

**Федеральное государственное автономное образовательное  
учреждение высшего образования  
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
УНИВЕРСИТЕТ «ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»  
Московский институт электроники и математики им. Тихонова  
Департамент электронной инженерии**

**ОТЧЕТ  
О ПРАКТИЧЕСКОЙ РАБОТЕ №1**

по дисциплине «Программные и аппаратные средства защиты информации»  
**«Средства безопасности Windows 7»**

Студент гр. БИБ201

Шадрунов Алексей

Дата выполнения: 5 февраля 2023 г.

Преподаватель:

Перов А. А.

«\_\_\_» \_\_\_\_\_ 2023 г.

Москва, 2023

## **Содержание**

|  |           |
|--|-----------|
| <b>1 Задание на практическую работу</b>                    | <b>3</b>  |
| <b>2 Ход работы</b>  | <b>3</b>  |
| 2.1 Пользователи . . . . .                                 | 3         |
| 2.2 Группы безопасности . . . . .                          | 4         |
| 2.3 Разграничение доступа . . . . .                        | 5         |
| 2.4 Шаблон безопасности системы . . . . .                  | 8         |
| 2.5 Анализ параметров безопасности системы . . . . .       | 10        |
| 2.6 Настройка параметров безопасности по шаблону . . . . . | 12        |
| 2.7 Работа с журналом безопасности . . . . .               | 13        |
| 2.8 Брандмауэр Windows . . . . .                           | 19        |
| 2.9 UAC . . . . .  | 22        |
| 2.10 Архивация и восстановление . . . . .                  | 23        |
| 2.11 Защитник Windows . . . . .                            | 25        |
| <b>3 Выводы о проделанной работе</b>                       | <b>26</b> |

# 1 Задание на практическую работу

Ознакомиться с функциями безопасности Windows 7, улучшениями и приложениями. Изучить брандмауэр Windows.

## 2 Ход работы

### 2.1 Пользователи

Создаём двух новых пользователей user1 и user2 (рисунки 1 и 2).

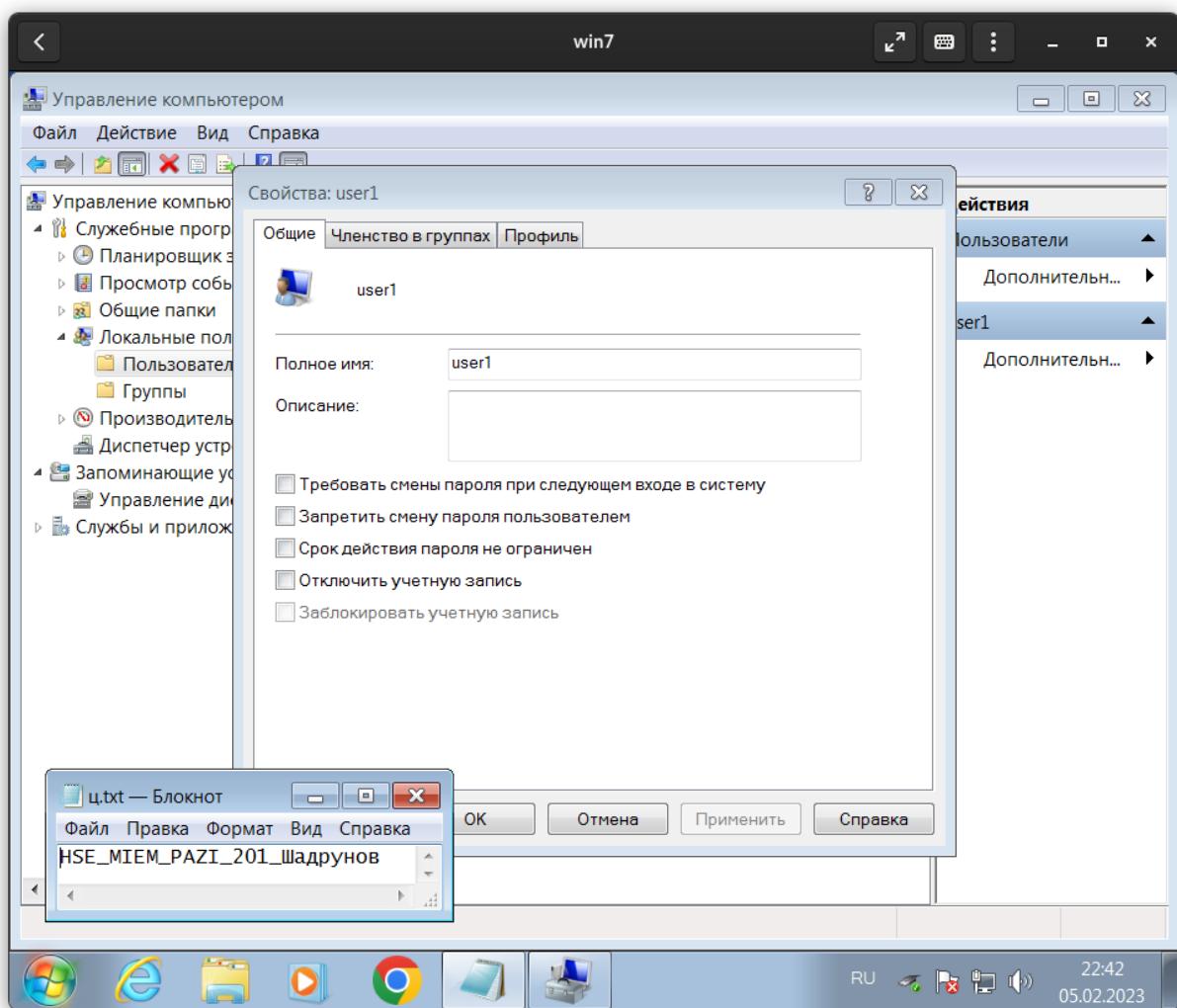


Рисунок 1 – User1

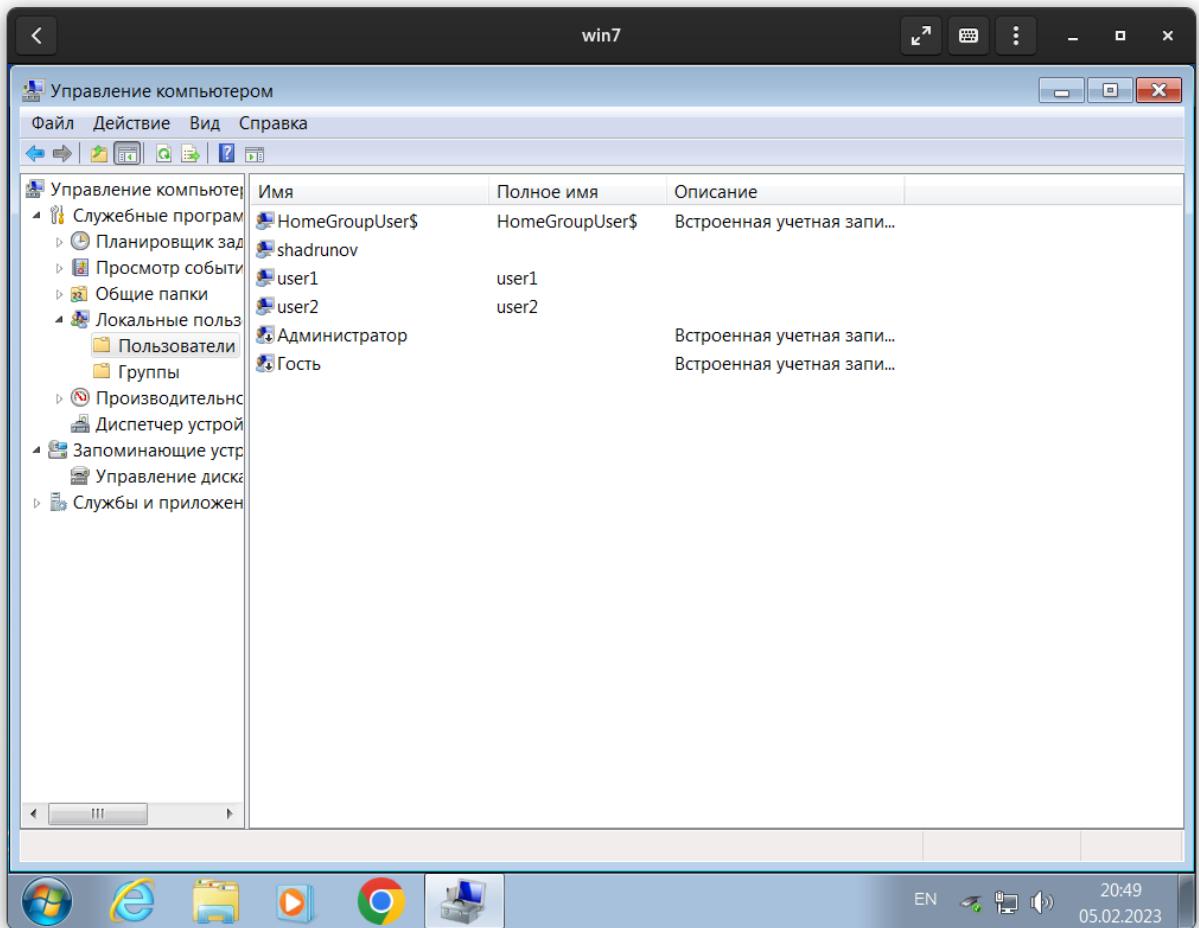


Рисунок 2 – Два пользователя в оснастке

## 2.2 Группы безопасности

Создаём две группы безопасности group1 и group2 (рисунок 3). Включаем каждого пользователя в свою группу.

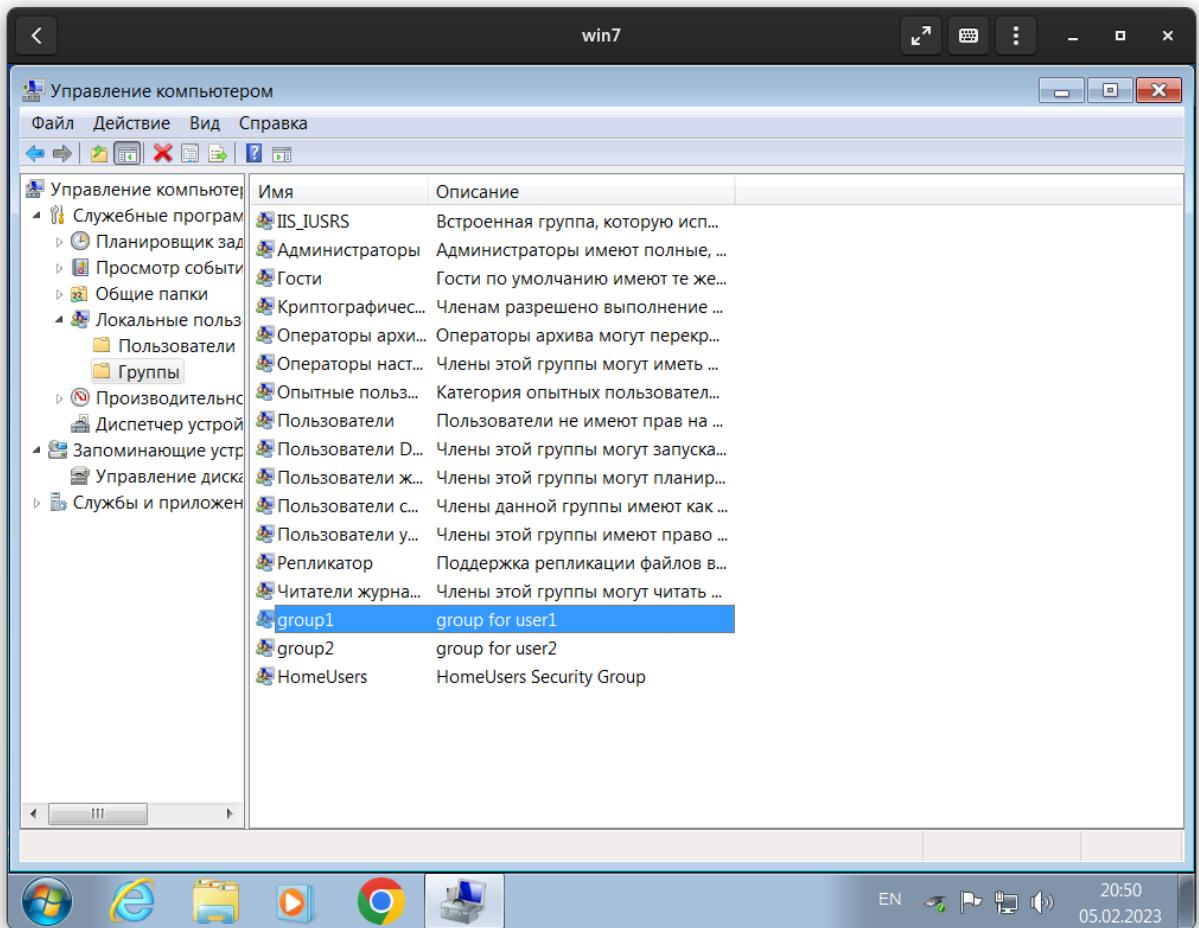


Рисунок 3 – Группы безопасности

### 2.3 Разграничение доступа

Создаём четыре каталога со следующими правами (рисунки 4-7):

- каталог1: только чтение для пользователя1, чтение, создание и изменение файлов для пользователя2;
- каталог2: нет доступа для пользователя1, только чтение для пользователя2;
- каталог3: только чтение для группы1, только чтение для группы2;
- каталог4: полный доступ для группы1, создание и изменение файлов для группы2;

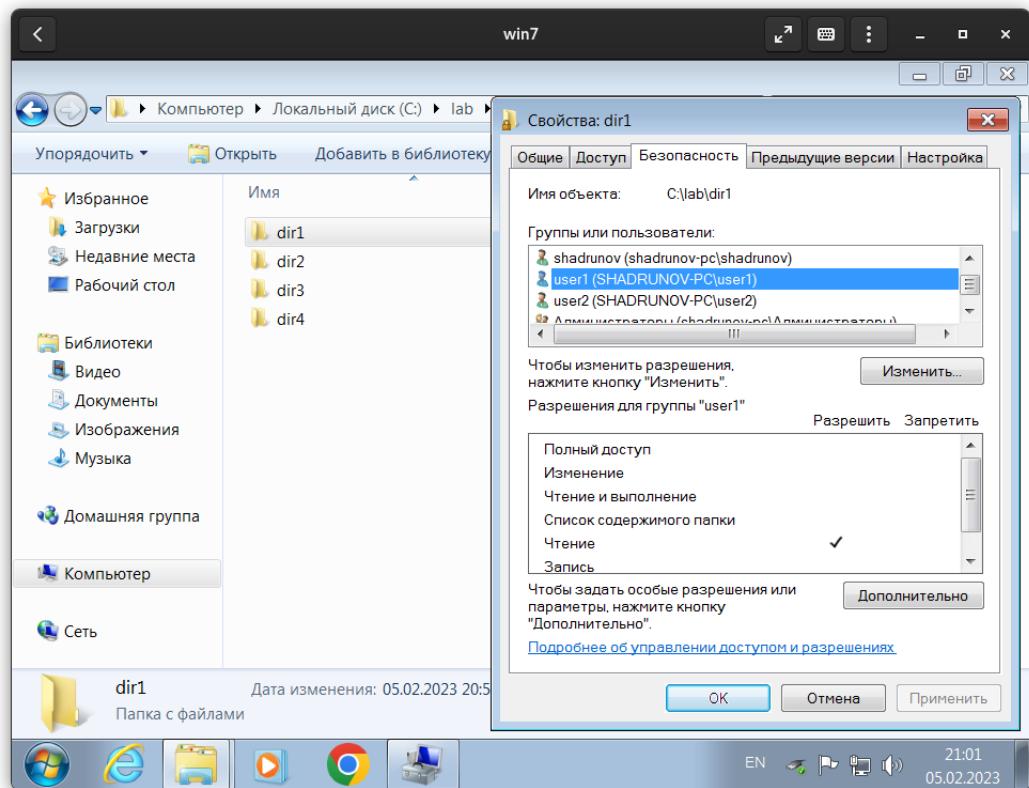


Рисунок 4 – каталог1

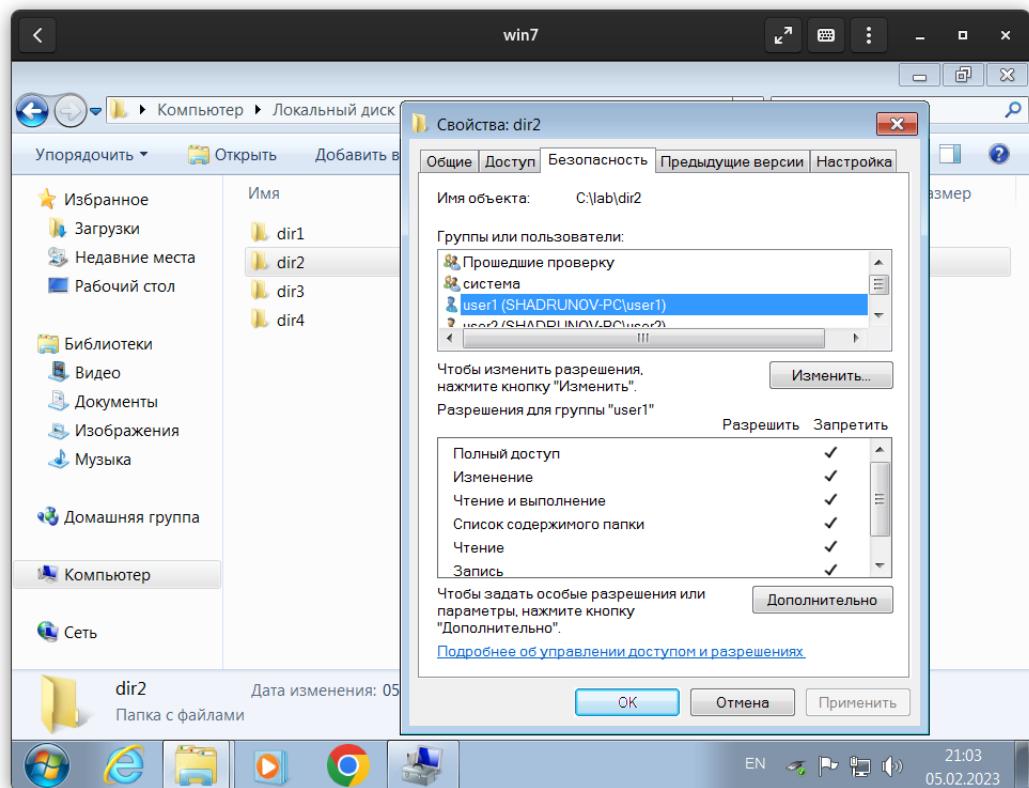


Рисунок 5 – каталог2

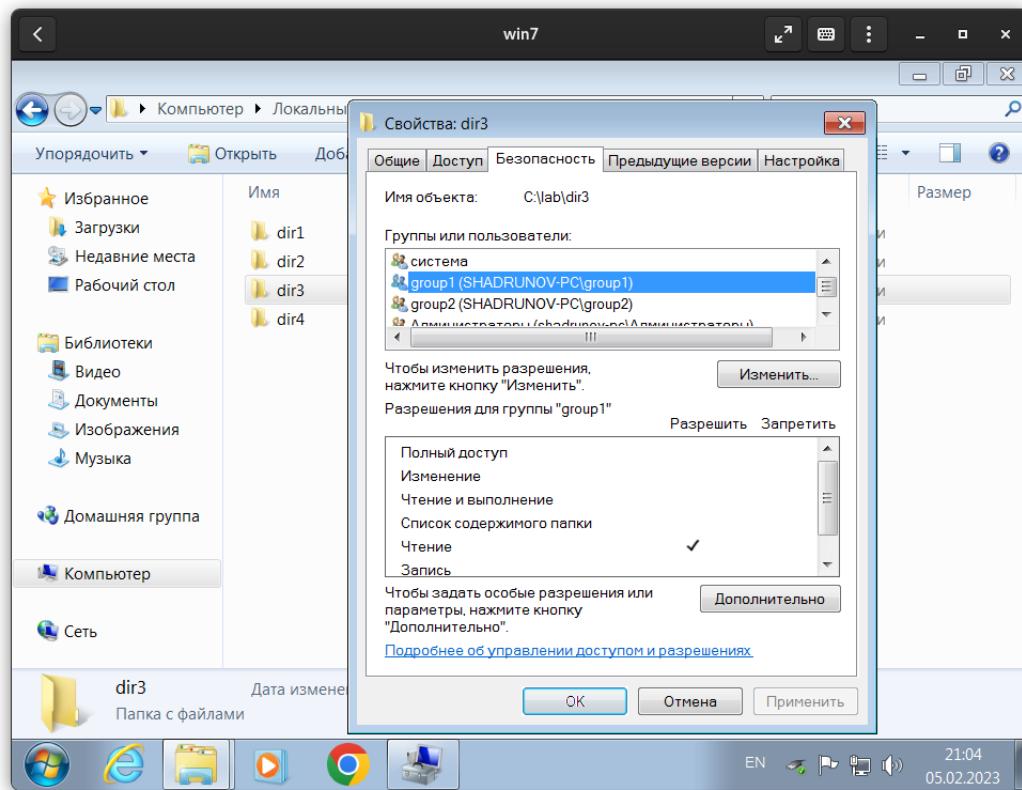


Рисунок 6 – каталог3

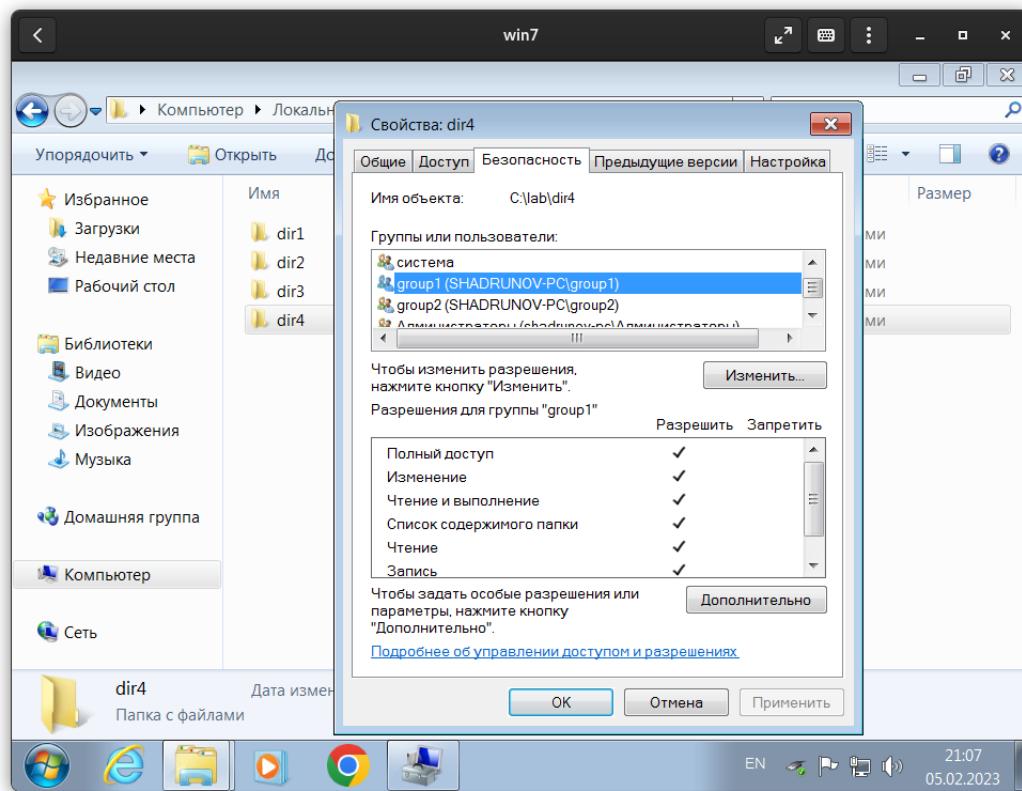


Рисунок 7 – каталог4

Видно, что у пользователя user1 нет доступа к dir2 (рисунок 8).

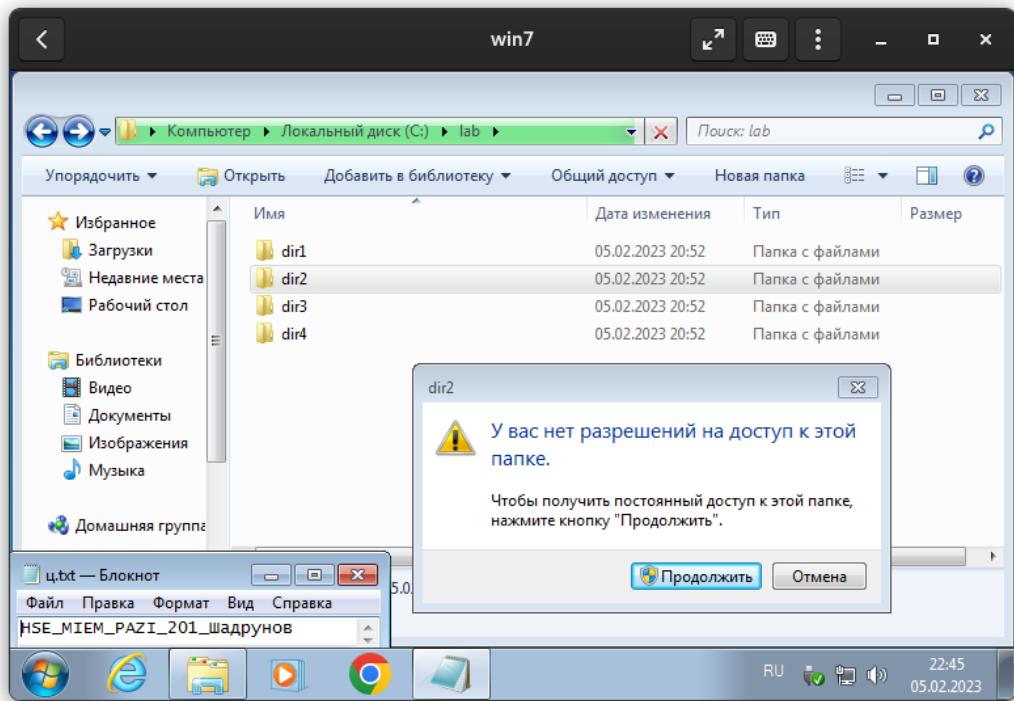


Рисунок 8 – У пользователя1 нет доступа к каталог2

## 2.4 Шаблон безопасности системы

Создаём шаблон безопасности системы, указав параметры по заданию: вести журнал паролей, минимальная длина пароля, пароль должен отвечать требованиям сложности, пороговое значение блокировки, аудит входа в систему, аудит доступа к объектам, аудит событий входа в систему, аудит управления учетными записями (рисунки 9-10).

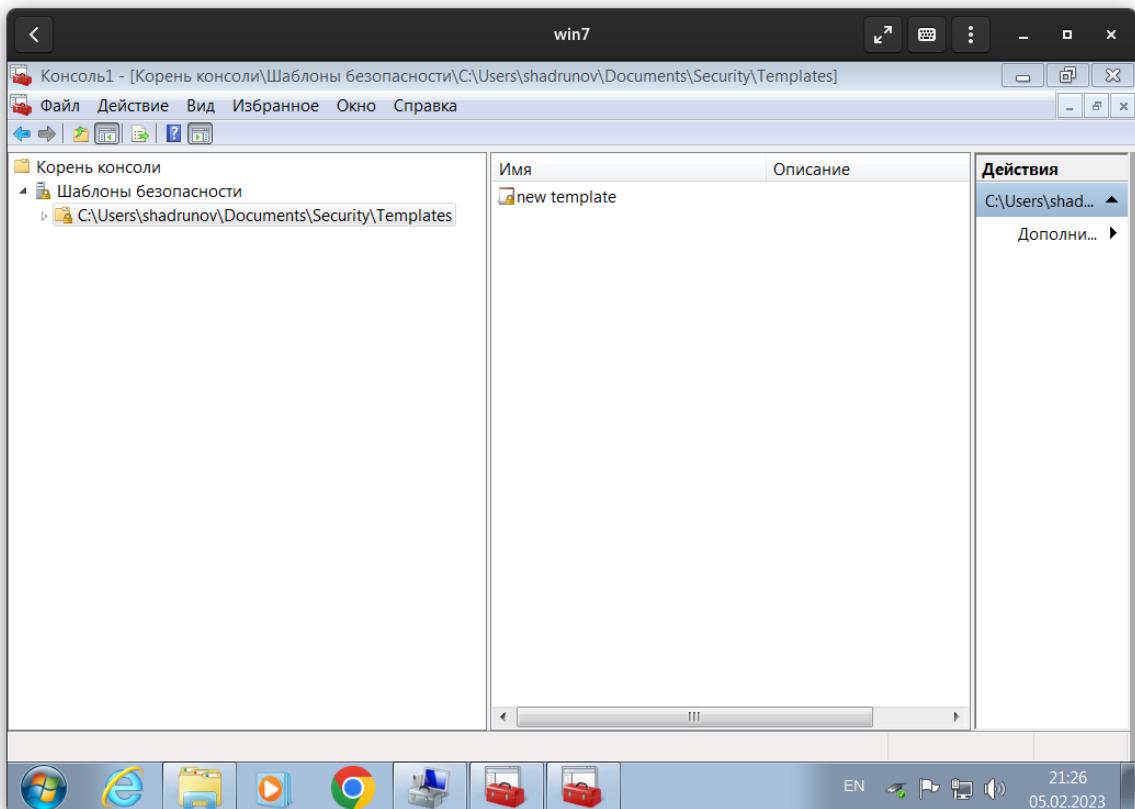


Рисунок 9 – Новый шаблон

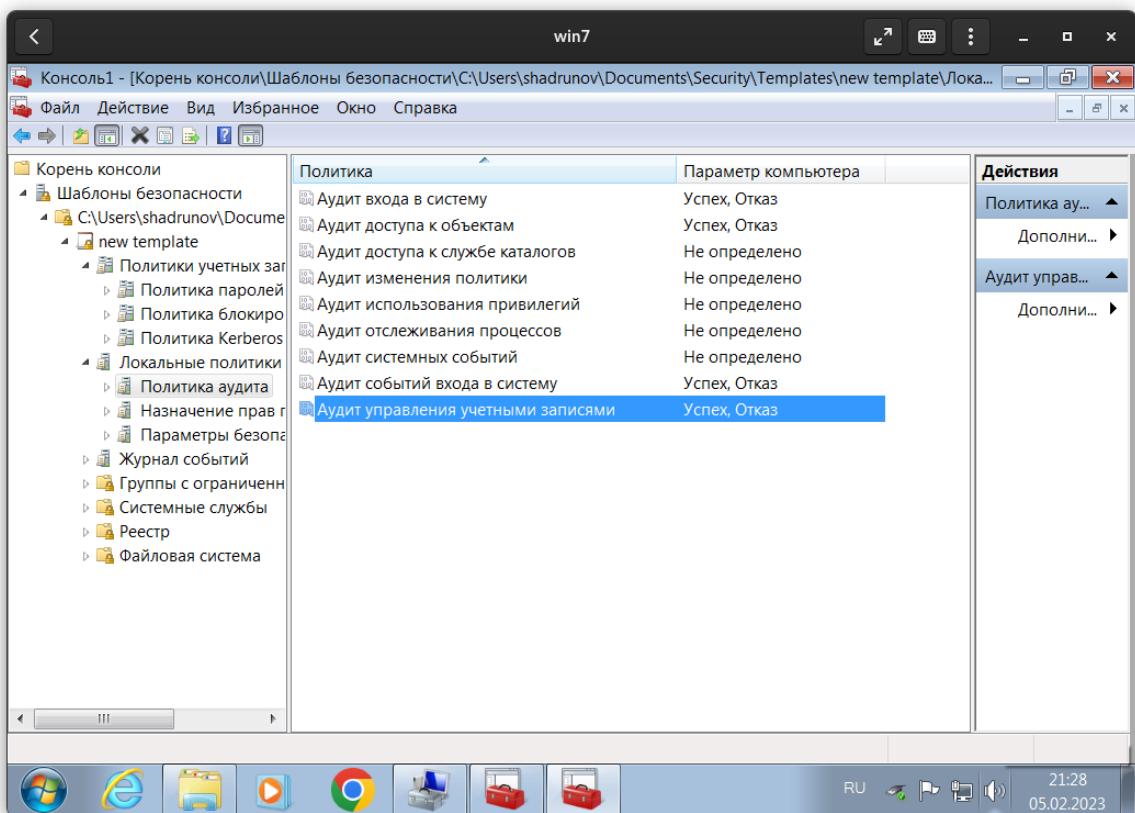


Рисунок 10 – Заданы параметры аудита

## 2.5 Анализ параметров безопасности системы

Проводим анализ параметров безопасности системы по заданному шаблону и выявляем различия между шаблоном и существующими параметрами (рисунки 11-13). Видно, что все заданные параметры отличаются от стандартных в системе.

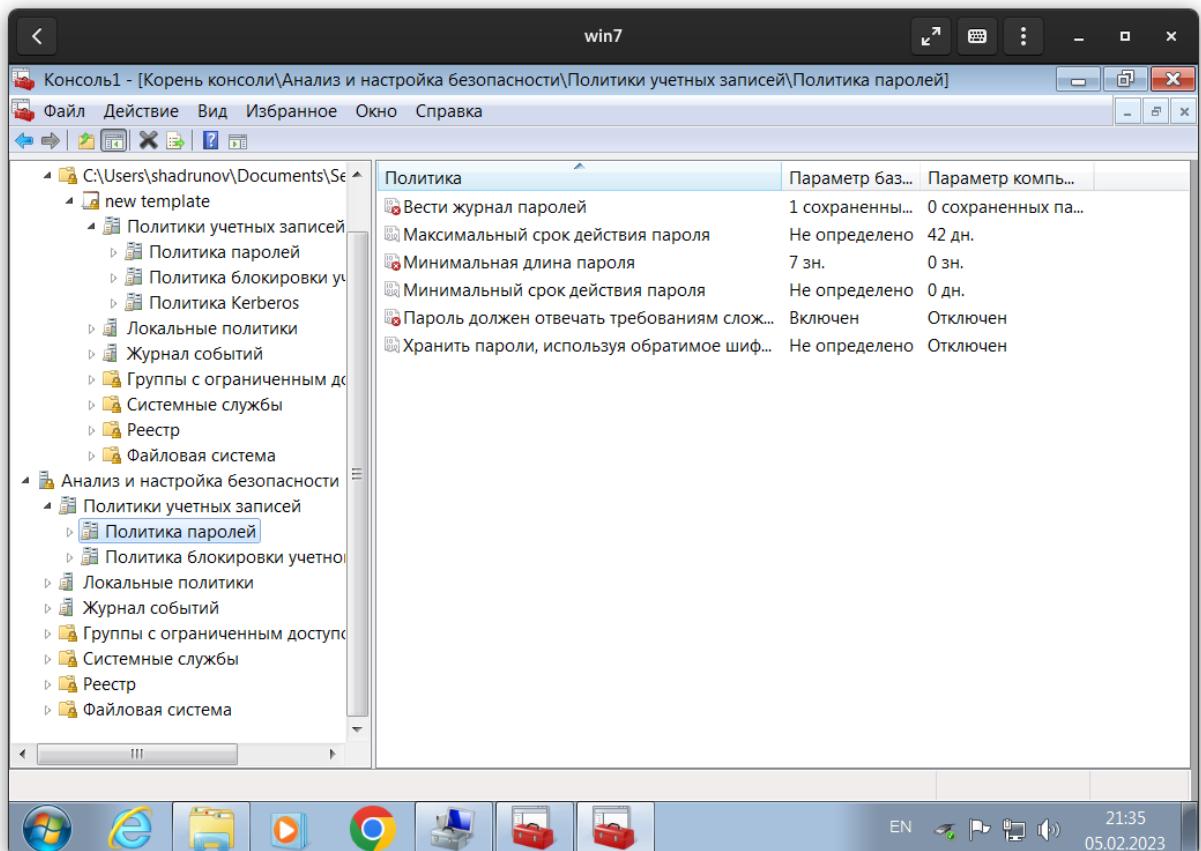


Рисунок 11 – Различия между шаблоном и текущей настройкой политики паролей

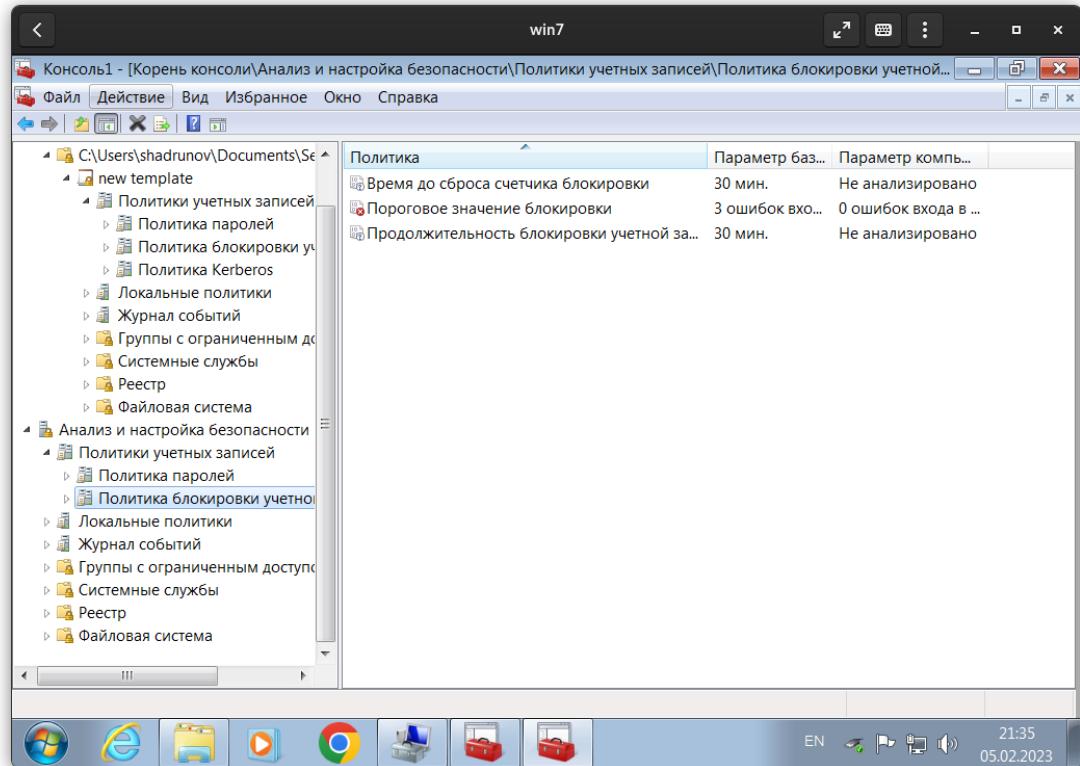


Рисунок 12 – Различия между шаблоном и текущей настройкой политики блокировки учётной записи

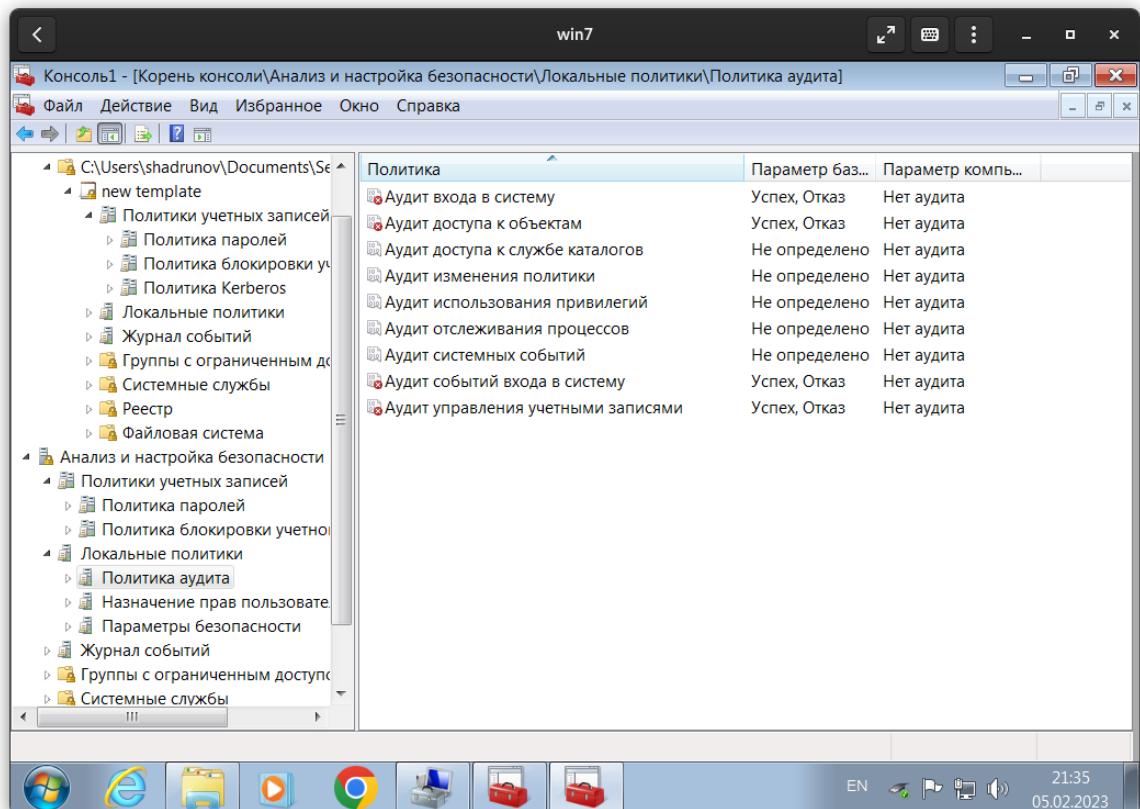


Рисунок 13 – Различия между шаблоном и текущей настройкой политики аудита

## 2.6 Настройка параметров безопасности по шаблону

Производим настройку параметров безопасности по заданному шаблону. Для этого нажимаем на Анализ и настройка безопасности и выбираем Настроить компьютер... (рисунок 14). После этого шаблон автоматически применяется к системе. На рисунке 15 видно, что различия между шаблоном и текущей настройкой исчезли.

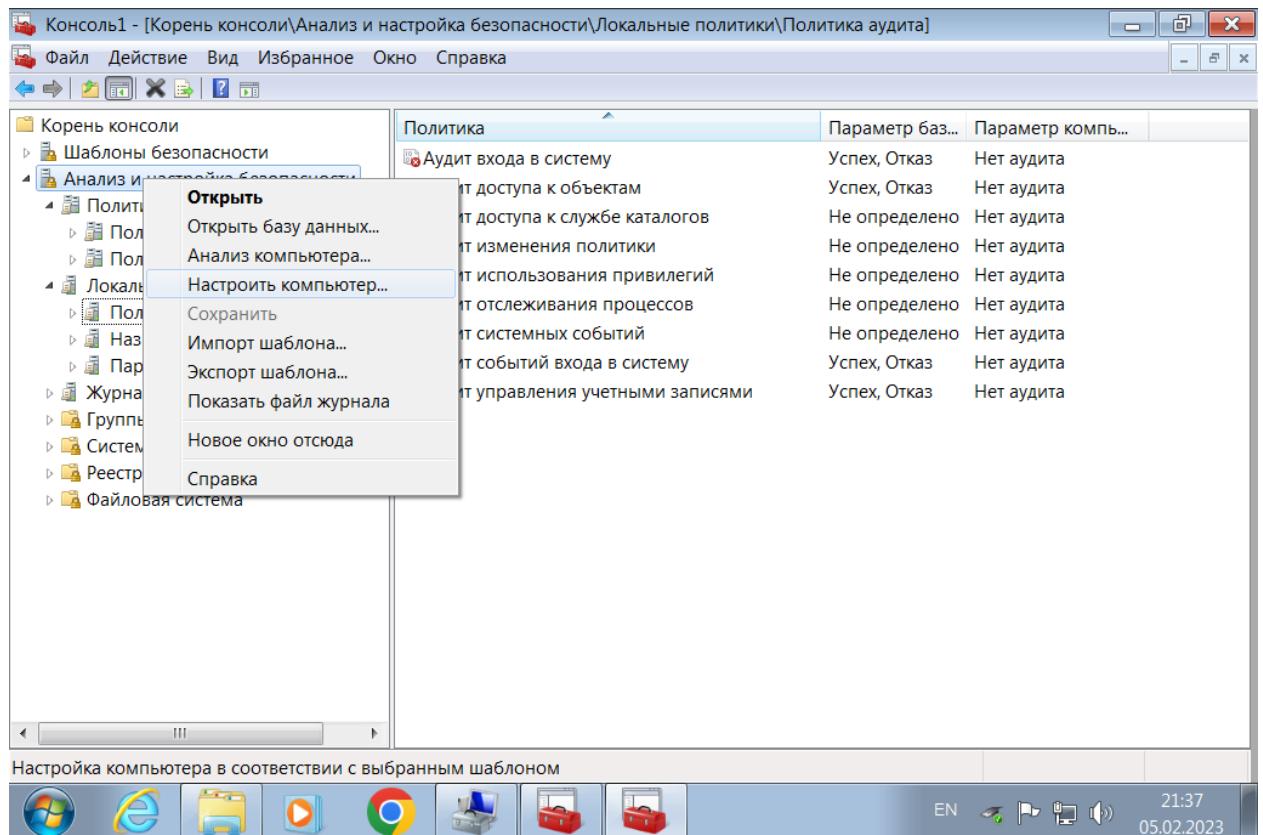


Рисунок 14 – Настроить компьютер...

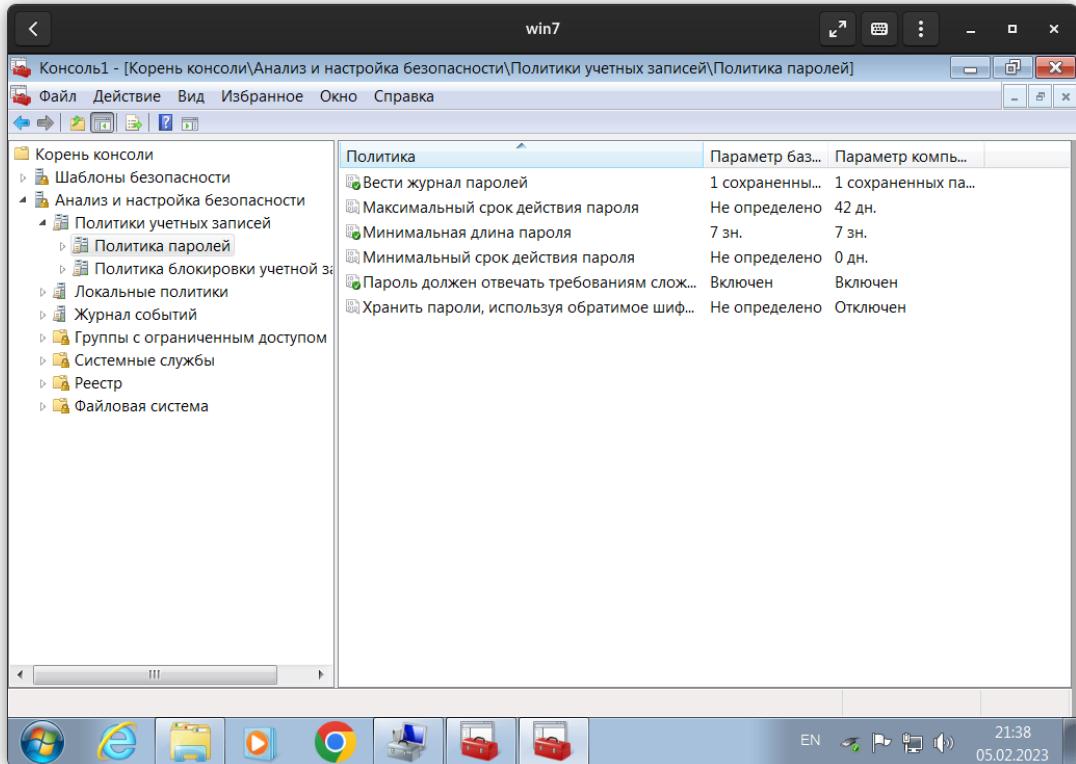


Рисунок 15 – Различия между шаблоном и текущей настройкой исчезли

## 2.7 Работа с журналом безопасности

Далее выполняем действия, влияющие на безопасность системы, и отслеживаем логи в соответствующем журнале аудита.

На рисунках 16-17 видно, что мы задаём пароль, удовлетворяющий требованиям локальной политики, а также запись об успешном доступе к учётной записи в журнале.

На рисунках 18-20 мы задаём пароль, не удовлетворяющий требованиям локальной политики (слишком короткий). Запись в журнале говорит о неудачной попытке изменения учётных данных (рисунок 20).

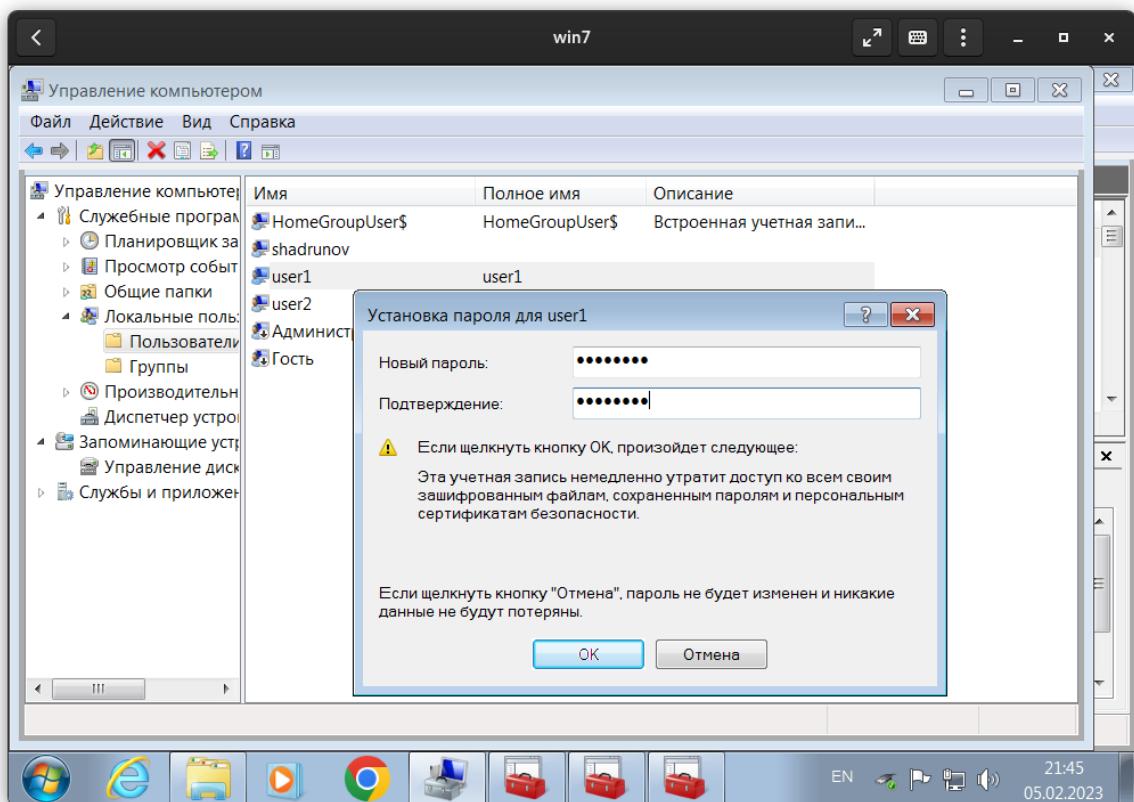


Рисунок 16 – Задаём безопасный пароль для user1

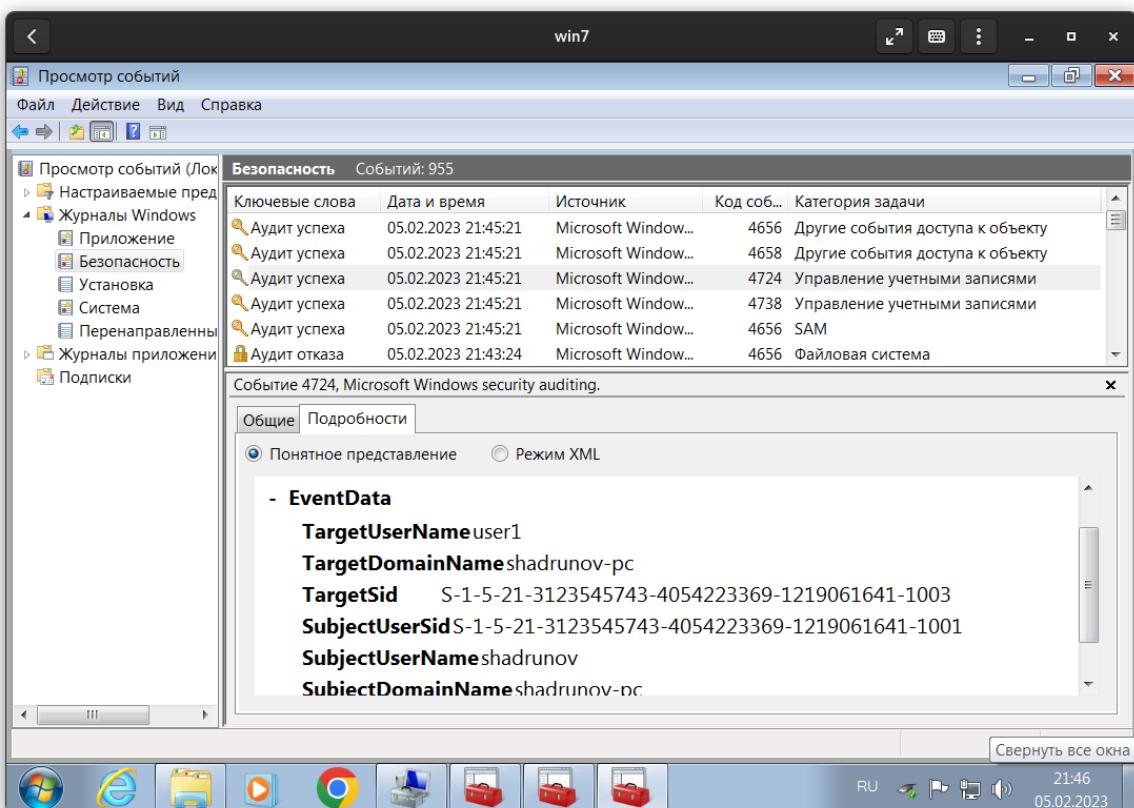


Рисунок 17 – Запись в журнале безопасности операционной системы

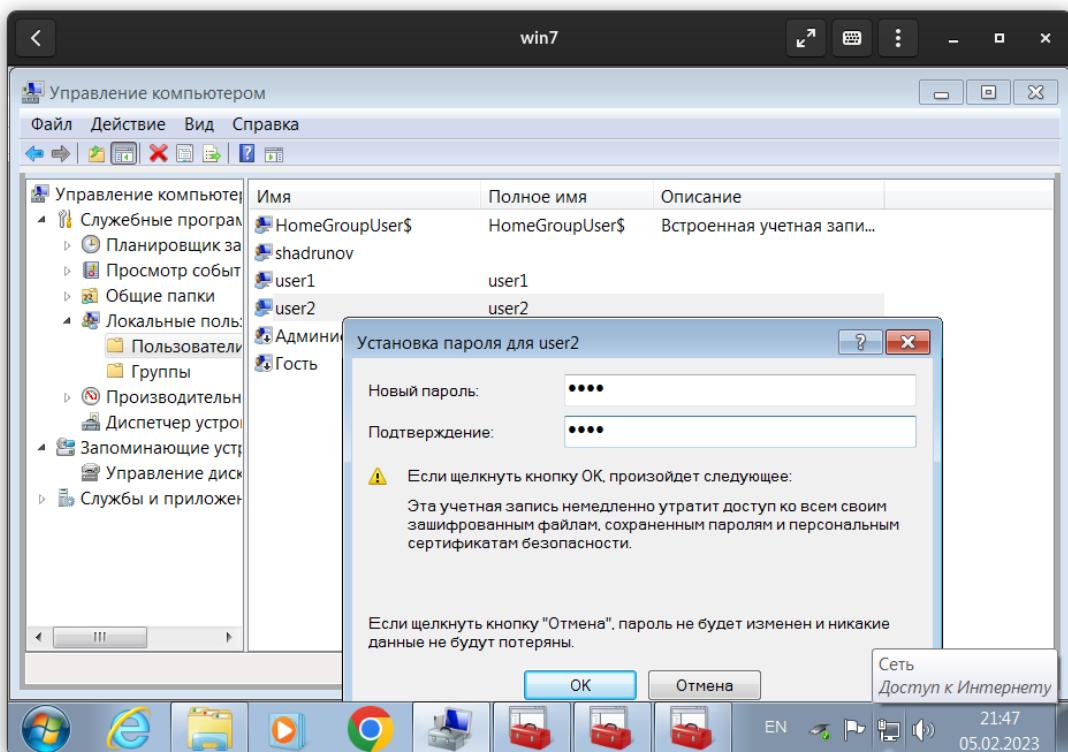


Рисунок 18 – Задаём небезопасный пароль для user2

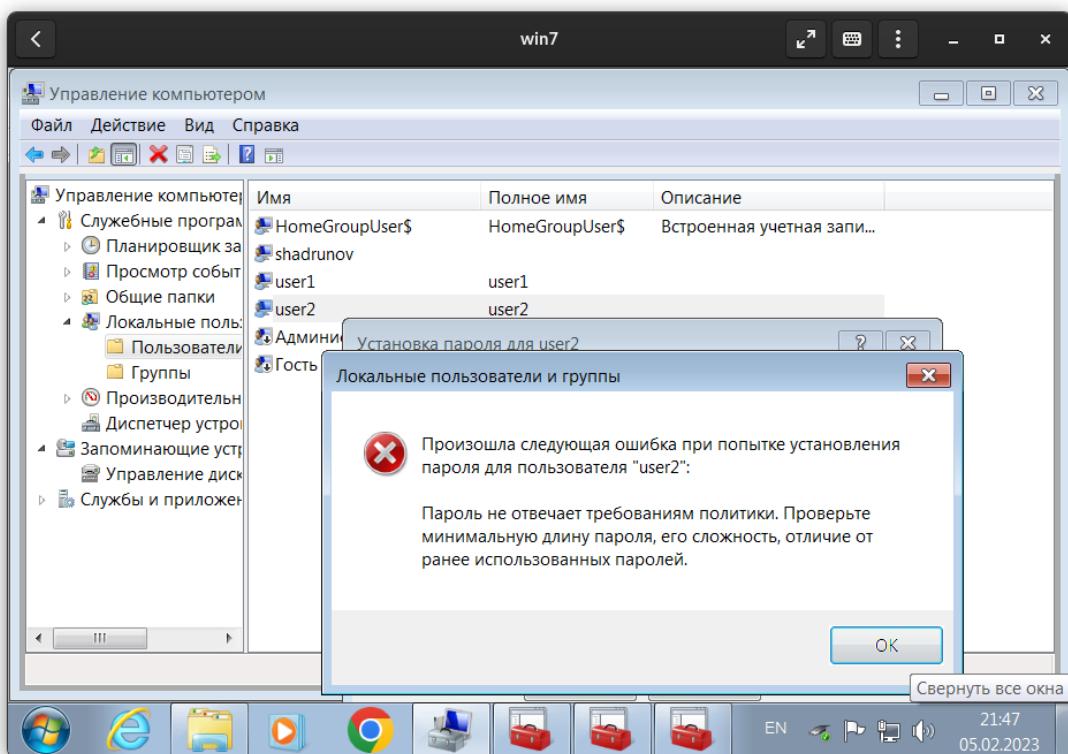


Рисунок 19 – Ошибка

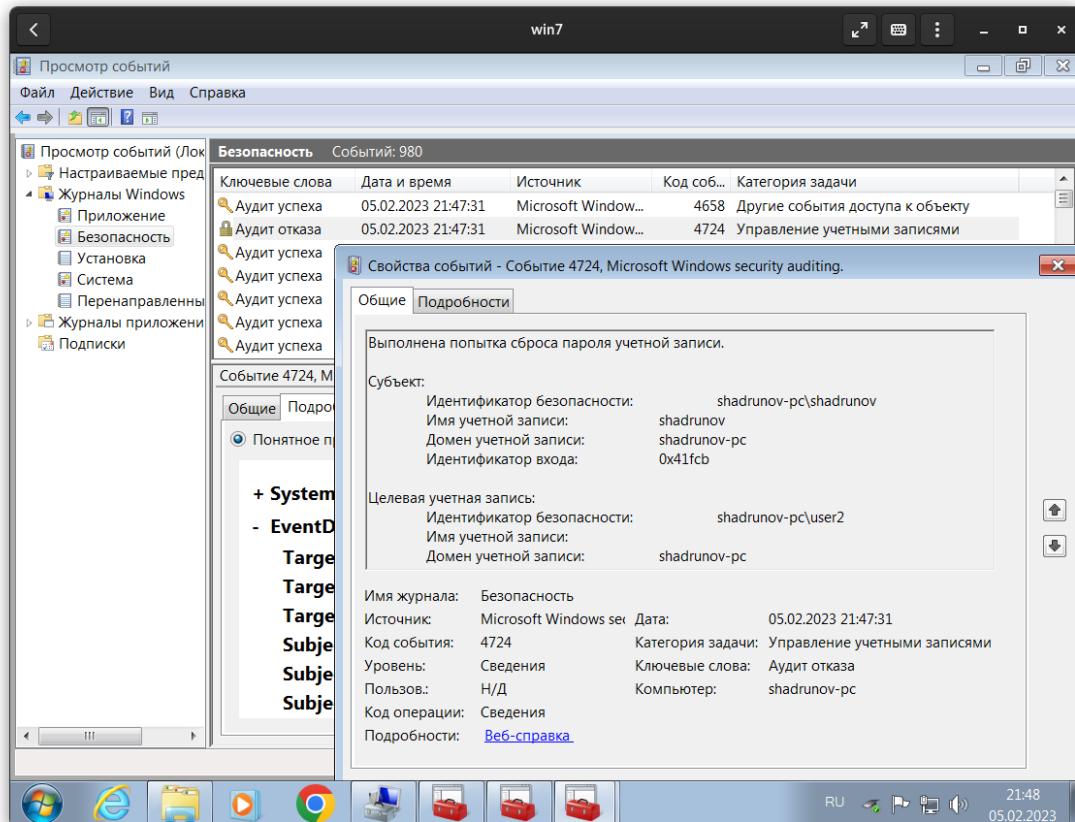


Рисунок 20 – Запись в журнале безопасности операционной системы

На рисунках 21-22 производим вход в систему под учетной записью пользователя user1 с ошибочными данными (неправильным паролем). Находим связанное с этим событие в журнале безопасности операционной системы.



Рисунок 21 – Указываем неверный пароль

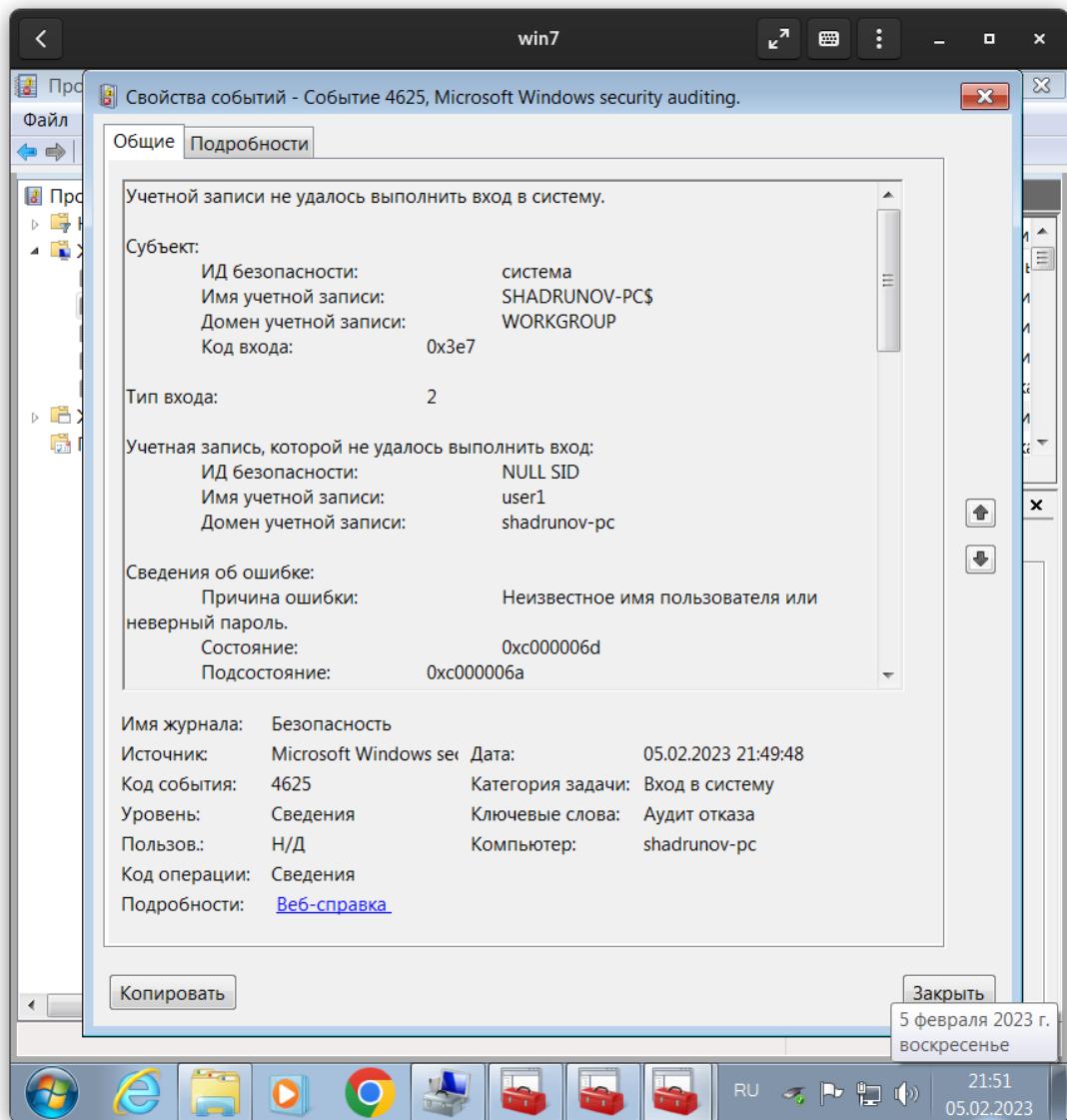


Рисунок 22 – Запись в журнале безопасности операционной системы

На рисунках 23-24 производим вход в систему под учетной записью пользователя user1 с верными данными. Находим связанное с этим событие в журнале безопасности операционной системы.

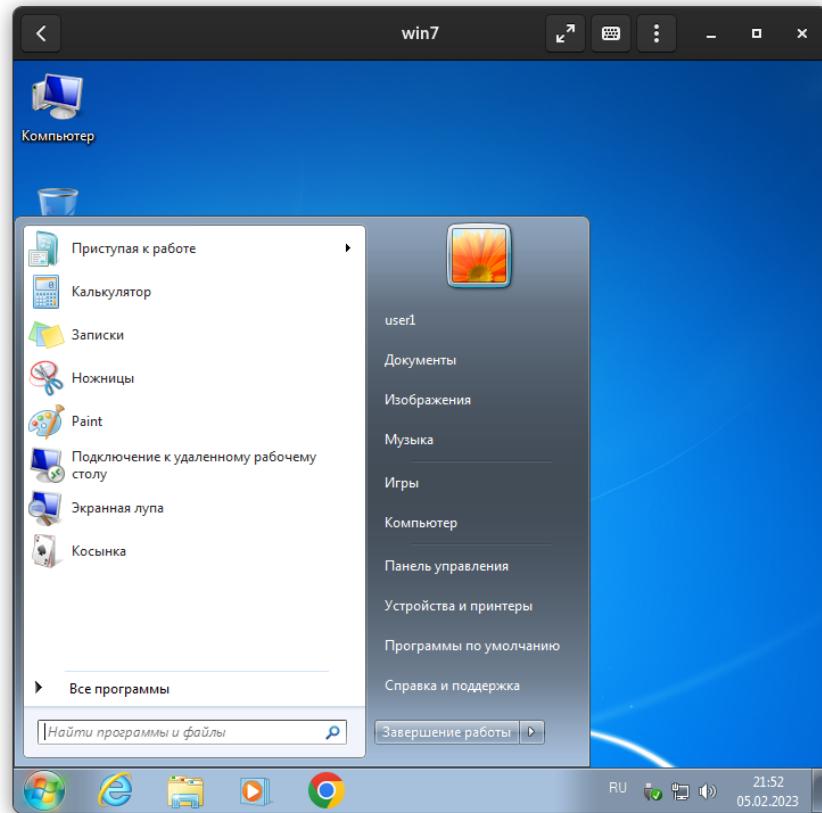


Рисунок 23 – Успешный вход под учетной записью пользователя user1

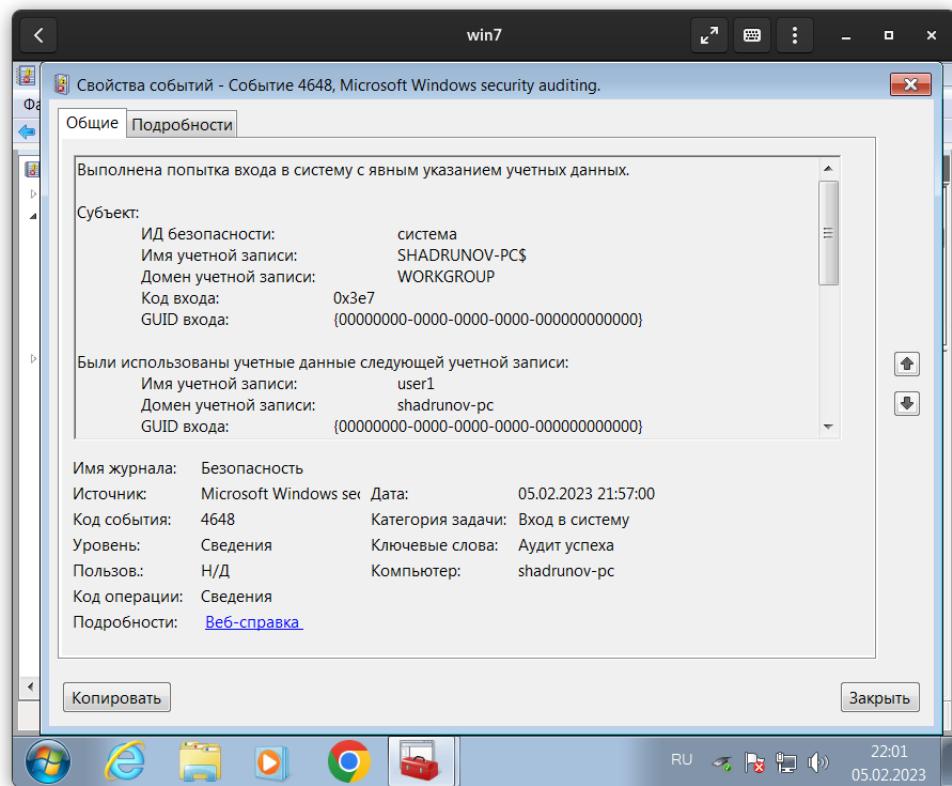


Рисунок 24 – Запись в журнале безопасности операционной системы

## 2.8 Брандмауэр Windows

Настраиваем правила в брандмауэре Windows по заданию (рисунки 25-13):

- запрет исходящего трафика для подключения к сайтам (html-страницам);
- запрет входящего трафика для удалённого подключения к рабочей станции по протоколу RDP (утилита mstsc)

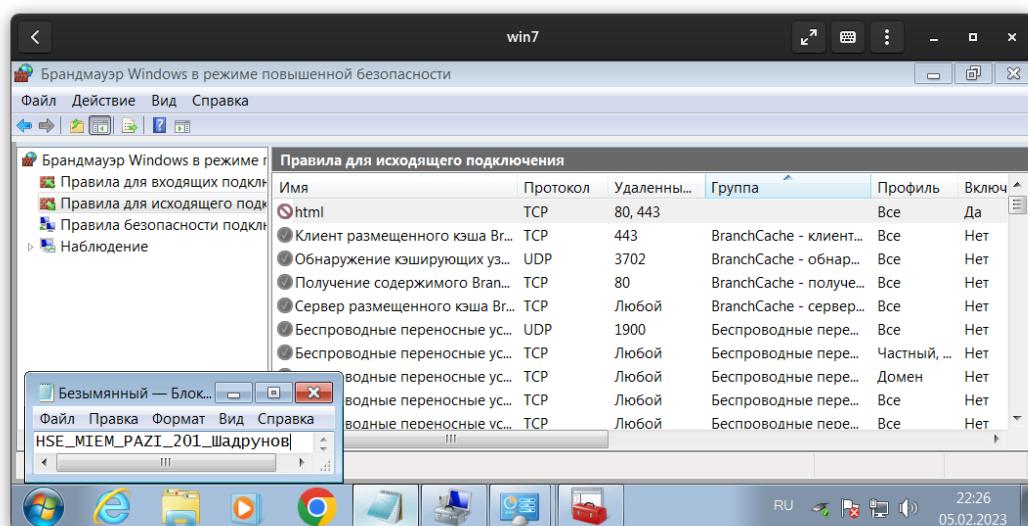


Рисунок 25 – Запрет html-страниц (порты 80 и 443)

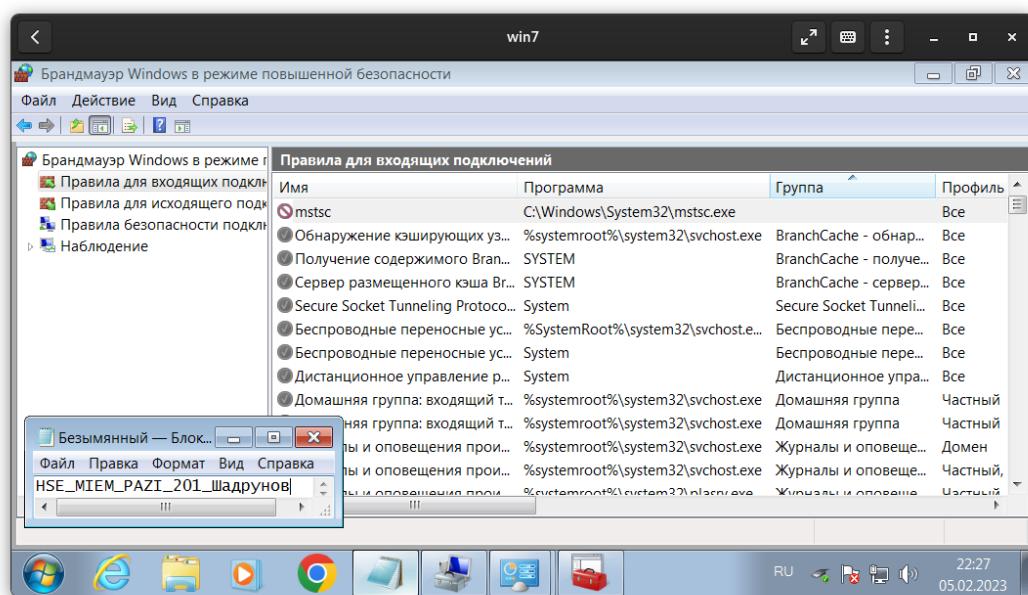


Рисунок 26 – Запрет RDP

Перед этим проверяем работу браузера и RDP (всё работает, рисунки 27-28).

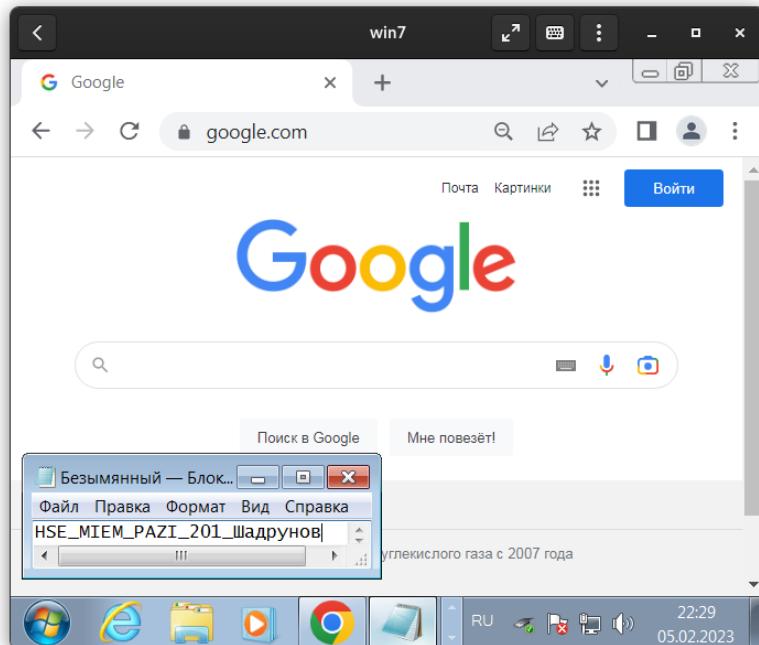


Рисунок 27 – Работа браузера (порт 443)

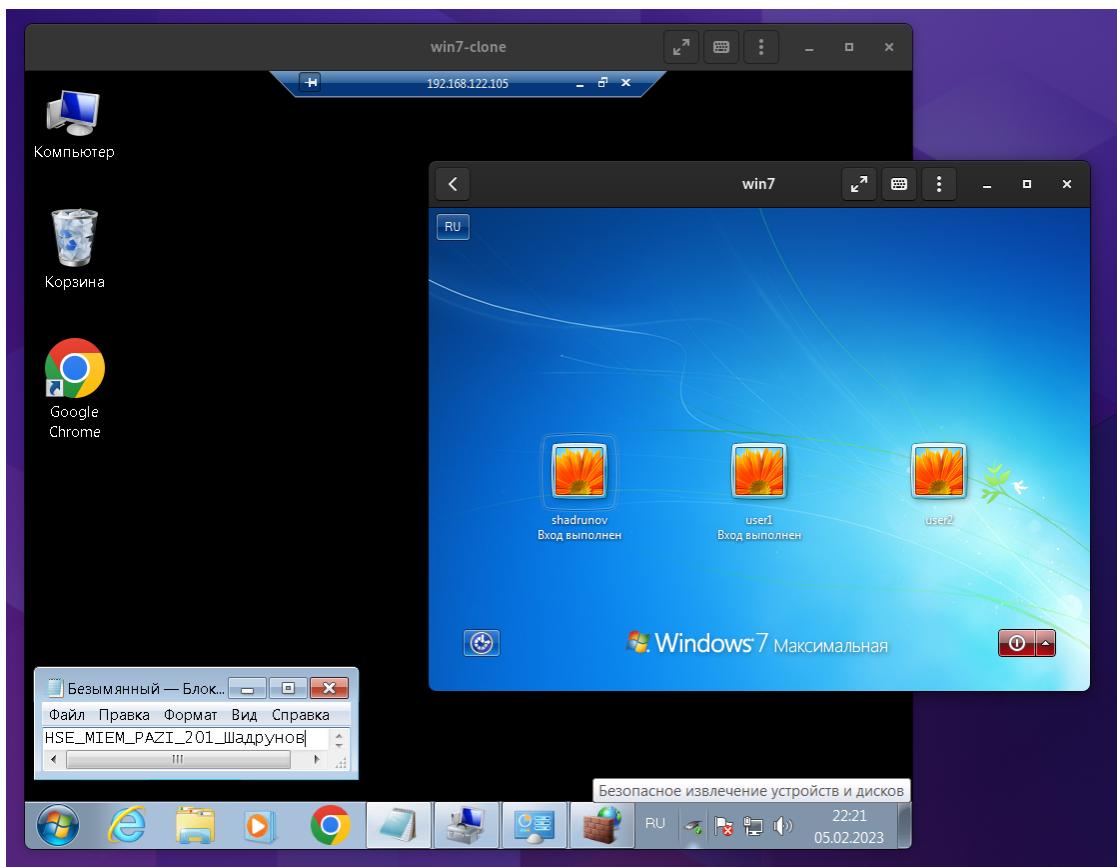


Рисунок 28 – Работа RDP-подключения к машине win7

После включения правил подключения нет (рисунки 29-30).

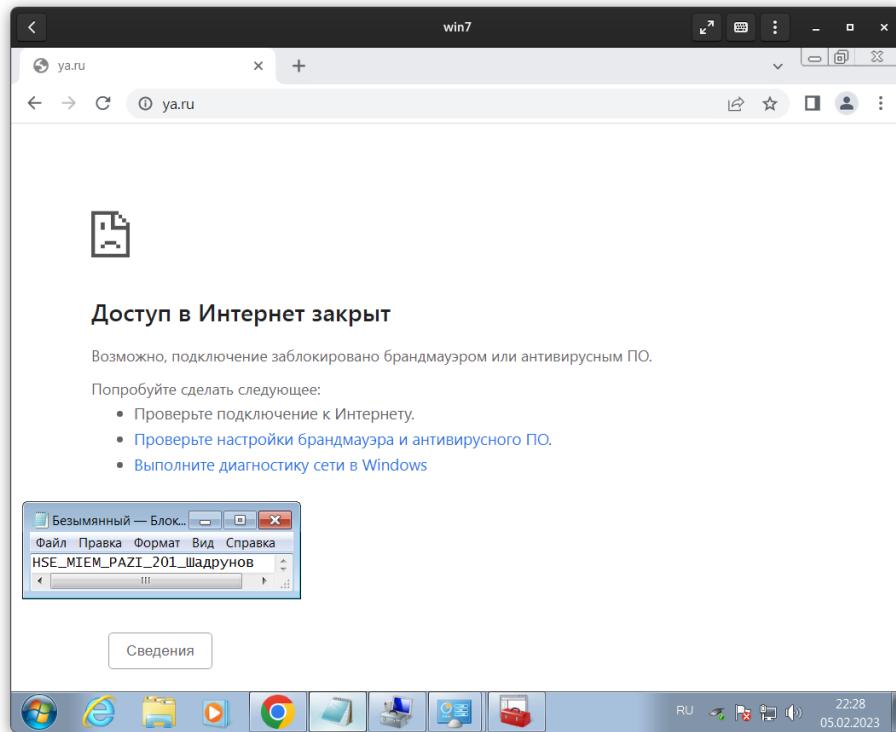


Рисунок 29 – Запрет html-страниц (порты 80 и 443)

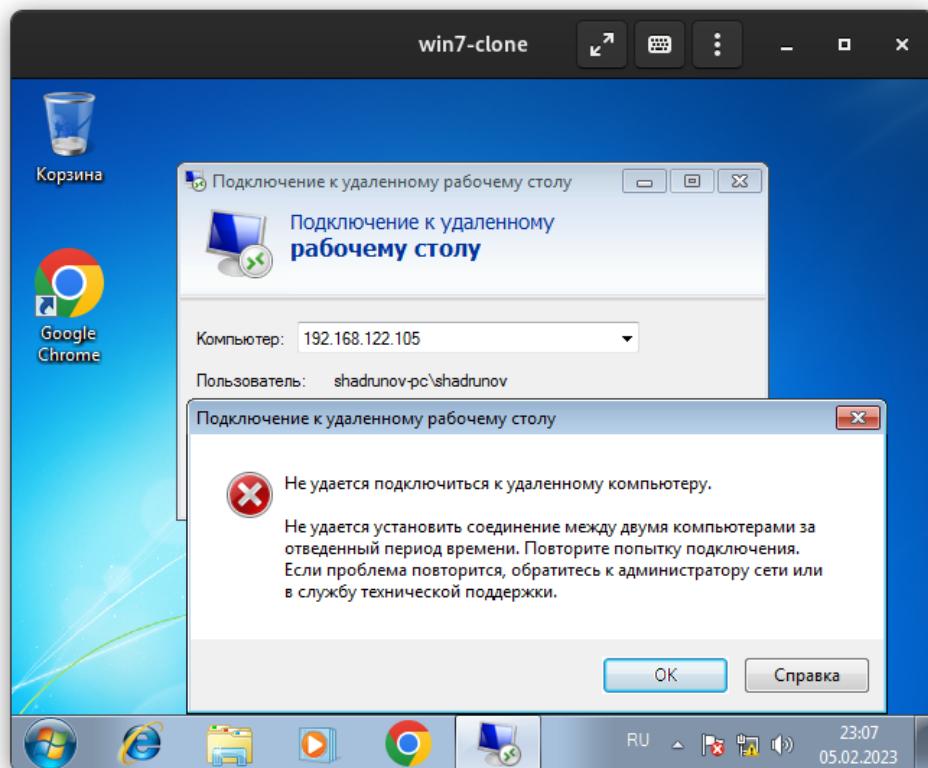


Рисунок 30 – Запрет RDP

## 2.9 UAC

Настраиваем параметры управления учетными записями пользователей на уведомление при любом изменении параметров компьютера (рисунок 31). После применения самой строгой настройки попытка изменить параметры компьютера вызывает уведомление и требует административный доступ к системе (рисунок 32).

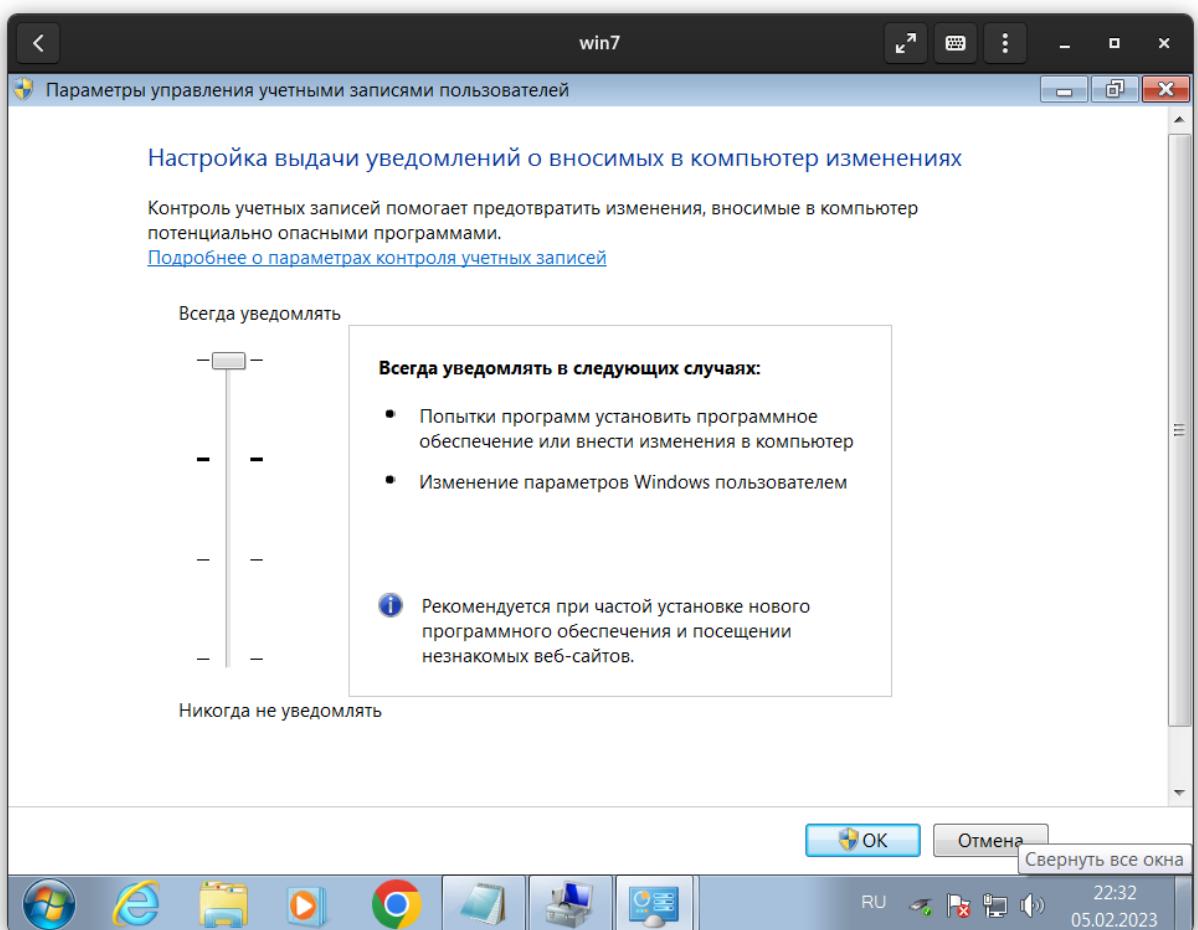


Рисунок 31 – Включение высокого уровня оповещений

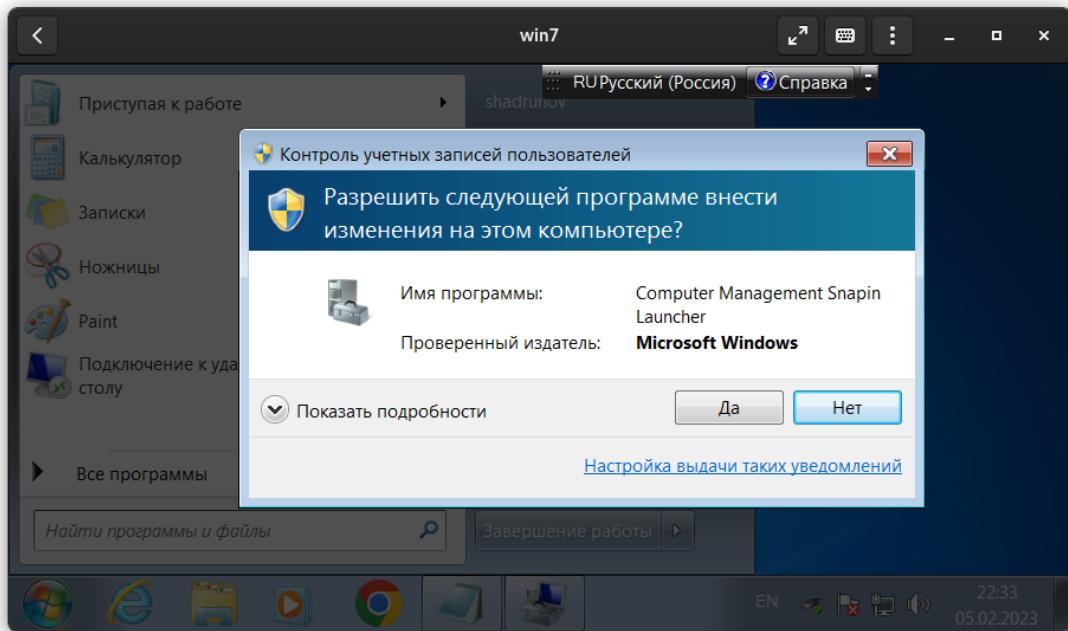


Рисунок 32 – Уведомление о внесении изменений в систему

## 2.10 Архивация и восстановление

С помощью инструмента «Архивация и восстановление» выполняем архивацию (резервное копирование) каталога с файлами lab (рисунок 33). Результат отображается в свойствах каталога (рисунок 34).

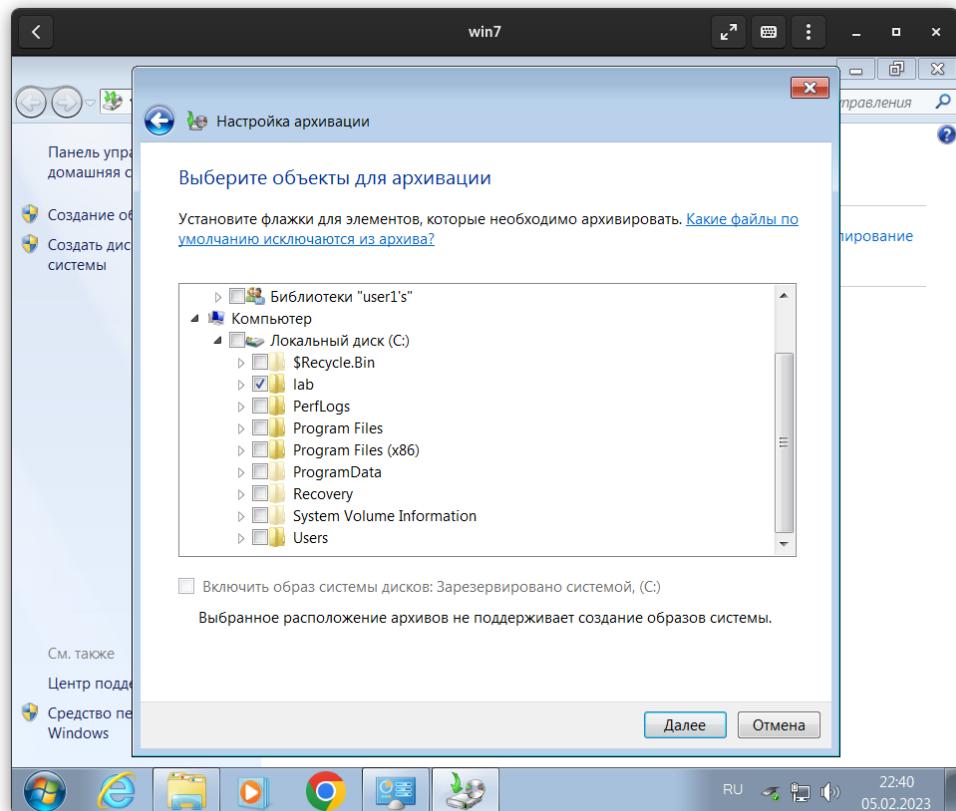


Рисунок 33 – Выбор папки для архивации

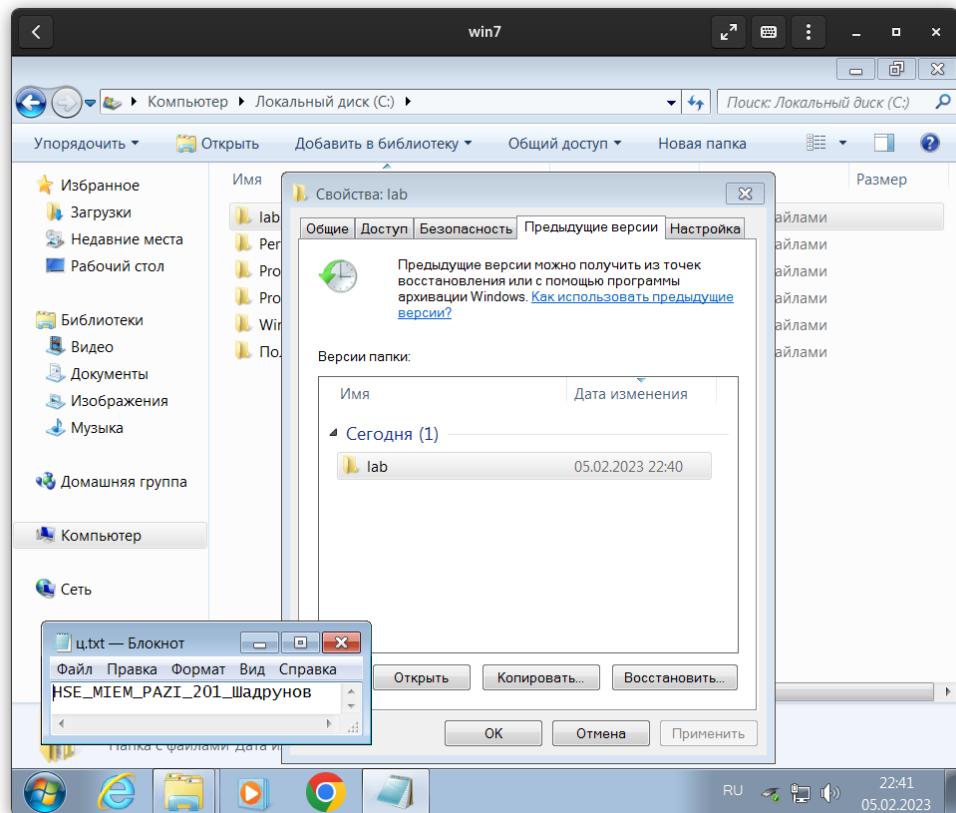


Рисунок 34 – Результат архивации

## 2.11 Защитник Windows

В качестве дополнительного средства защиты рассмотрен защитник Windows. Для начала требуется его включить (рисунок 35). Затем можно провести антивирусную проверку (рисунок 36).

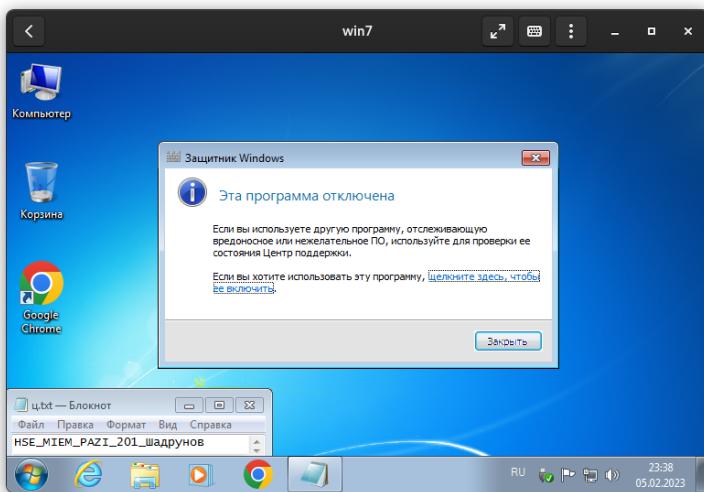


Рисунок 35 – Включение защитника

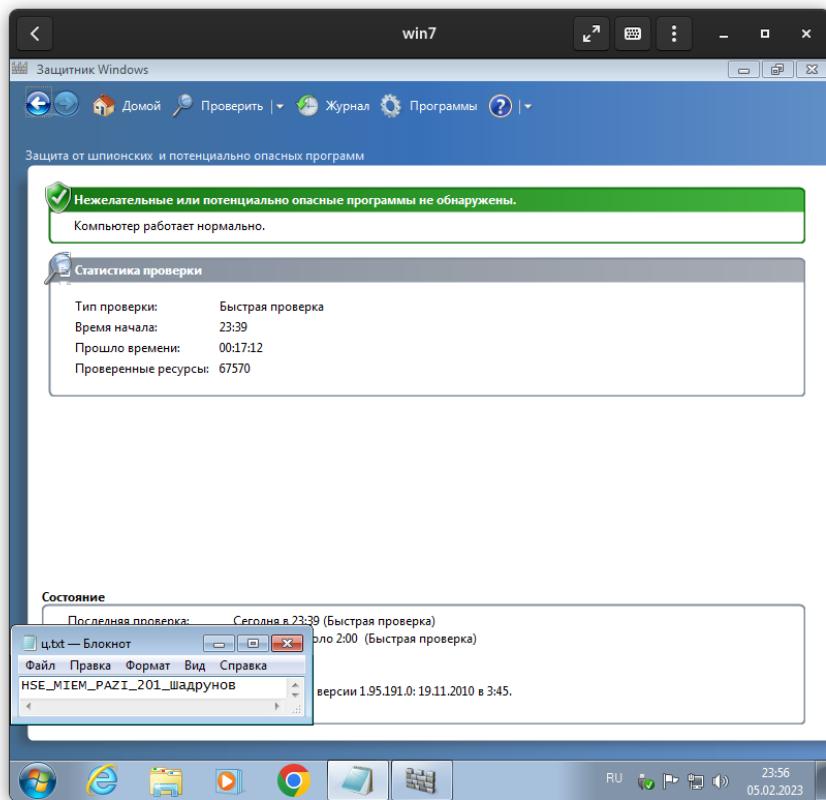


Рисунок 36 – Быстрая проверка

### **3 Выводы о проделанной работе**

В рамках данной работы я ознакомился с функциями безопасности Windows 7, улучшениями и приложениями, изучил брандмауэр Windows.