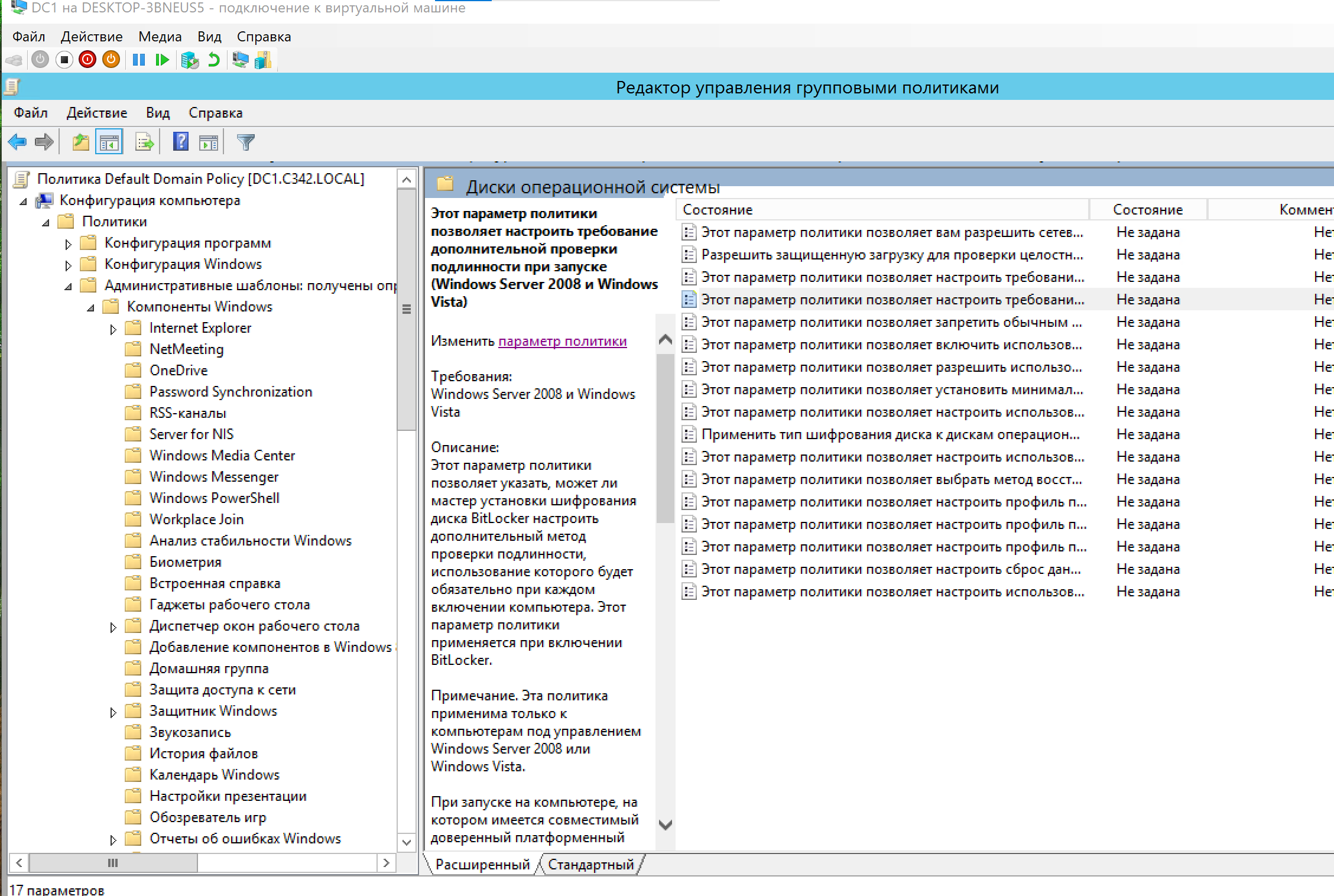


Рисунок 24 – изменение политики для BitLocker

На данном этапе необходимо перейти в редактор управления групповыми политиками и перейти по пути

“конфигурация компьютера” \”Политики”\”Административные шаблоны получены определения политик”\”Компоненты Windows”, а далее необходимо прокрутить вниз.

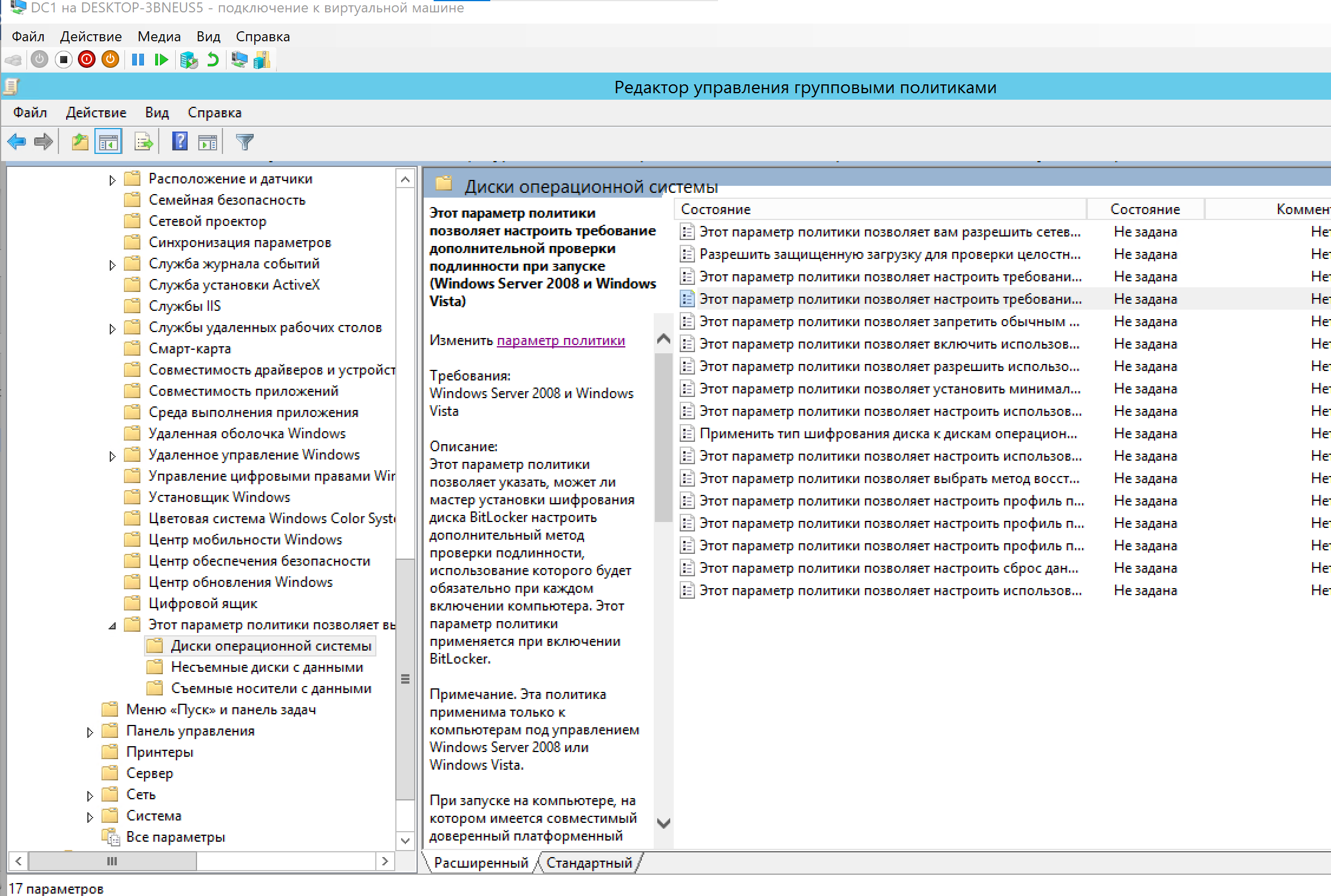


Рисунок 24.1 - изменение политики для BitLocker

На данном этапе необходимо перейти по пути “Этот параметр политики позволяет выбрать шифрование диска BitLocker” \” Диски операционной системы”, а далее выбрать политику “Этот параметр политики позволяет настроить требование дополнительной проверки подлинности при запуске”

## Включение TPM в Hyper-V manager

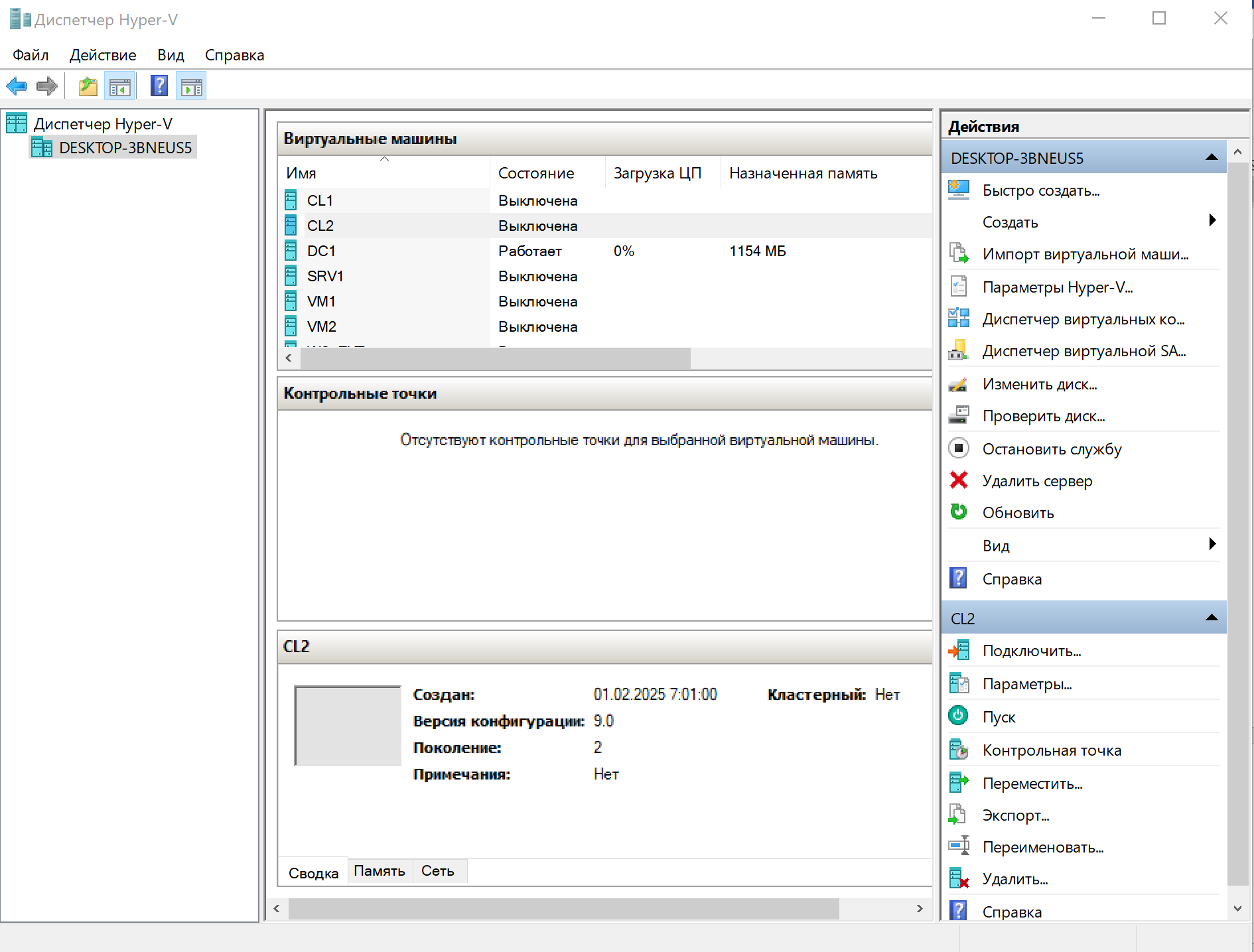


Рисунок 25 – Диспетчер Hyper-V

На данном этапе необходимо включить модуль TPM в настройках безопасности клиентской машины. Чтобы это сделать, необходимо выбрать клиентскую машину, а затем нажать параметры.

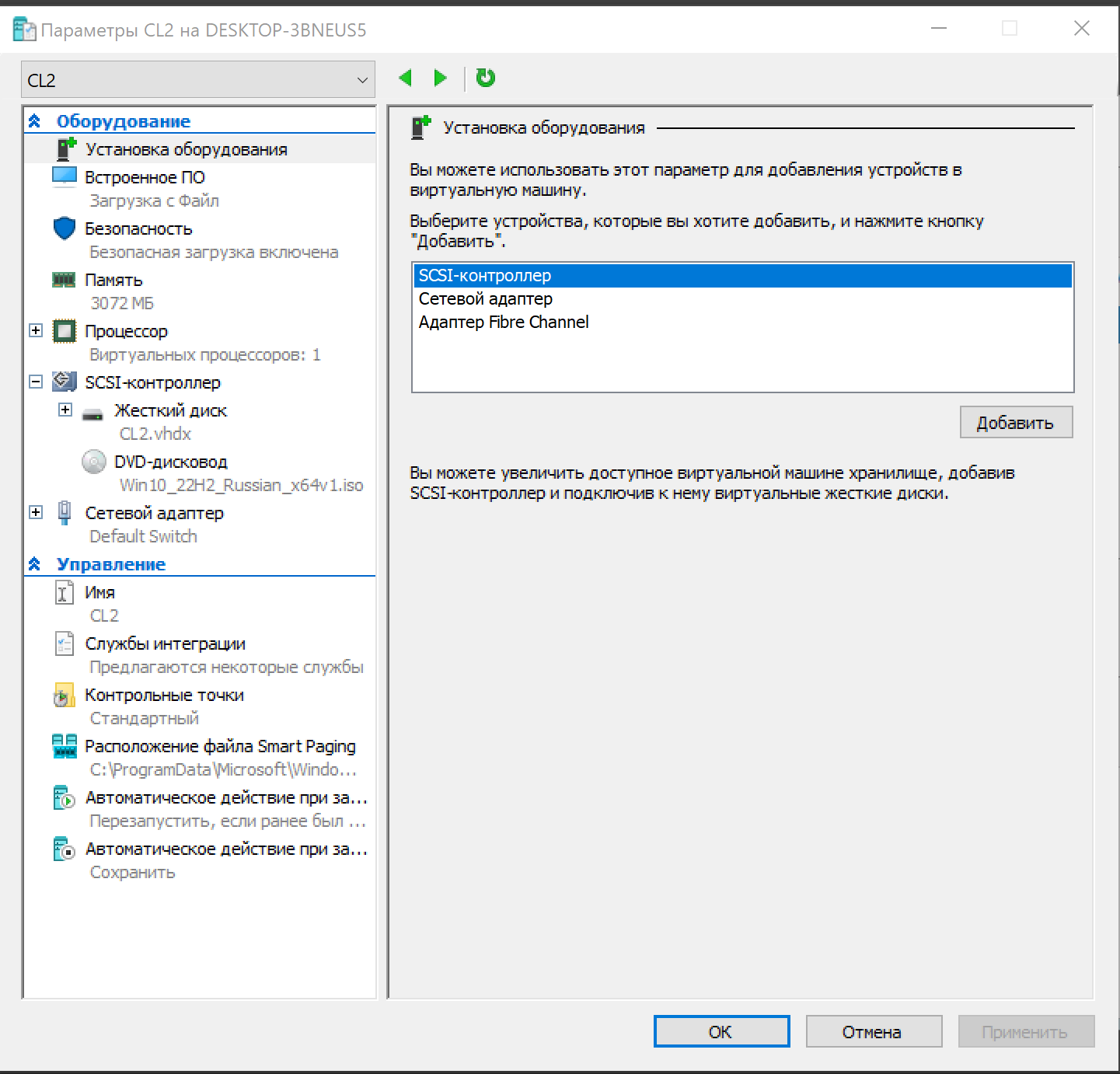


Рисунок 25.1 – параметры CL2

На данном этапе необходимо нажать кнопку “Безопасность”.

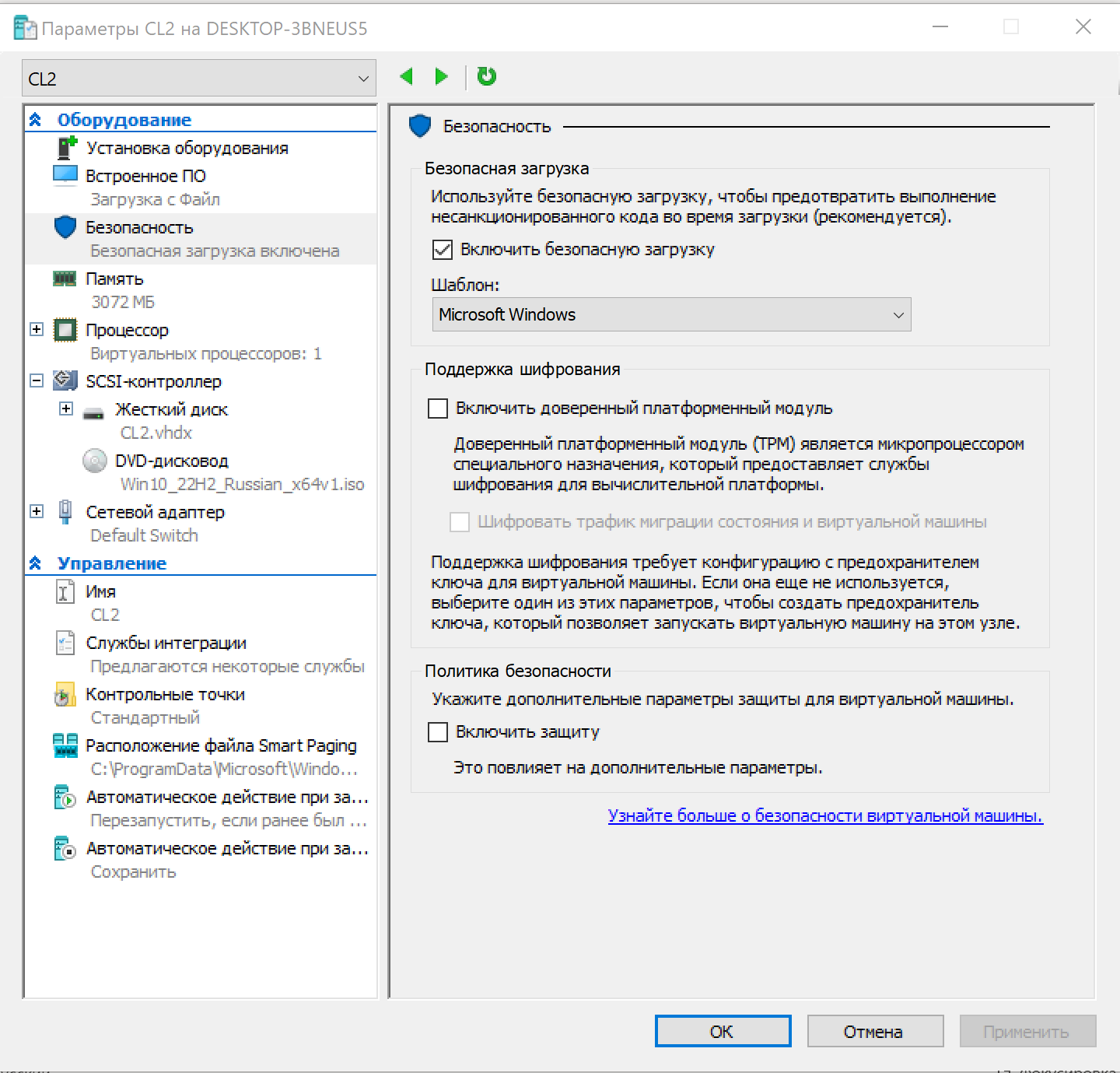


Рисунок 25.2 – Безопасность CL2

На данном этапе необходимо включить доверенный платформенный модуль TPM, а затем нажать кнопку “Применить”, а далее нажать “ОК”. TPM является микропроцессором специального назначения, который предоставляет службы шифрования для вычислительной платформы.

## Отсоединение образа от машины

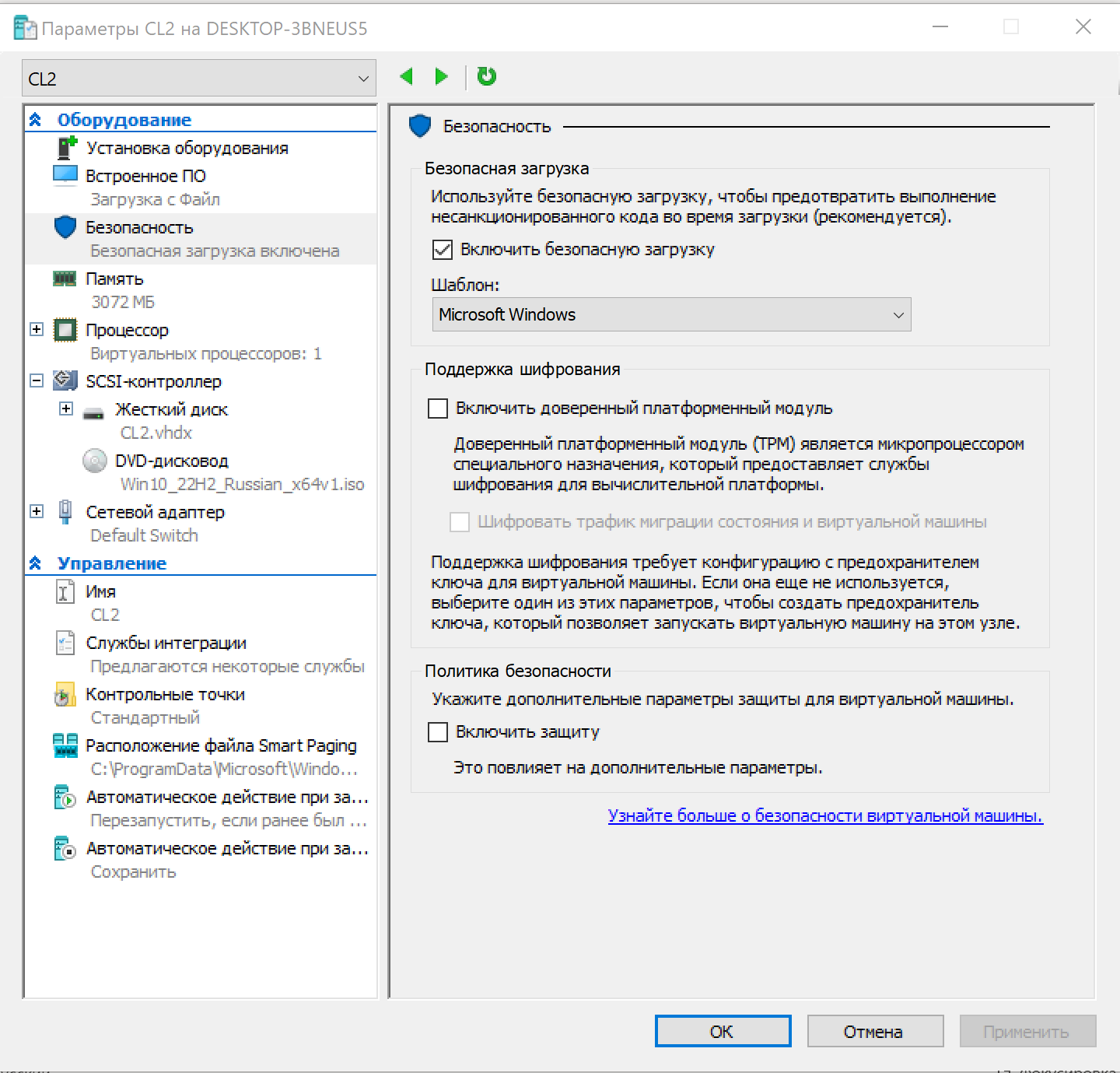


Рисунок 26 – Параметры CL2

На данном этапе необходимо отсоединить DVD диск от клиентской машины.

Для этого необходимо нажать кнопку “DVD-дисковод”.

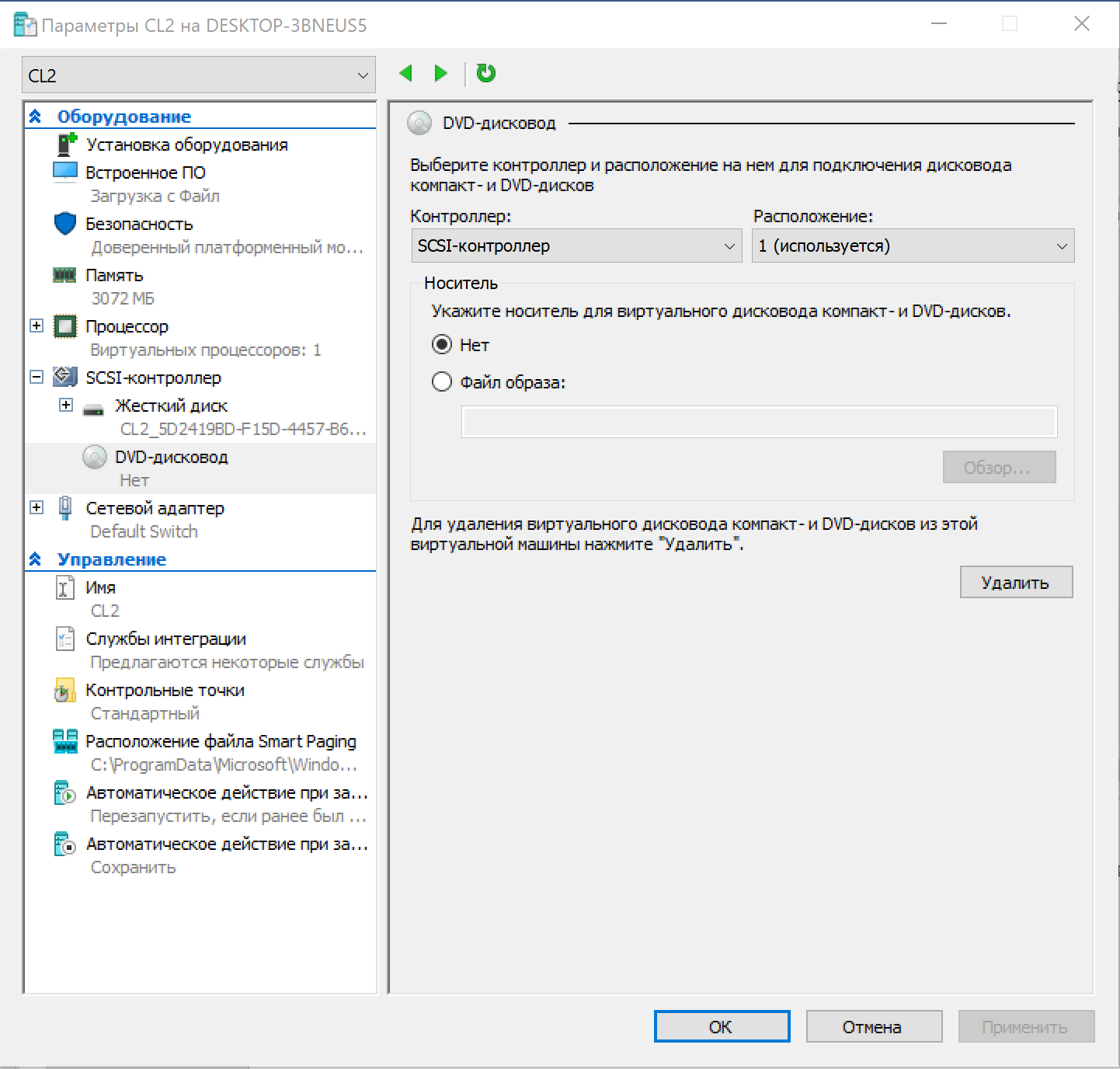


Рисунок 26.1 – DVD-дисковод

На данном этапе необходимо выбрать пункт “Нет” и нажать “Применить”.

## Включение групповой политики для BitLocker

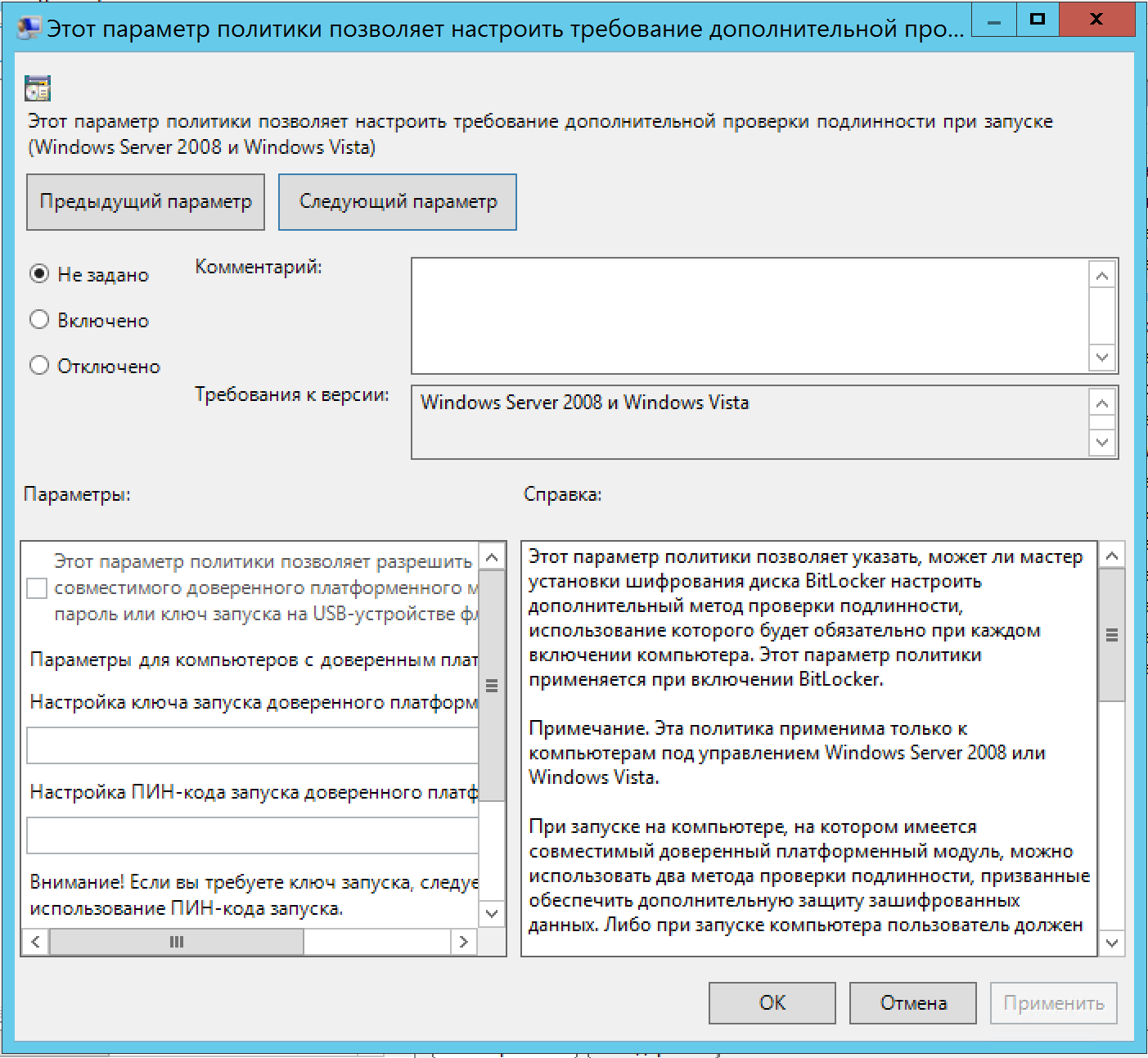


Рисунок 25 - изменение политики для BitLocker

На данном этапе нужно включить эту политику. Необходимо выбрать флаг “Включено”.

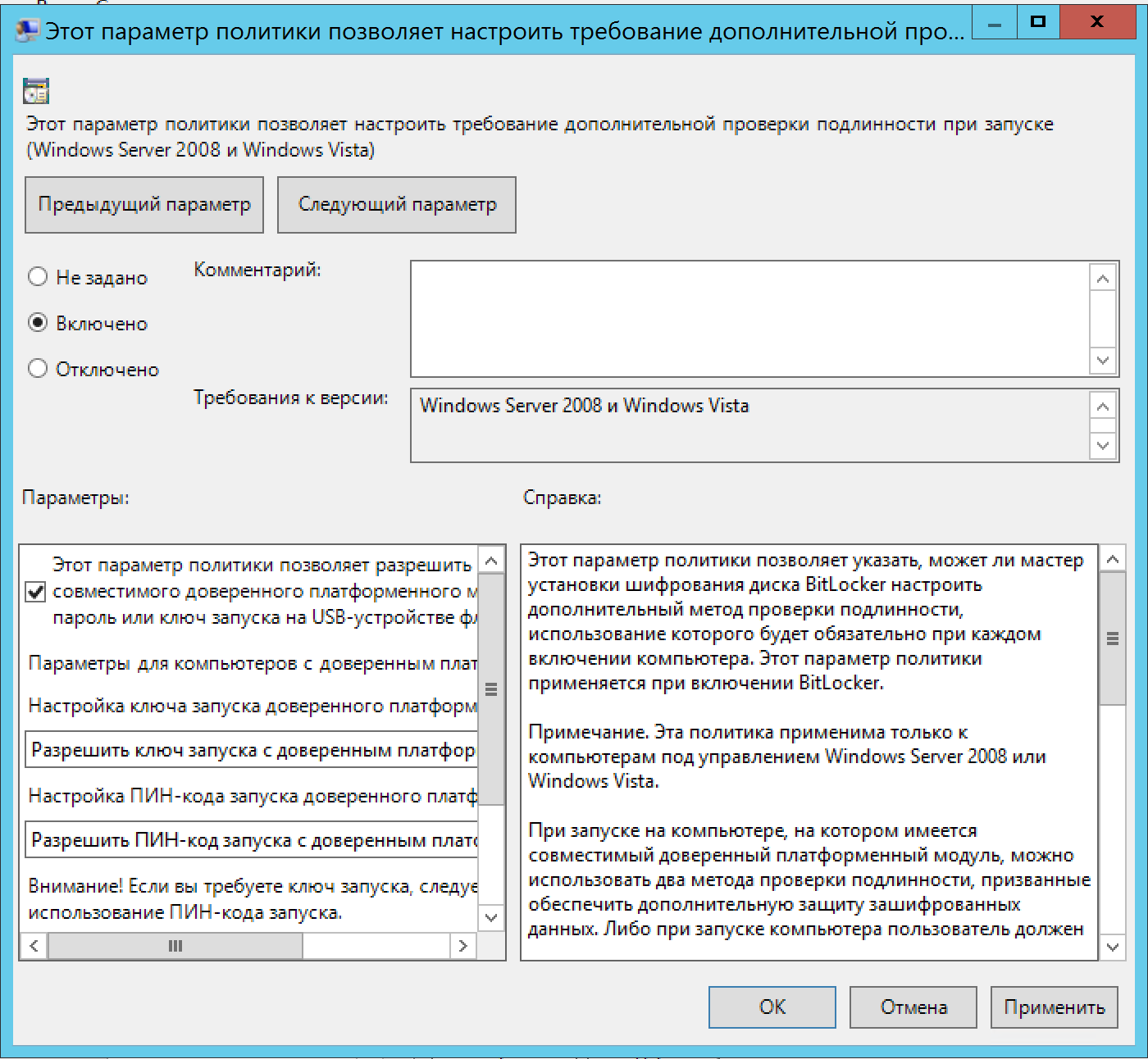


Рисунок 25.1 - изменение политики для BitLocker

На данном этапе необходимо включить флаг “этот параметр политики позволяет разрешить BitLocker без совместимого доверенного платформенного модуля”, а далее нажать на кнопку “Применить”.

## Включение BitLocker

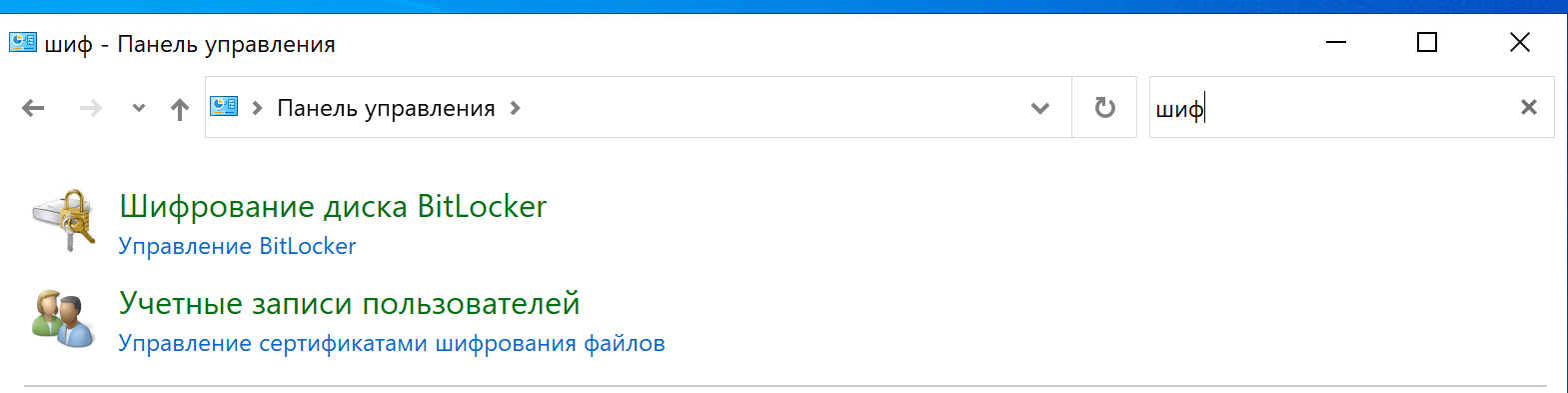


Рисунок 26 – Шифрование диска BitLocker

На данном этапе необходимо войти в программу “Шифрование диска BitLocker”, для этого необходимо нажать на текст “шифрование диска BitLocker”.

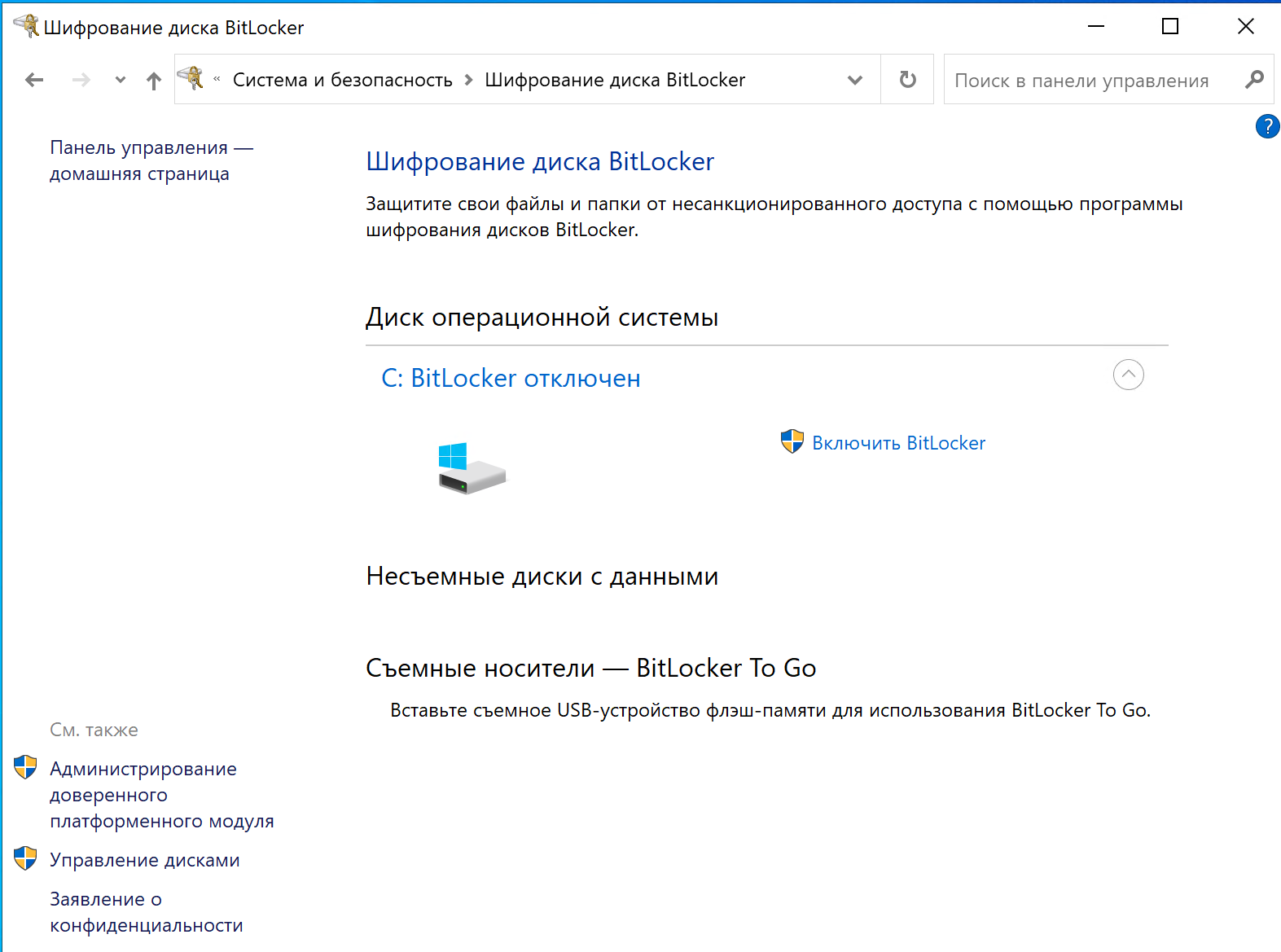


Рисунок 27 – Включение BitLocker

На данном этапе необходимо включить BitLocker.

BitLocker — это внутренний инструмент Windows, разработанный для надёжной защиты данных и восстановления информации в случае потери или повреждения устройства.

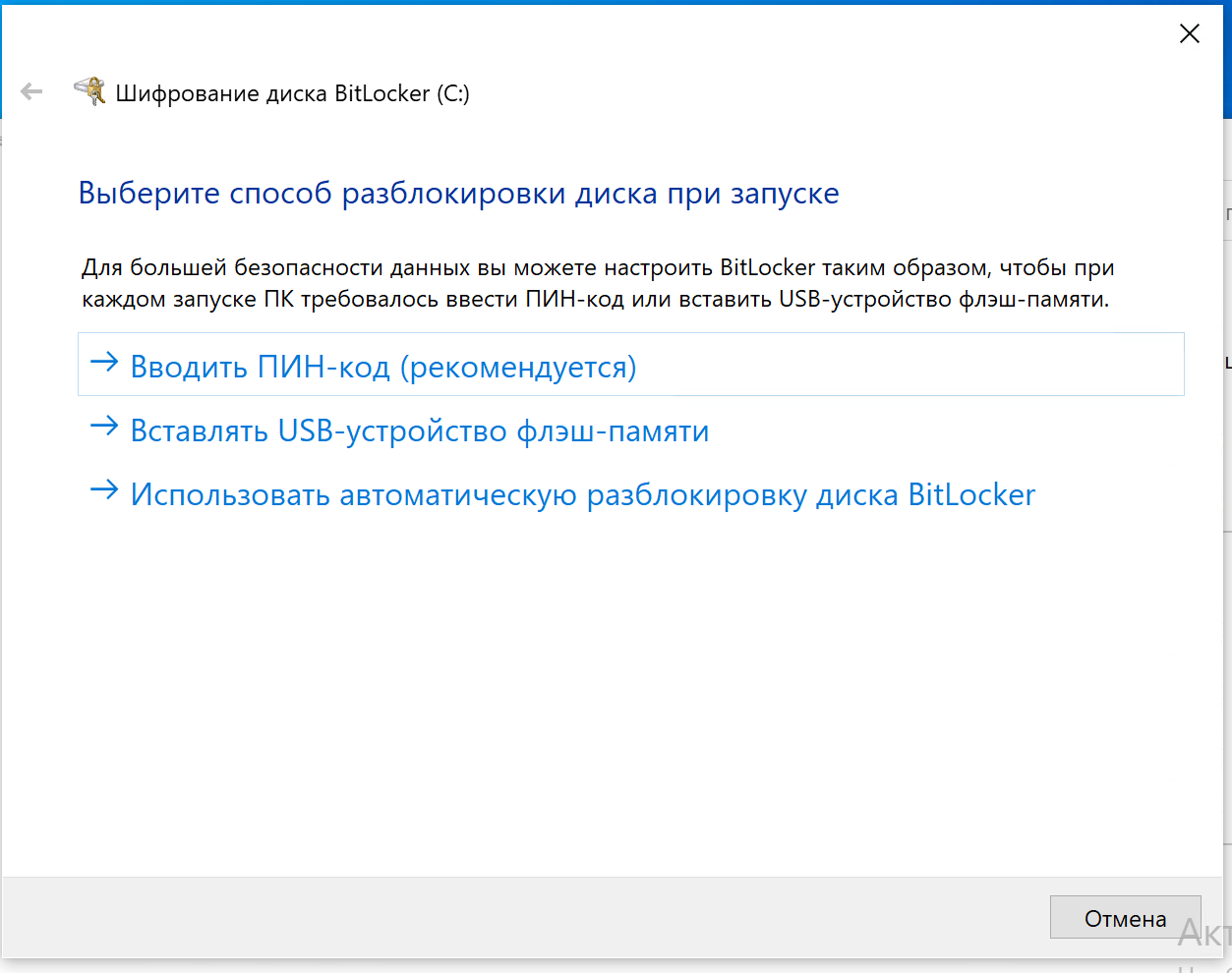


Рисунок 28 – Выбор способа разблокировки диска при запуске

На данном этапе необходимо выбрать ПИН-код.

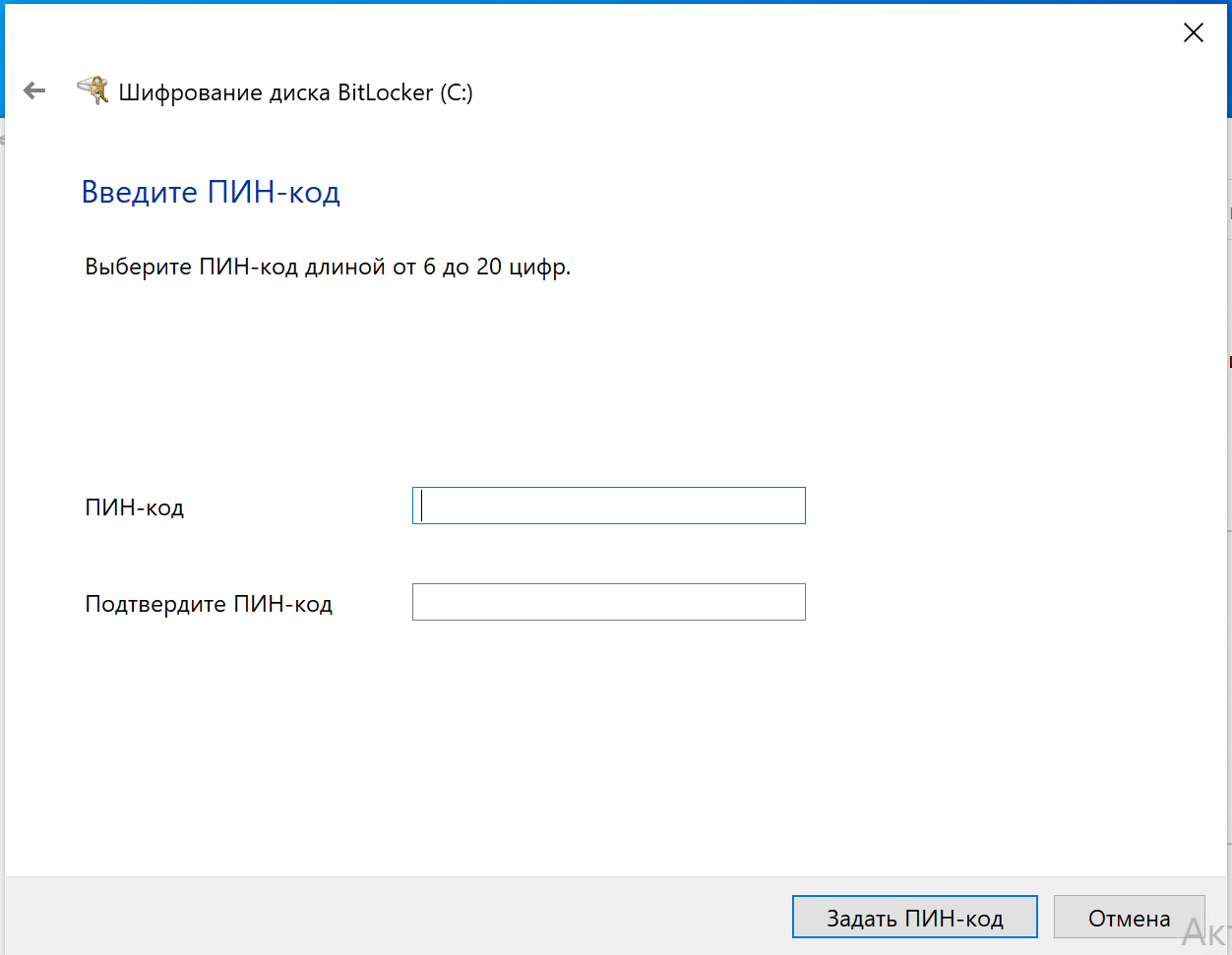


Рисунок 29 – Ввод ПИН-кода

На данном этапе нужно ввести ПИН-код для дальнейшей работы BitLocker.

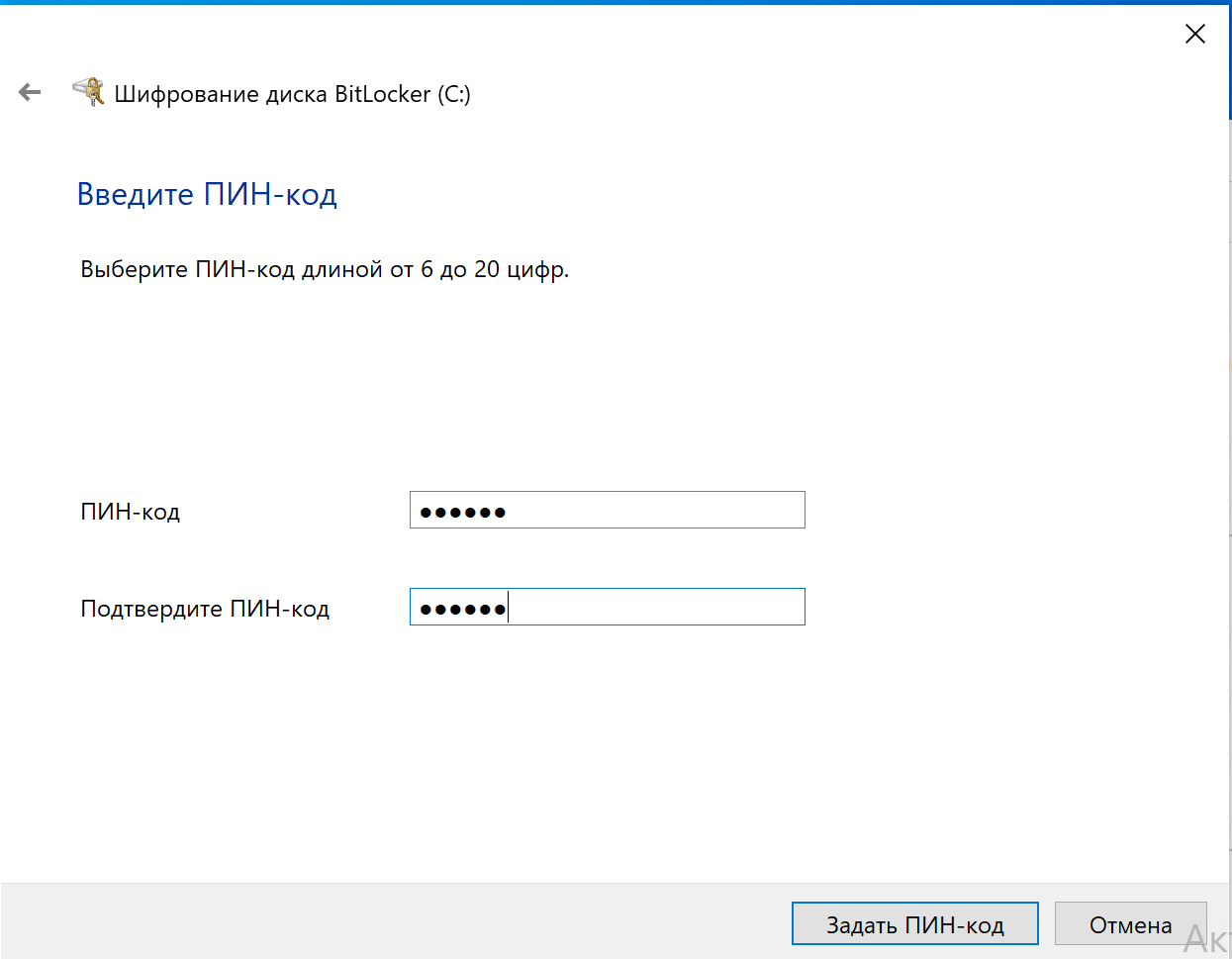


Рисунок 30 – Ввод ПИН-кода

На данном этапе необходимо нажать кнопку “Задать ПИН-код”.

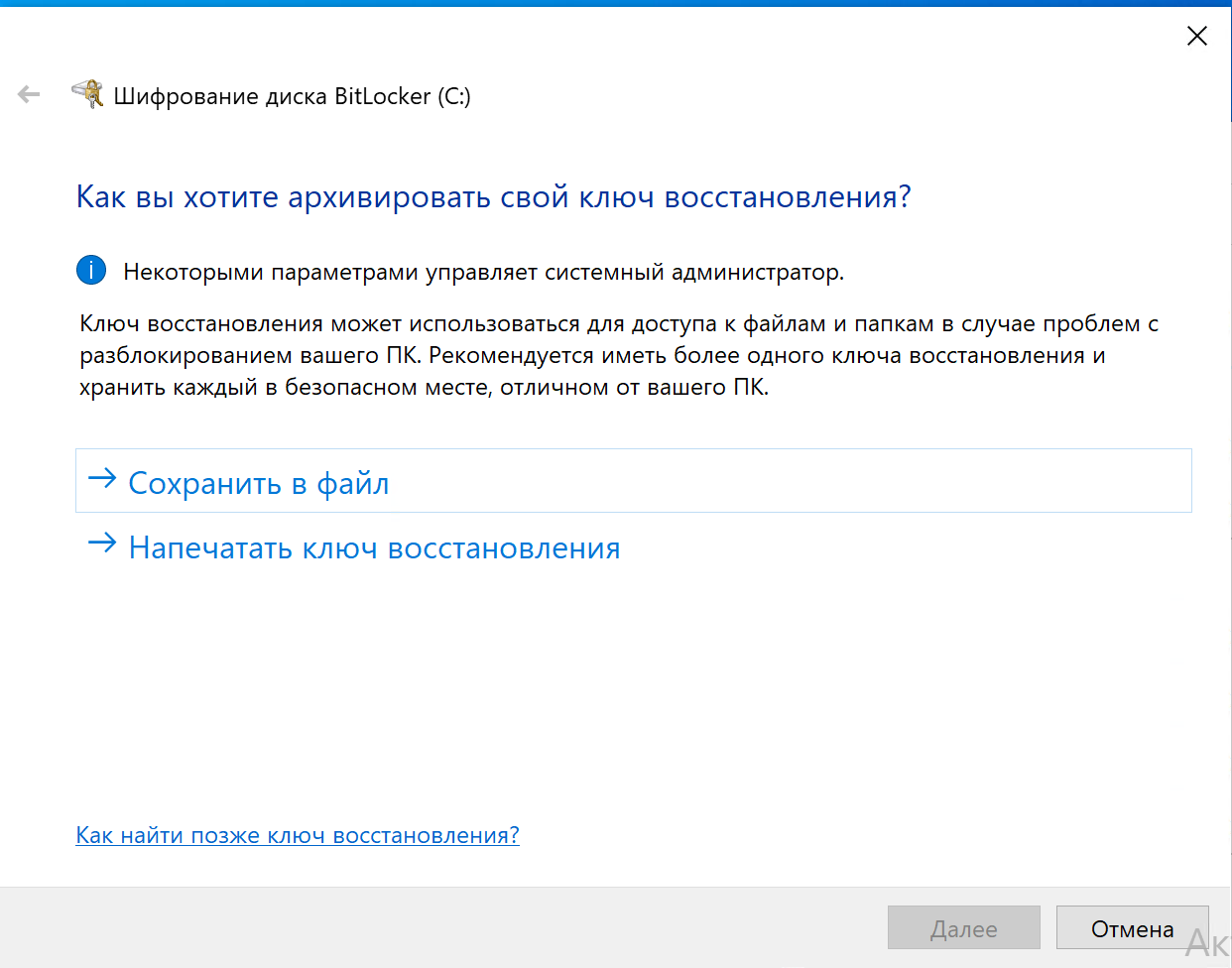


Рисунок 31 – Архивация ключа восстановления

Ключ восстановления может использоваться для доступа к файлам и папкам в случае проблем с разблокированием вашего ПК. Рекомендуется иметь более одного ключа восстановления и хранить каждый в безопасном месте, отличном от вашего ПК. На данном этапе необходимо нажать “сохранить в файл”.

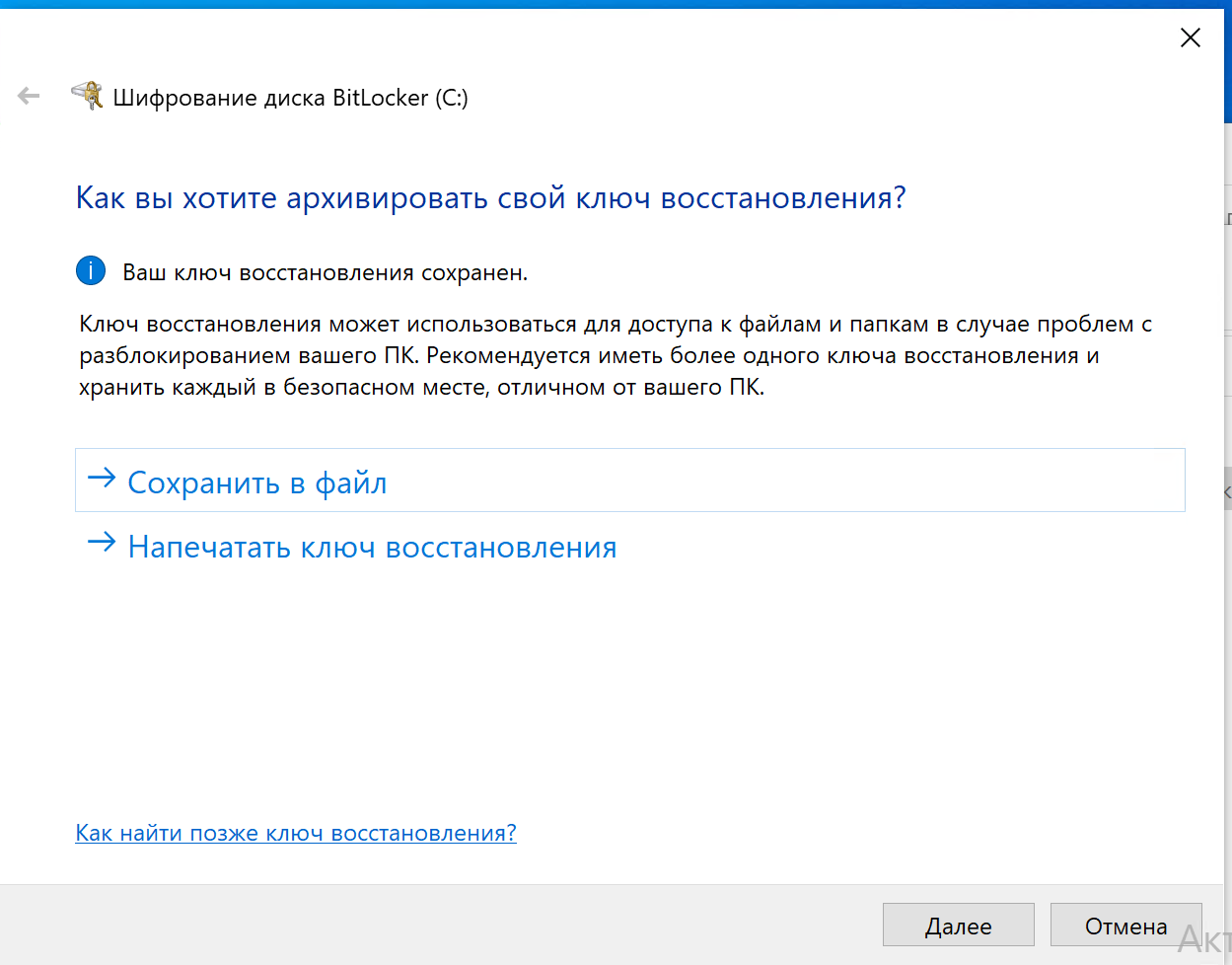


Рисунок 32 – Архивация ключа восстановления

После сохранения ключа восстановления на данном этапе необходимо нажать “Далее”.

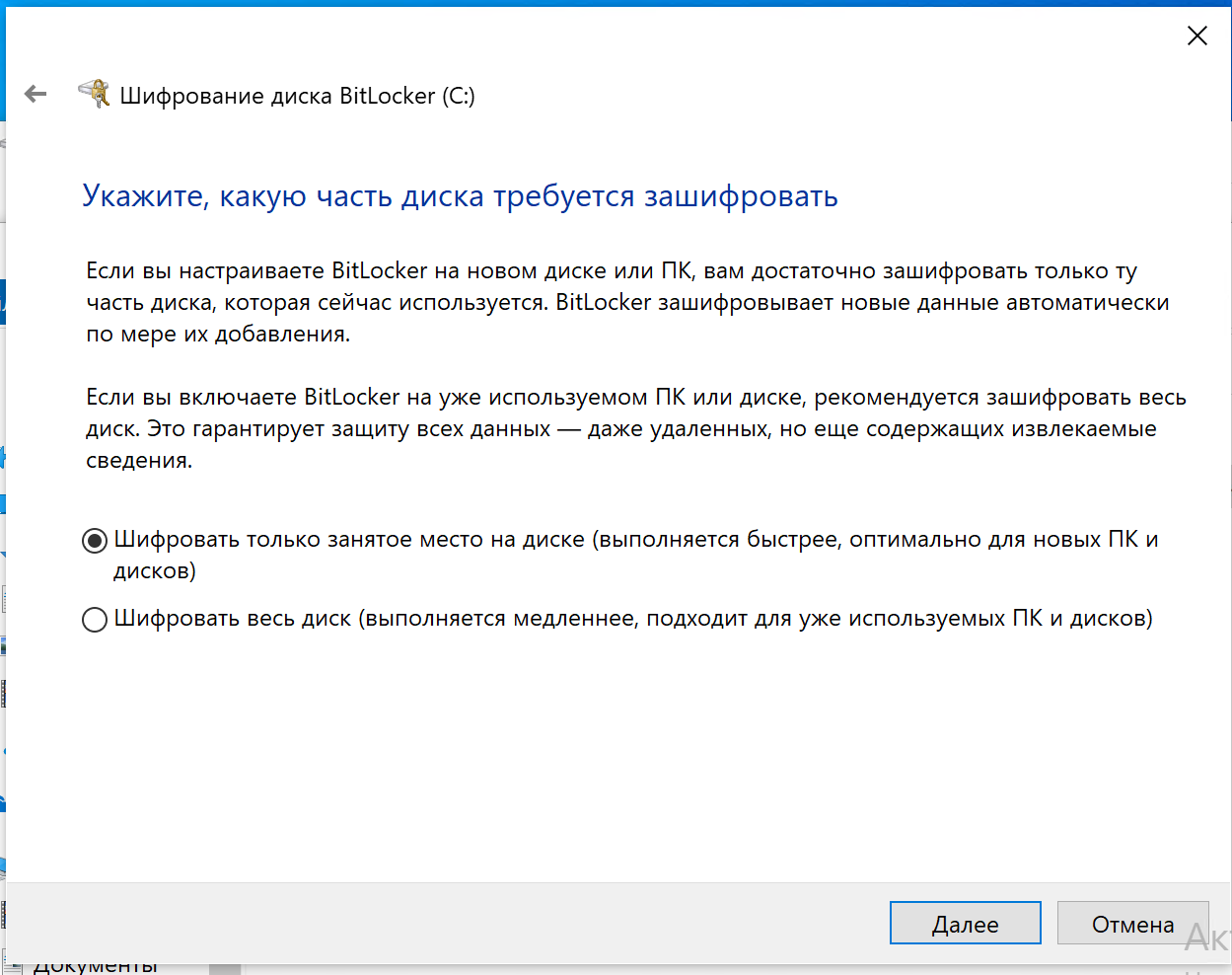


Рисунок 33 – выбор части диска, которую необходимо шифровать

Если шифровать только определенную часть диска, то новые данные будут шифроваться по мере их добавления.

Если шифровать весь диск, то абсолютно все файлы на диске будут зашифрованы.

На данном этапе необходимо выбрать пункт “Шифровать только занятое место на диске.”, а затем кнопку “Далее”.

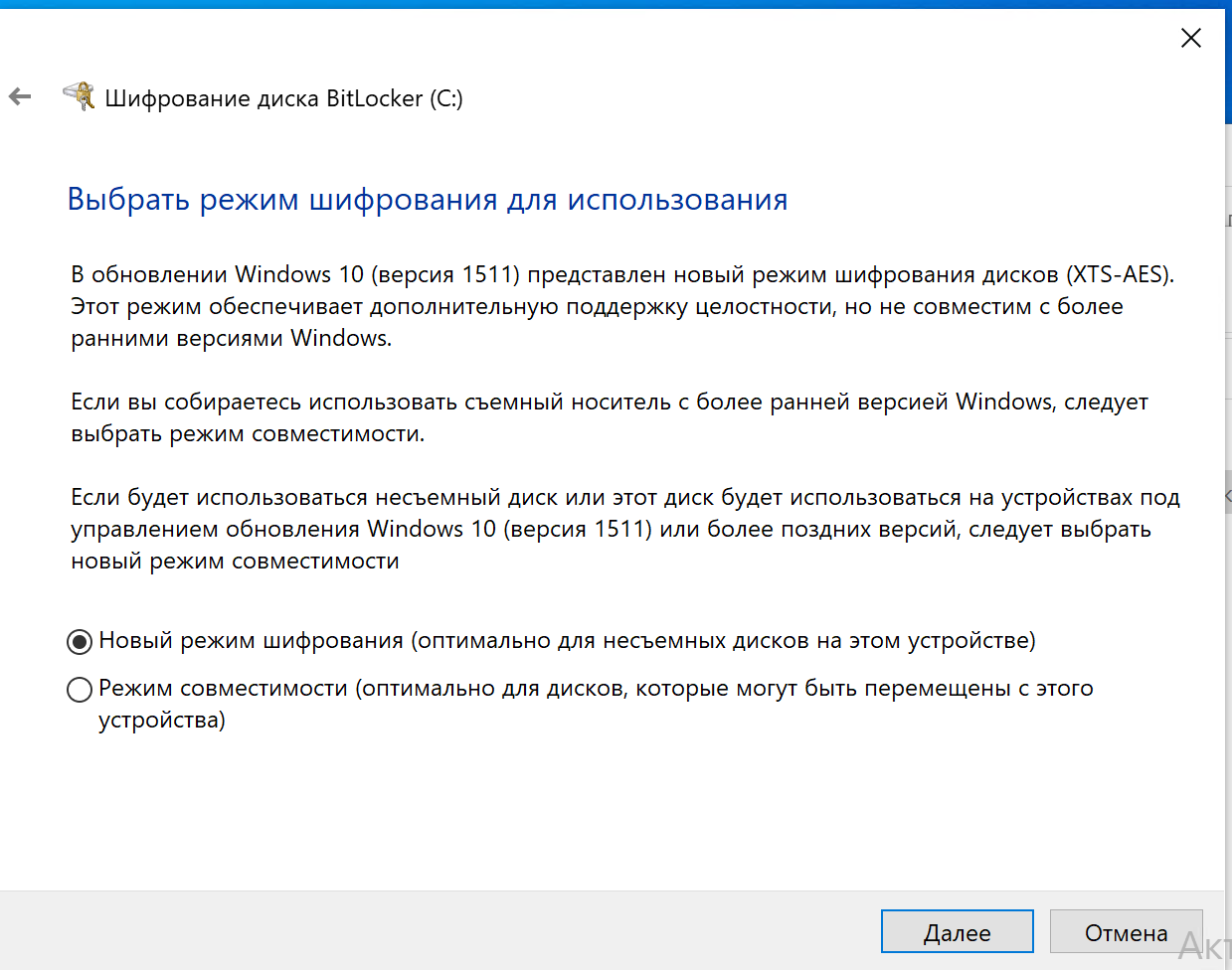


Рисунок 34 – выбор режима шифрования для использования

На данном этапе необходимо выбрать “новый режим шифрования”, так как он оптимален для несъемных дисков на этом устройстве., а затем нажать кнопку “Далее”.

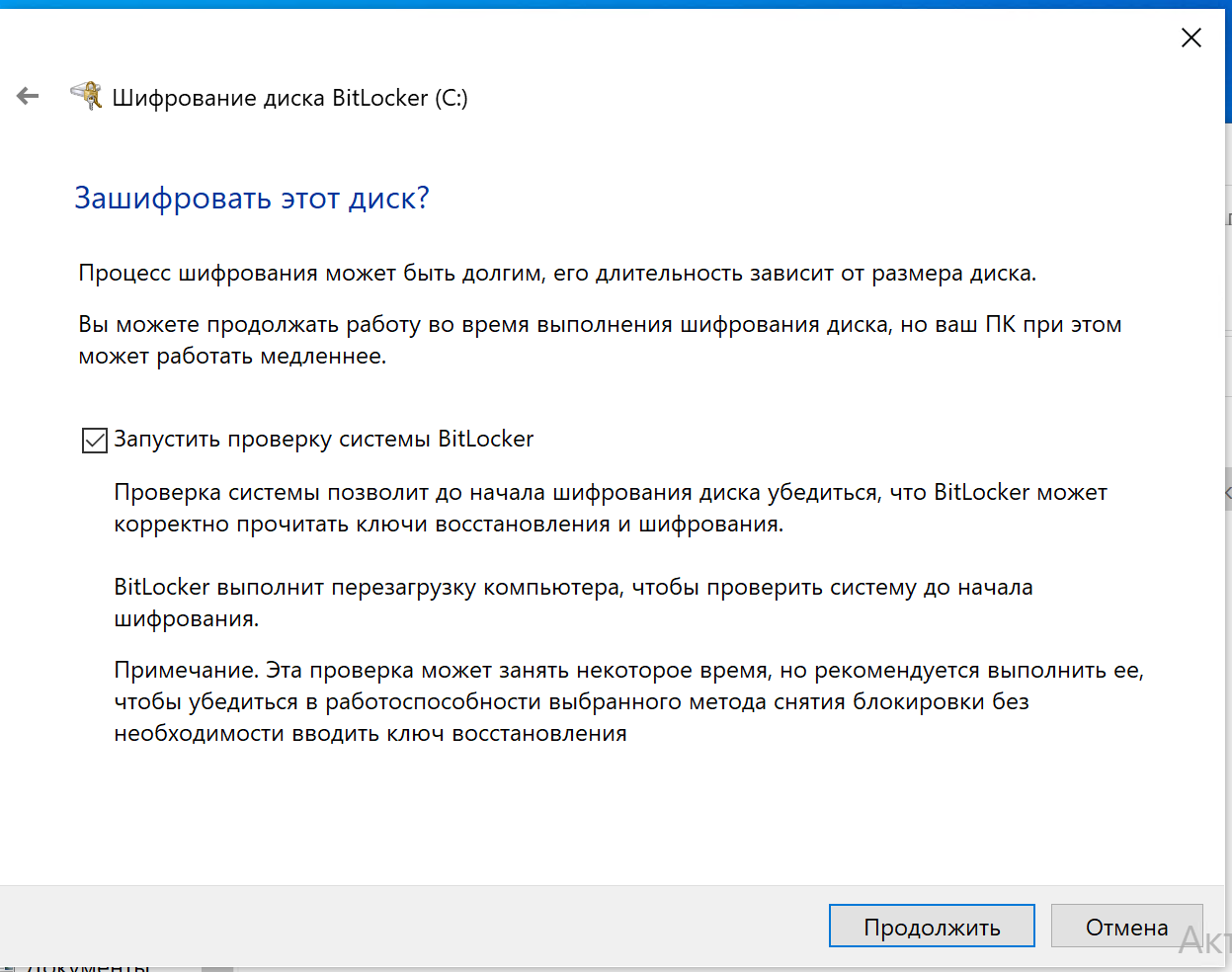


Рисунок 35 – Шифрование диска

На данном этапе необходимо нажать кнопку “Продолжить”.

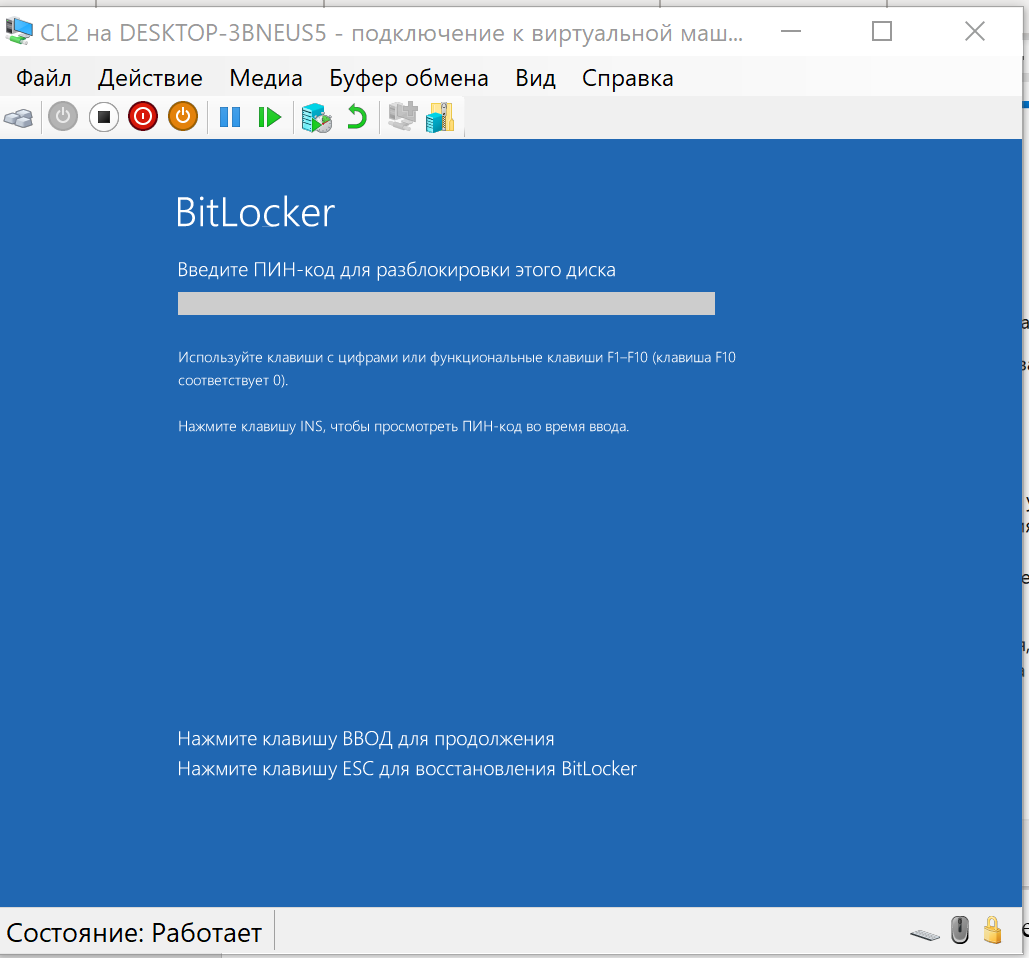


Рисунок 36 – Ввод ПИН-кода для разблокировки системного диска

Шифрование – изменение данных с помощью определенного ключа, эти данные модернизируются с помощью математических формул, также данные демодернизируются налету.

Шифрование системного тома не рекомендуется, так как слишком много сервисов обращается к системному тому, а значит очень большие ресурсы будут тратиться на дешифровку этого диска.

## Шифрование папки

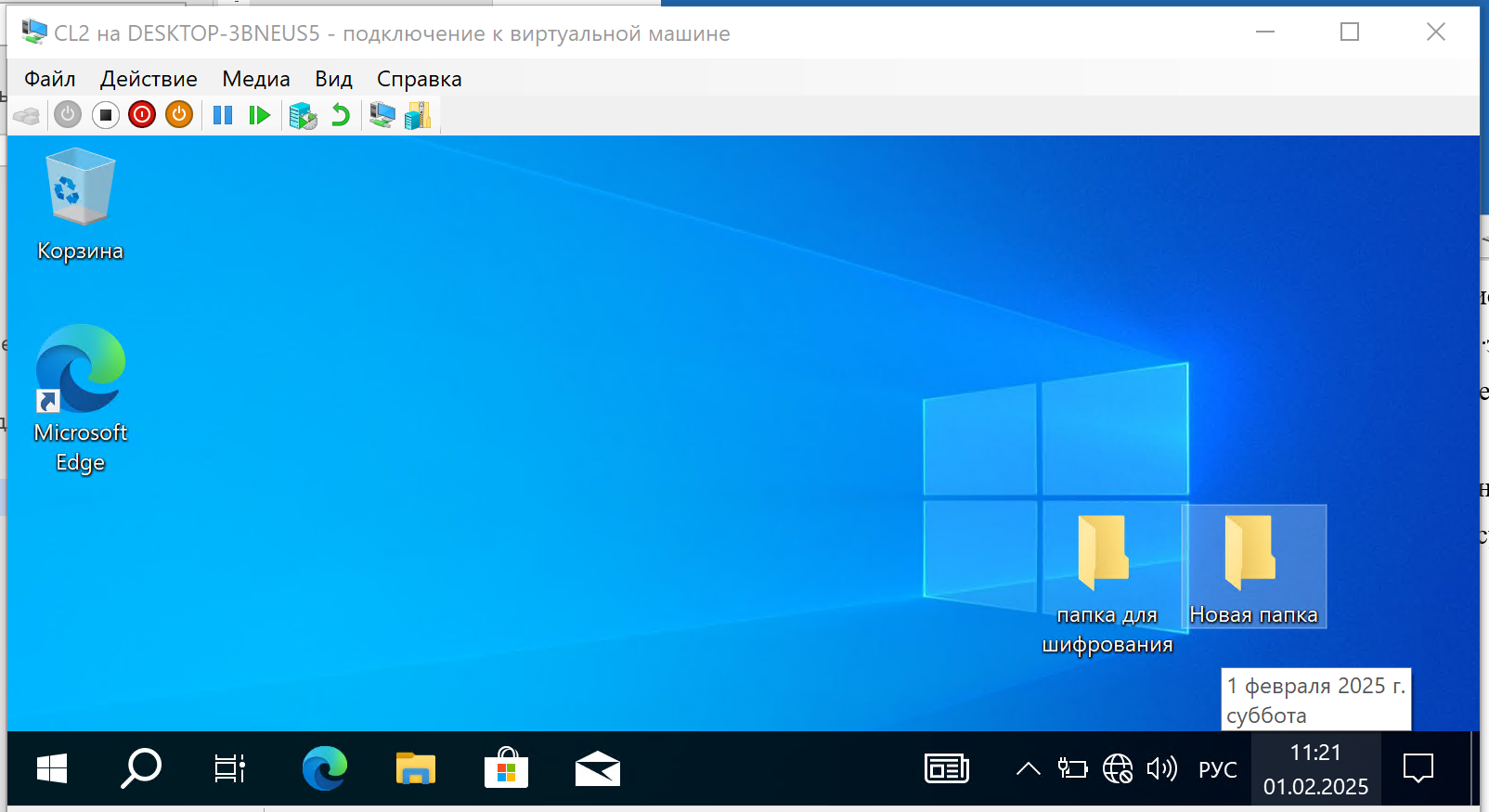


Рисунок 37 – Рабочий стол CL2

На данном этапе необходимо будет совершить шифрование папки. Для этого необходимо нажать правой кнопкой мыши по папке.

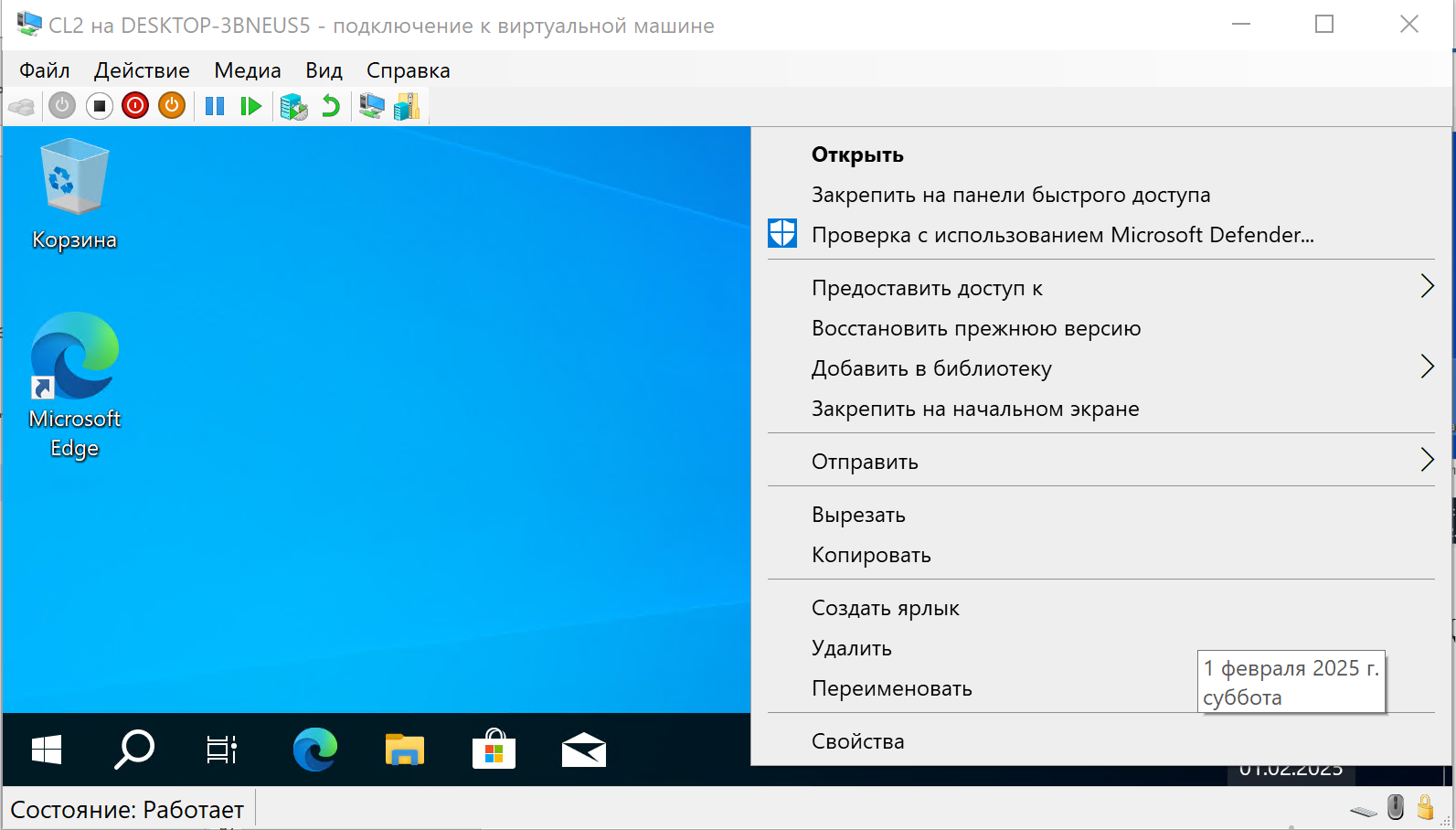


Рисунок 38 – Опции папки

На данном этапе необходимо нажать кнопку “Свойства”.

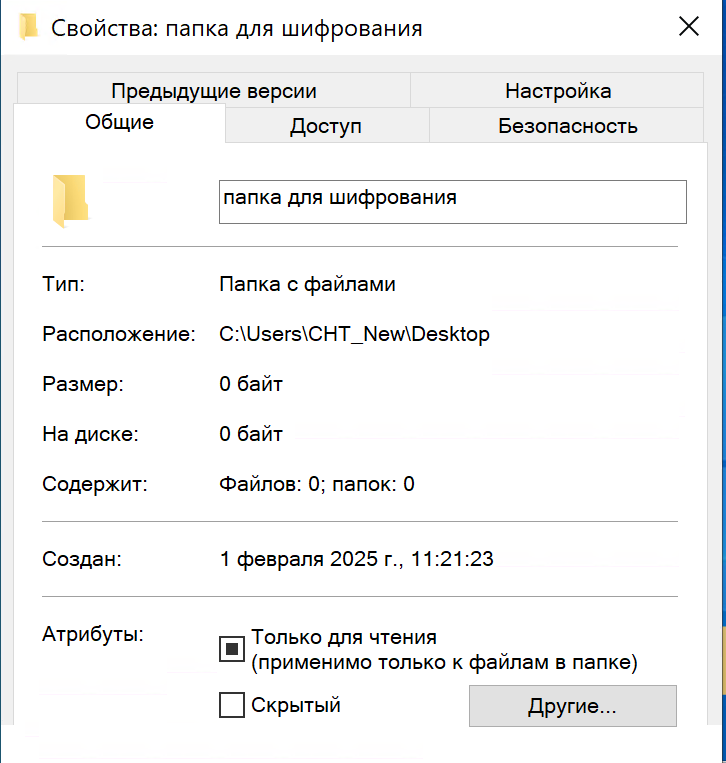


Рисунок 39 – Свойства папки

На данном этапе необходимо нажать кнопку “Другие”.

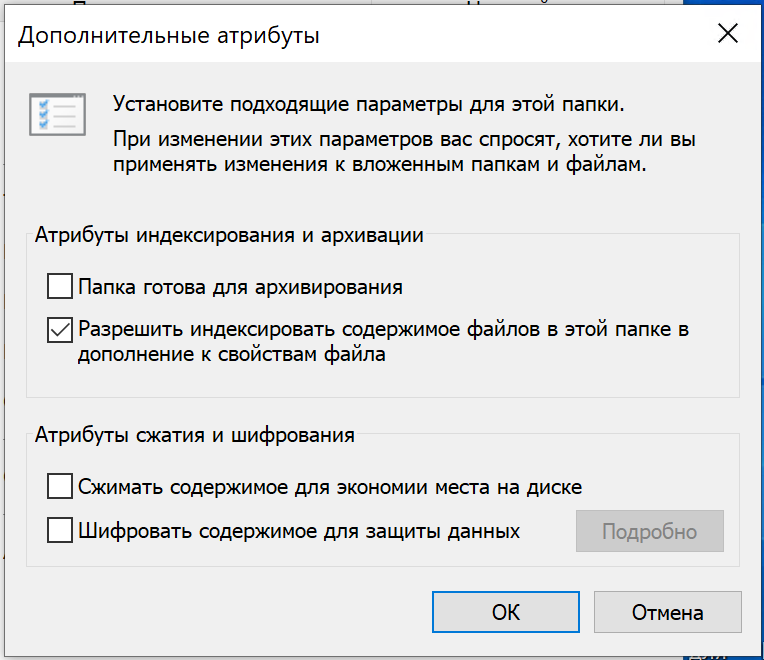


Рисунок 40 – Дополнительные атрибуты

Чтобы начать шифрование папки необходимо нажать флаг “Шифровать содержимое для защиты данных”, а далее нажать кнопку “ОК”

Данные буду доступны только той учетной записи, с которой было выполнено шифрование, а названия зашифрованных файлов и папок становятся зеленого цвета.