МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технологический университет «СТАНКИН»
(ФГБОУ ВО «МГТУ «СТАНКИН»)

Институт
информационных
технологий

Кафедра
Информационных систем

ОТЧЕТ О ВЫПОЛНЕНИИ ЛАБОРАТОРНОЙ РАБОТЫ № 2

ПО ДИСЦИПЛИНЕ

« Защита информации »

СТУДЕНТА 4 КУРСА бакалавриата ГРУППЫ ИДБ-20-02

Ердоган Дениз Ердалович

Тема: « Изучение программных средств защиты от несанкционированного доступа и разграничения прав пользователей »

Направление: 09.03.01 Информатика и вычислительная техника
Профиль подготовки: Информатика и вычислительная техника

Отчет сдан «_____»_____2023 г.

Оценка _____

Преподаватель _____Симонов М.Ф._____ _____.

МОСКВА 2023

1. Запустить программы просмотра и редактирования реестра Windows regedit.exe и regedt32.exe (с помощью команды «Выполнить» главного меню). Ознакомиться со структурой реестра, включить в отчет краткие сведения о содержании основных разделов реестра (HKEY_CURRENT_USER и HKEY_LOCAL_MACHINE). Включить в отчет сведения о различиях в функциональных возможностях изученных программ редактирования реестра. Включить в электронную версию отчета копии экранных форм, иллюстрирующих использование редакторов реестра. Примечание: в операционную систему Windows XP Professional включен один редактор реестра, который можно запустить с помощью любого из указанных выше имен:

Все низкоуровневые настройки *Windows* и настройки приложений хранятся в базе данных, называемой **реестром Windows**. В нем хранятся: настройки драйверов устройств, пользовательского интерфейса, ядра, пути к папкам, ярлыки меню *Пуск*, расположение установленных приложений, файлы DLL, значения программного обеспечения и информация об оборудовании. Представление информации в реестре организовано в виде распределения всех параметров по специальным папкам - **кустам**, с многочисленными вложениями - **ветками реестра**, в которых хранятся доступные для редактирования параметры - **ключи реестра**, каждый из которых способствует определенной функции *Windows*. Так например:

- - **HKEY_CURRENT_USER (HKCU)** - корневой каталог сведений конфигураций пользователя, который в настоящее время выполнил вход. Различные значения реестра в различных разделах реестра, расположенных в кусте *HKEY_CURRENT_USER*, управляют параметрами пользовательского уровня, такими как: установленные принтеры, обои рабочего стола, параметры отображения, переменные среды, раскладка клавиатуры, подключённые сетевые диски. Многие из параметров, которые вы настраиваете в различных апплетах на панели управления, хранятся в кусте реестра *HKEY_CURRENT_USER*;
- - **HKEY_LOCAL_MACHINE (HKLM)** – куст реестра, который содержит сведения о конфигурации, относящиеся к компьютеру для любого пользователя. Он включает в себя детали конфигурации: ОС *Windows*, установленного ПО, драйверов устройств, загрузки *Windows*, служб *Windows*, драйверов оборудования. Наиболее интересным является подраздел *Software*, который включает в себя настройки всех установленных в системе приложений.

В каждой новой версии *Windows* в реестре появляются все новые и новые ветки, отвечающие за различные тонкие и скрытые настройки. Однако, остаются и неизменные пути, такие как: автозапуск программ и служб, ветки хранения параметров установленных программ, ветки управления устройствами.

Программы уборки реестра позволяют любому пользователю с определенной степенью безопасности найти и удалить неиспользуемые ветки, которые потенциально могут тормозить работу компьютера. Суть безопасности в том, что пользователь не правит реестр напрямую, а значит, теоретически не может повредить важные и нужные разделы.

Существуют стандартные утилиты операционных систем семейства *Windows*, которые предоставляют пользователю доступ к многочисленным служебным файлам в графическом режиме. Так существуют: *regedit* (“registry editor”). и *regedt32***.** Они предназначены для изменения настроек и конфигураций реестра.

- **Regedit** - является стандартным редактором реестра, доступным в операционной системе *Windows NT 4.0* и более поздних версиях, таких как *Windows 2000, Windows XP, Windows 7, Windows 8*. Основные функции, которых нет в *regedit32*:
  1. Поиск (на соответствие некоторой текстовой строке) разделов, имен параметров и содержимого параметров;
  2. Использование привычного двухпанельного интерфейса в стиле Проводника *Windows*, помогающего сравнить взаимное расположение двух разделов или параметров. Он содержит и другие возможности в стиле Проводника *Windows*, такие как контекстные меню, редактирование прямо на месте и удобное управление деревом;
  3. Импорт и экспорт нужных разделов (и нижележащих в них элементов данных) в пригодные для чтения людьми текстовые файлы, а не только импорт и экспорт разделов в двоичном виде;
  4. В версии для *Windows XP* имеется меню *Favorites* в которое вы можете добавлять разделы, которые будут, по вашему мнению, редактироваться часто.

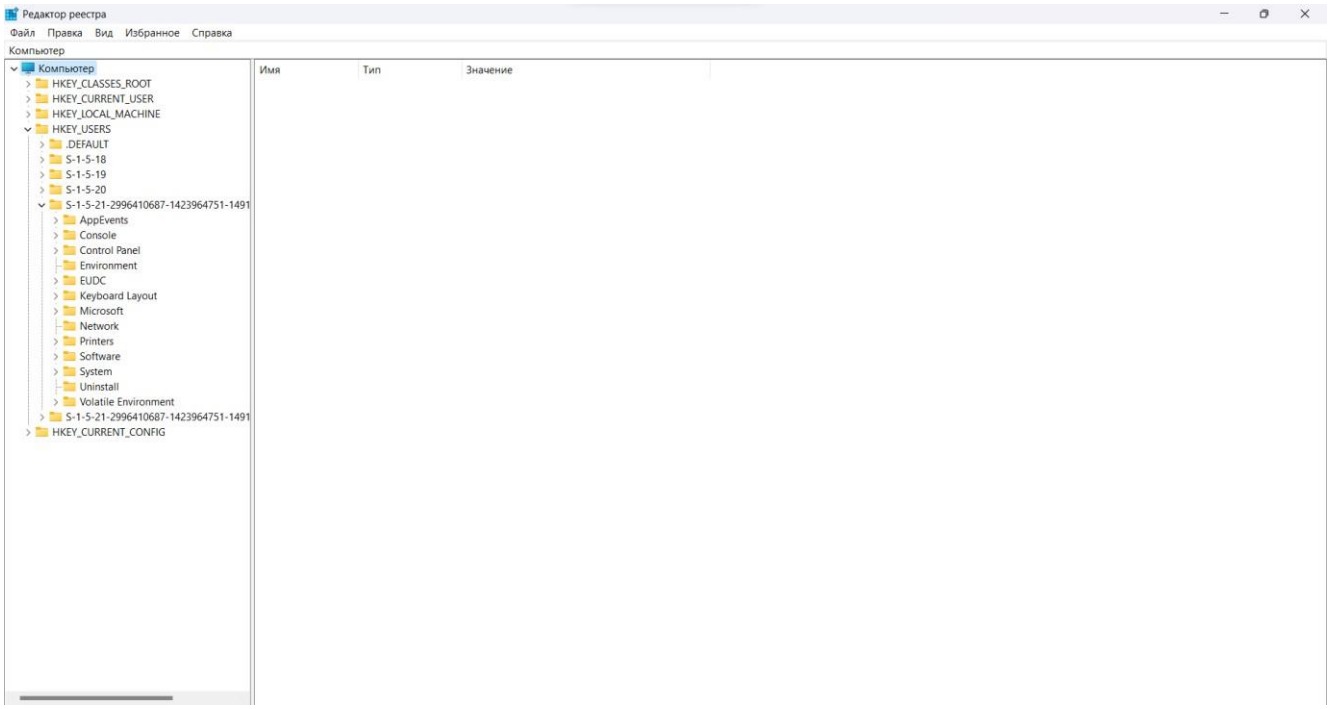

Рисунок № 2 – regedit.exe (Windows 11)

- **Regedit32** - был введен в операционной системе *Windows NT 3.51*, и продолжал использоваться в *Windows NT 4.0*. В более поздних версиях *Windows*, *Regedit32* был заменен на *Regedit*, однако, для обратной совместимости оставленный как программный инструмент. *Regedit32* обладает более продвинутыми функциями по сравнению с *Regedit*. А именно:
  - Редактирование защищенных системных разделов. *Regedit32* позволяет изменять значения ключей реестра, которые защищены в *Regedit*, и предоставляет доступ к разделам, которые недоступны в *Regedit*;
  - Создание разделов. *Regedit32* позволяет создавать новые подразделы ключа реестра, в то время как в *Regedit* можно только создавать, удалять и изменять значения ключей, но не создавать новые разделы;
  - Импорт и экспорт ключей реестра. *Regedit32* предоставляет возможность импорта и экспорта ключей реестра в файлы *.reg*, что позволяет сохранять конфигурации реестра и восстанавливать их при необходимости. Эта функция отсутствует в *Regedit*;
  - Установка разрешений доступа. *Regedit32* позволяет устанавливать и изменять разрешения доступа к разделам ключей реестра, что

позволяет настраивать права доступа для пользователей или групп пользователей. Эту функцию нельзя выполнить в *Regedit*.

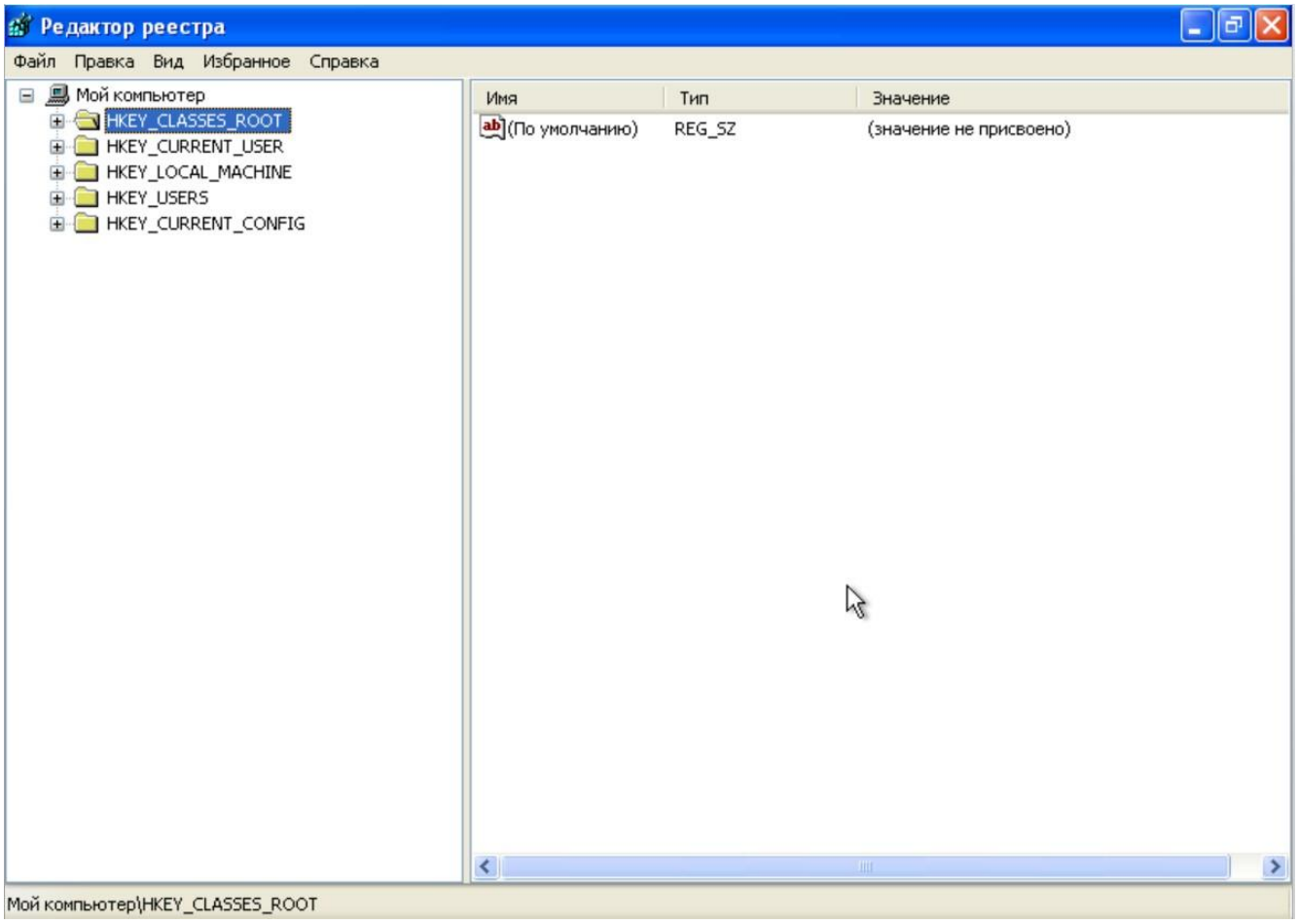

Рисунок № 2 – regedit32.exe (Windows XP)

Общие возможности:

1. Просматривать в графическом виде древовидную иерархическую структуру;
2. Просматривать и изменять разделы, подразделы, параметры и значения параметров (в соответствии с имеющимися у вас полномочиями доступа);
3. Соединяться с удаленным компьютером (для доступа к которому у вас имеются полномочия) и проверять или даже изменять содержимое Реестра.

2. Скопировать в произвольную папку на диске рабочей станции файл rt.zip из указанного преподавателем сетевого диска;

3. Извлечь файлы из скопированного в пункте 2 архива;

4. Запустить программу restrick.exe, позволяющую ограничить возможности пользователей ОС Windows. Включить в отчет сведения о назначении и основных функциях программы. С помощью редактора реестра найти и отразить в отчете разделы реестра Windows, хранящие информацию о выбранной политике безопасности. Включить в отчет ответ на вопрос, какое ограничение на работу пользователя должно быть обязательно установлено, чтобы обеспечить минимальную эффективность рассмотренных и аналогичных средств. Включить в электронную версию отчета копии экранных форм, используемых при работе с программой restrick.exe. Завершить работу с программой restrick.exe:

Выше было упомянуто, что существуют программы с удобными интерфейсами для работы с реестром. Примером такой программы является *RESTrick*. Панель управления **RESTrick** - функциональная утилита для настройки среды *Windows* и повышения безопасности работы в *Windows*. Это приложение является апплетом. С его помощью можно: определить опции загрузки системы, задать перечень иконок, которые будут отображаться на рабочем столе, запретить запуск определенных приложений, предотвратить изменение системных настроек.

Функции *RESTrick* вкладки *Explorer* (обозреватель):

- *Restrict "Run program" window* - скрывает кнопку "*Выполнить*" из меню "*Пуск*";
- *Restrict "Run" command* - запрещает запуск программ, которые не являются разрешёнными;
- *Restrict "Find" window* - скрывает кнопку "*Поиск*" из меню "*Пуск*";
- *Restrict "Exit Windows" command* – запрещает завершать работу *Windows*;
- *Restrict folder "Control panel" and folder "Printers"* – скрывает раздел "*Панель управление*" и "*Принтеры*";
- *Restrict Task Bar settings and "Start" mouse right click* – запрещает вызывать контекстное меню нажатием правой кнопкой мыши и запускать программы при помощи пункта "*Запустить*";
- *Hide desktop shortcuts and disabled copying at desktop* - скрывает все значки с рабочего стола и запрещает копирование на рабочий стол;
- *Restrict "Delete Printer"* – запрещает удалять принтер;
- *Restrict "Add Printer"* – запрещает добавлять принтер;

- *Hide floppys at "My computer"* – скрывает внешние диски устройства;
- *Hide all folders at "My computer"* - скрывает все подразделы раздела "*Мой компьютер*";
- *Restrict to run old Win applications. In particular – DOS based* – запрещает запускать старые приложения, в частности, на основе *DOS*.

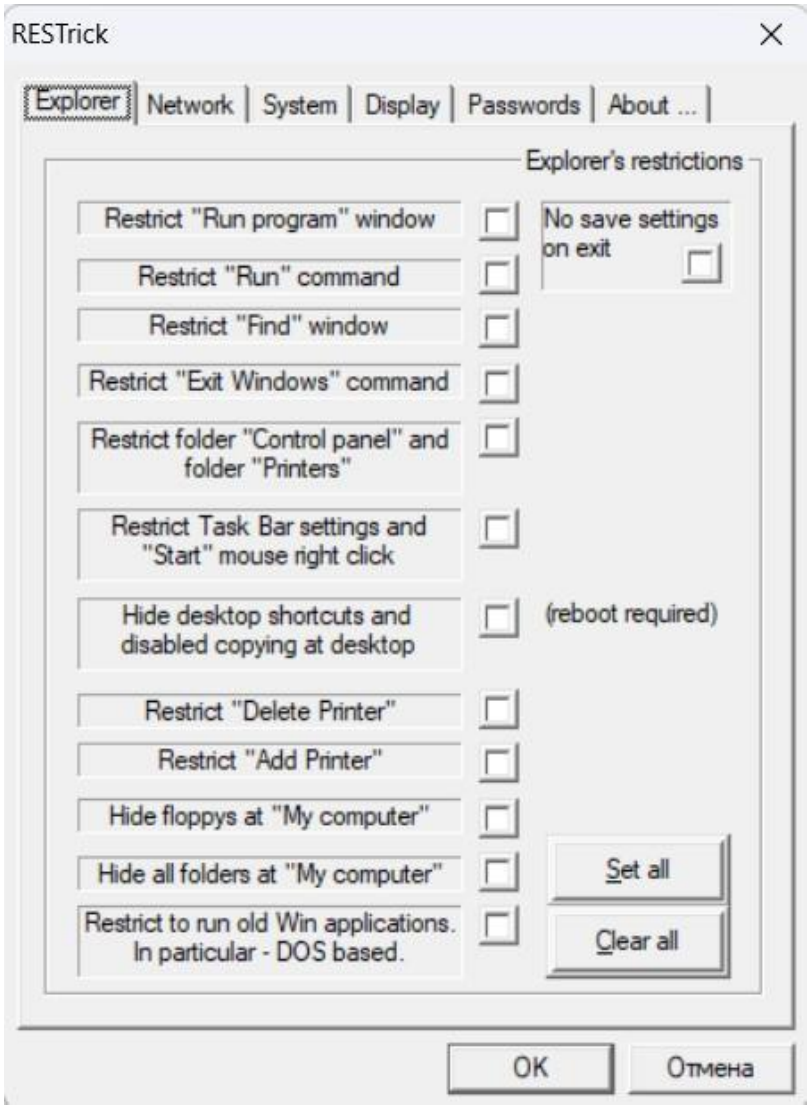

Рисунок № 3 – RESTrick (Explorer)

Функции *RESTrick* вкладки *Network* (сеть):

- *Restrict "Computer" property page* – скрывает раздел "*Компьютер*";
- *Restrict "Access manage" property page* - скрывает раздел "*Управление доступом*";
- *Restrict "Net properties"* - скрывает раздел "*Настройки сети*";
- *Restrict "Access to files' button* - скрывает раздел "*Доступ к файлам*";

- *Restrict "Access to printer" button* - скрывает раздел "*Доступ к принтерам*";
- *Restrict Net Setup* – запрещает настраивать сетевые параметры;
- *No "Network Neigbourhood"* – скрывает раздел "*Сетевые устройства*".

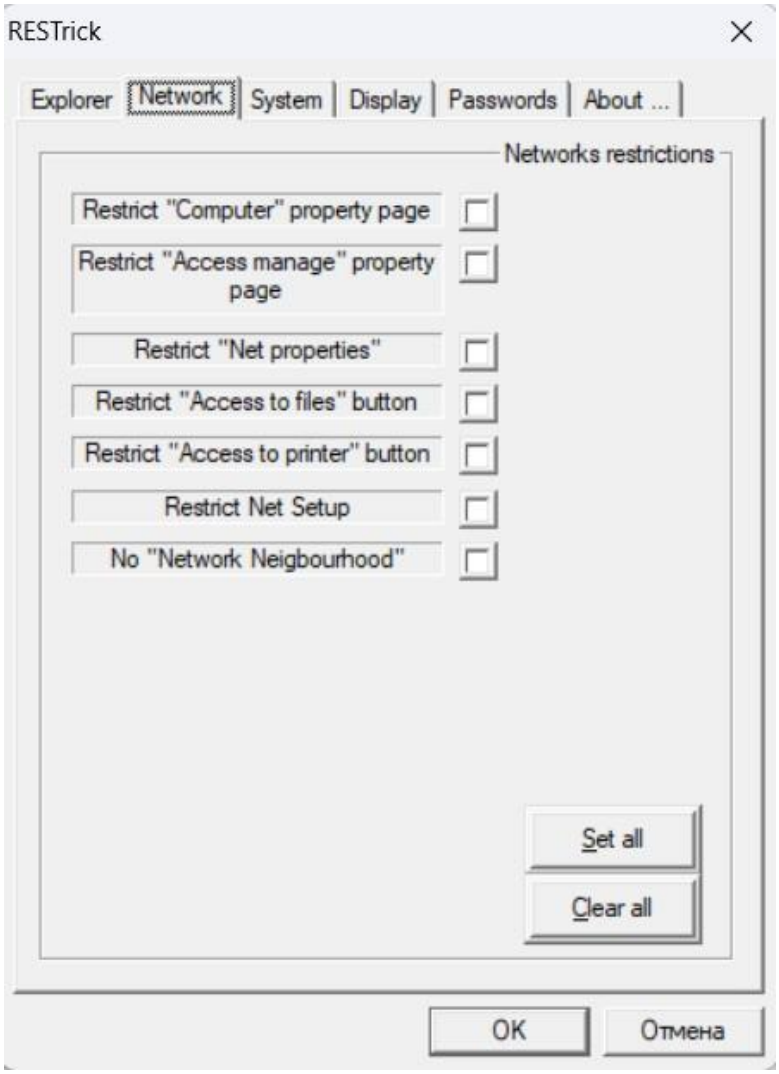

Рисунок № 4 – RESTrick (Network)

Функции *RESTrick* вкладки System (система):

- *Restrict "System: Devices" property page* - скрывает подпункт "*Устройства*" в разделе "*Система*";
- *Restrict "System: Configurations" property page* - скрывает подпункт "*Настройки*" в разделе "*Система*";
- *Restrict "System: File system" button* – скрывает раздел "*Системные файлы*";

- *Restrict "System: Virtual memory" button* – скрывает раздел "*Виртуальная память*";
- *Restrict "Power: Disks" property page* – скрывает подпункт "*Диски*" в разделе "*Система*";
- *Restrict to run Registry editor* – запрещает обращаться к редактору реестра;
- *Disable Task Manager (NT stuff)* – запрещает обращаться к менеджеру задач (в системе *NT*).

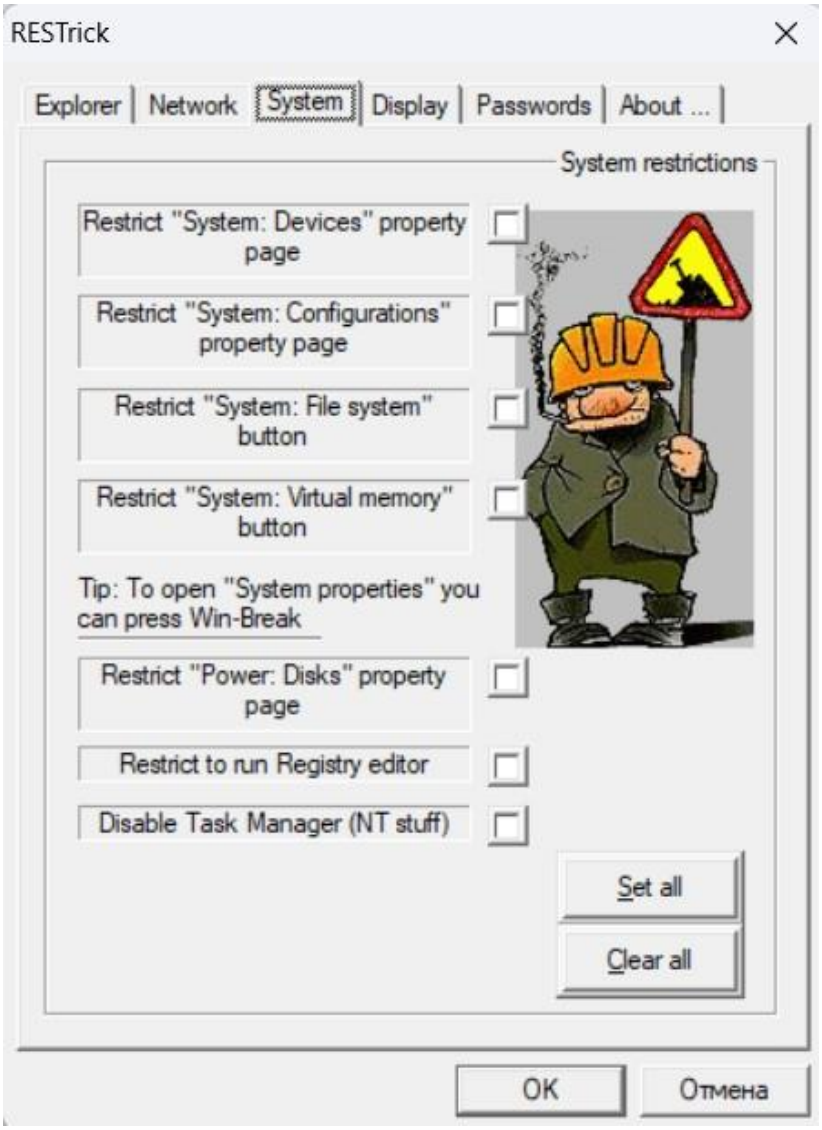

Рисунок № 5 – RESTrick (System)

Функции *RESTrick* вкладки *Display* (отображение):

- *Restrict "Display: Parameters" property page* - скрывает подпункт "*Параметры*" в разделе "*Экран*";

- *Restrict "Display: Background" property page* - скрывает подпункт "*Фон*" в разделе "*Экран*";
- *Restrict "Display: Screen Saver" property page* - скрывает подпункт "*Заставка*" в разделе "*Экран*";
- *Restrict "Display: Appearance" property page* – скрывает подпункт "*Внешний вид*" в разделе "*Экран*";
- *Restrict "Display" properties* – скрывает раздел "*Экран*".

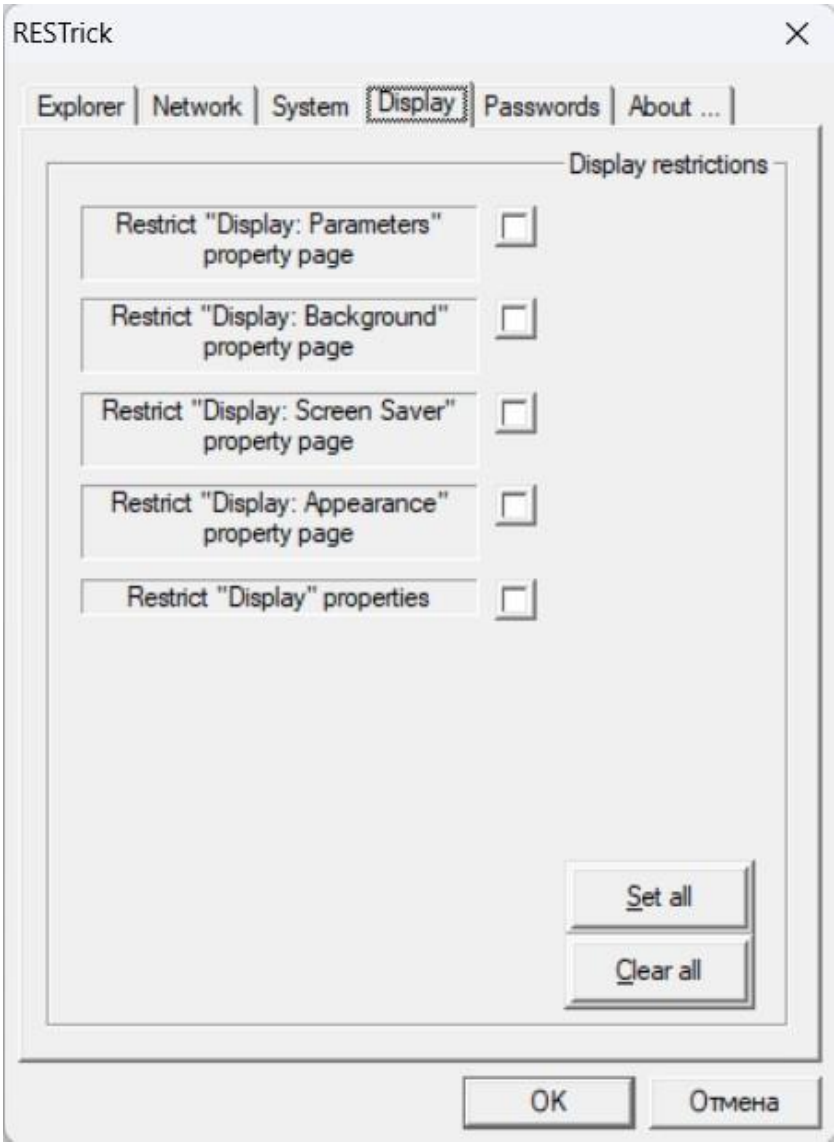

Рисунок № 6 – RESTrick (Display)

Функции *RESTrick* вкладки *Passwords* (пароли):

- *Restrict "Passwords: Change passwords" property page* - скрывает подпункт "*Изменить пароль*" в разделе "*Пароли*";

- *Restrict "Passwords: Remote manage" property page* - скрывает подпункт "*Удалённое управление*" в разделе "*Пароли*";
- *Restrict "Passwords: Configurations" property page* – скрывает подпункт "*Конфигурация*" в разделе "*Пароли*";
- *Restrict "Passwords" properties* – запрещает изменение настроек паролей.

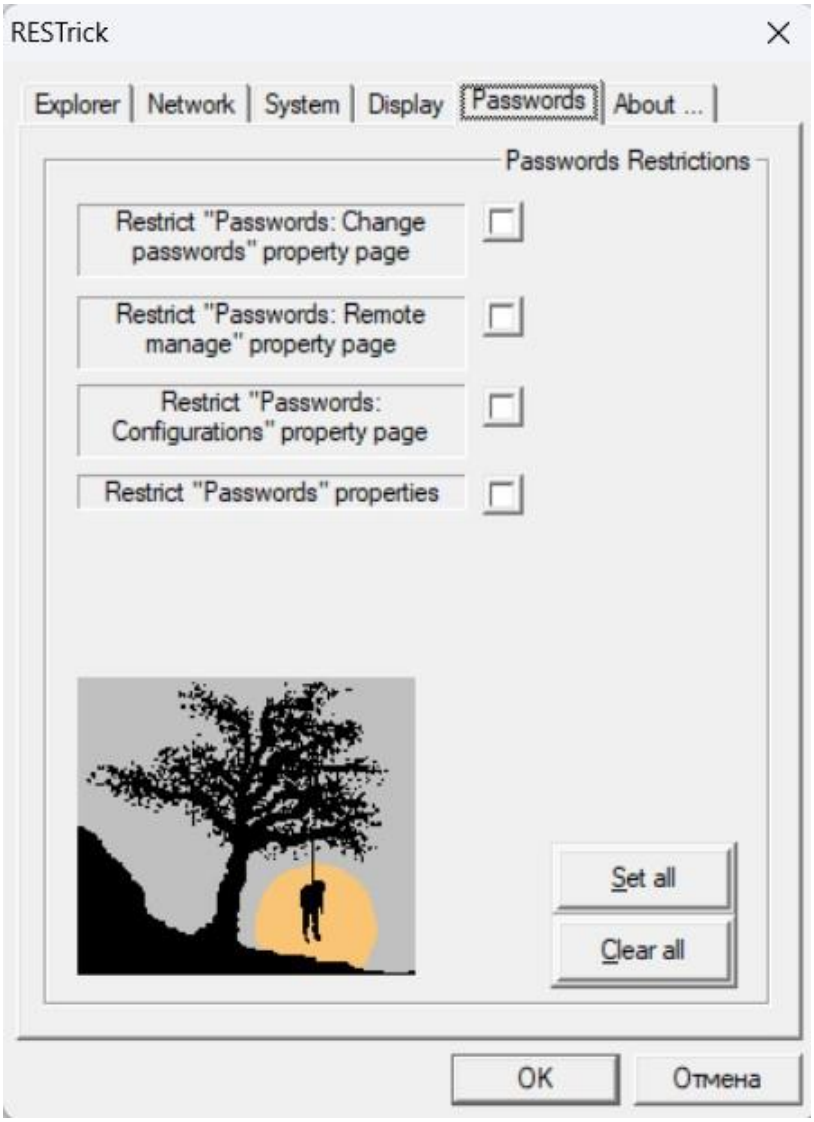

Рисунок № 7 – RESTrick (Passwords)

В операционных системах семейства *Windows* присутствует множество оснасток и политик, представляющих собой набор параметров для настройки различных функциональных составляющих ОС. Среди них находится оснастка под названием «*Локальная политика безопасности*». Она отвечает за редактирование защитных механизмов *Windows*.

Так в *Windows XP* политика безопасности находится в разделе ***HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\ (Explorere* “**Проводник**”, *Network* “**Сеть**”, *System* “**Система**”, *WinOldApp* “**Старые приложения Windows**”**):**

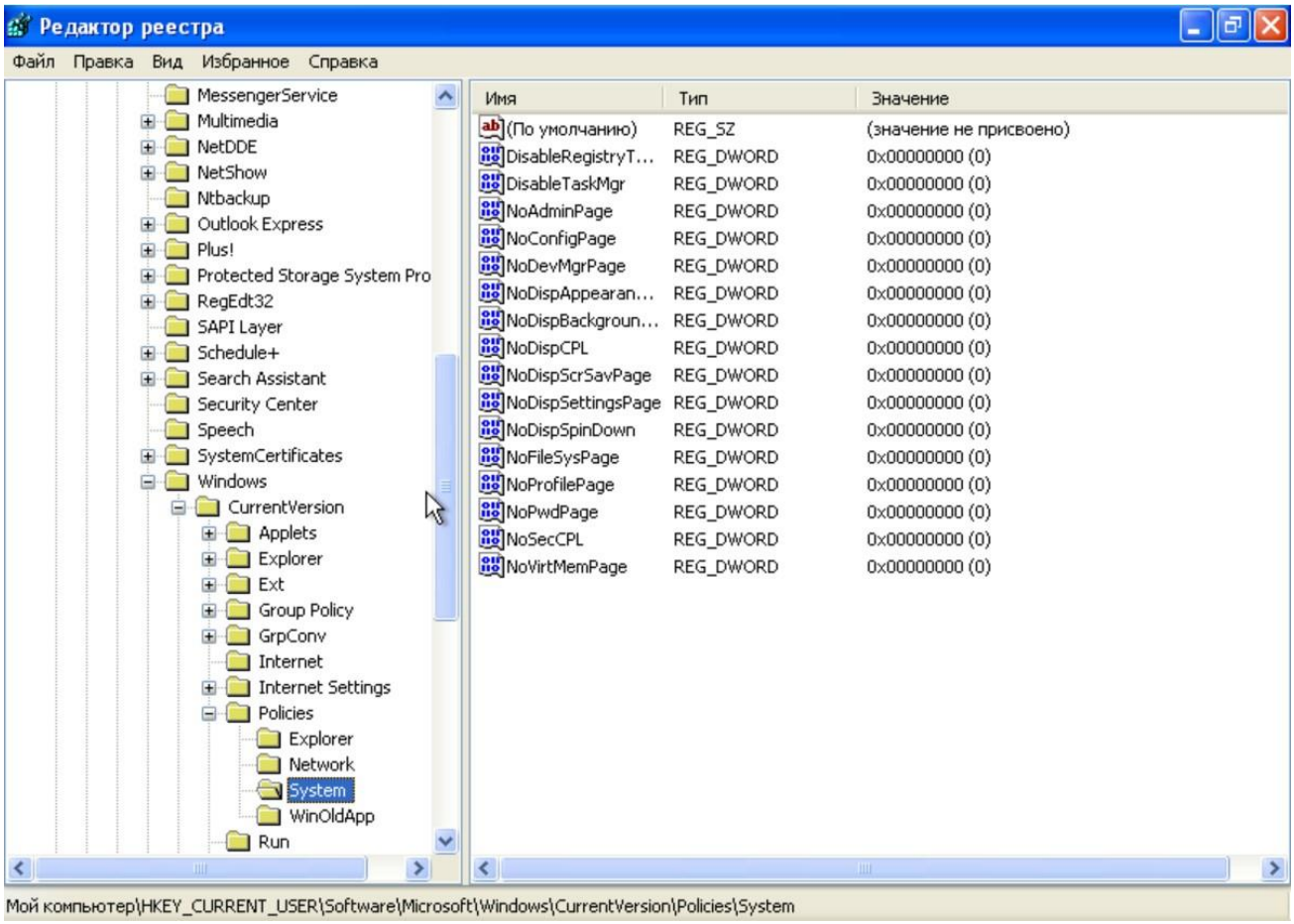

Рисунок № 8 – Policies (Windows XP)

А в *Windows 11* политика безопасности находится в разделе ***HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SettingSync\Groups\ (Accessibility*** “**Доступность**”, ***AppSync*** “**Приложения**”, ***BrowserSettings*** “**Настройки браузера**”, ***Credentials*** “**Учётные данные**”, ***Desktop Theme*** “**Фон рабочего стола**”, ***Language*** “**Язык**”, ***PackageState*** “**Состояние продуктов**”, ***Personalization*** “**Персонализация**”, ***Windows*** “**Виндоус**”**):**

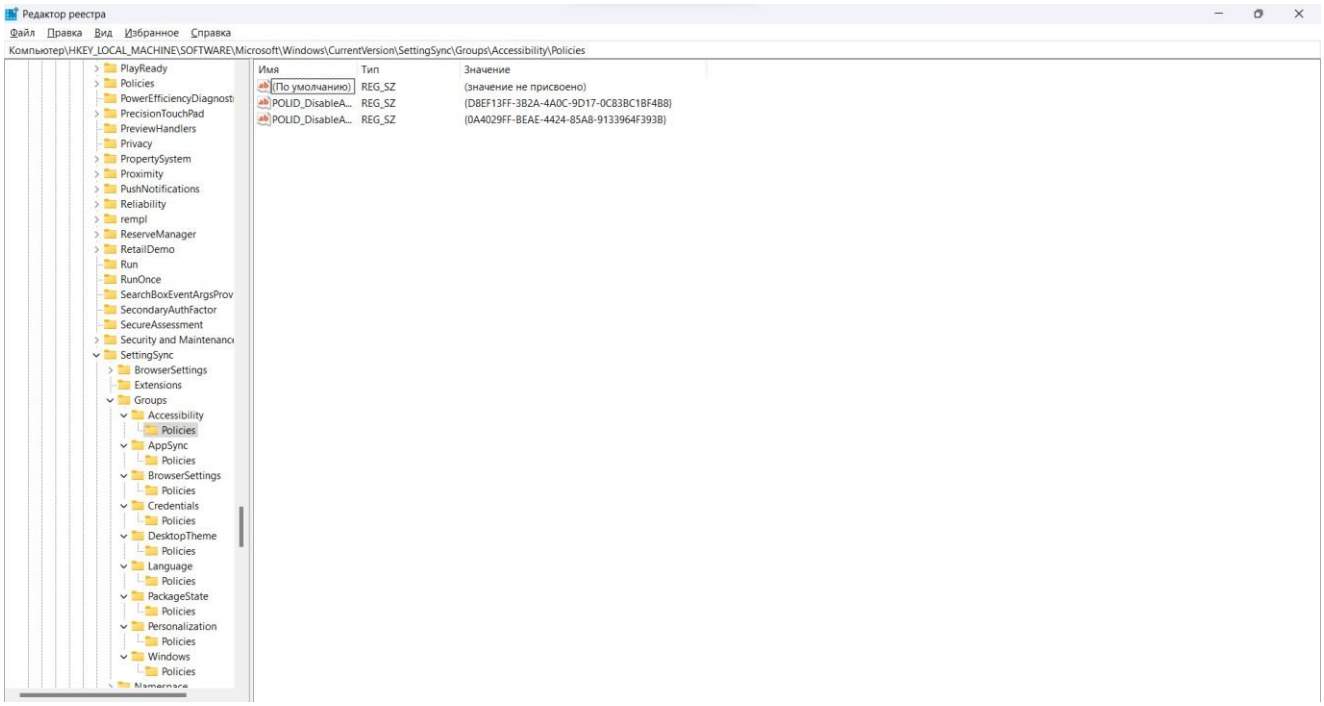

Рисунок № 9 – Policies (Windows 11)

Для обеспечения минимальной эффективности рассмотренных и аналогичных средств необходимо включить функцию *Restrict "Run" command*.

Следующий пункт будет проводиться только с ОС *Windows XP* в связи простой ОС по сравнению с *Windows 11*.

5. Заблокировать работу с используемой рабочей станцией на период временного отсутствия пользователя. Разблокировать работу рабочей станции. Включить в отчет сведения о порядке защиты рабочей станции на период временного отсутствия пользователя и о других функциях операционной системы, доступных при этом наряду с блокировкой.

При длительном отсутствии пользователя следует блокировать рабочую станцию с целью обеспечения защиты от несанкционированного доступа к информации. А также заблокировав *Windows* вы можете сэкономить энергию, так как компьютер переходит в режим ожидания. На ОС *Windows XP* это проделывается путём нажатия комбинации клавиш *CTR + WIN + DEL* или же: Правая кнопка мыши на область рабочего стола => "*Свойства"*, ставим метку на "*Защите паролем*", выбираем интервал и заставку, нажимаем применить.

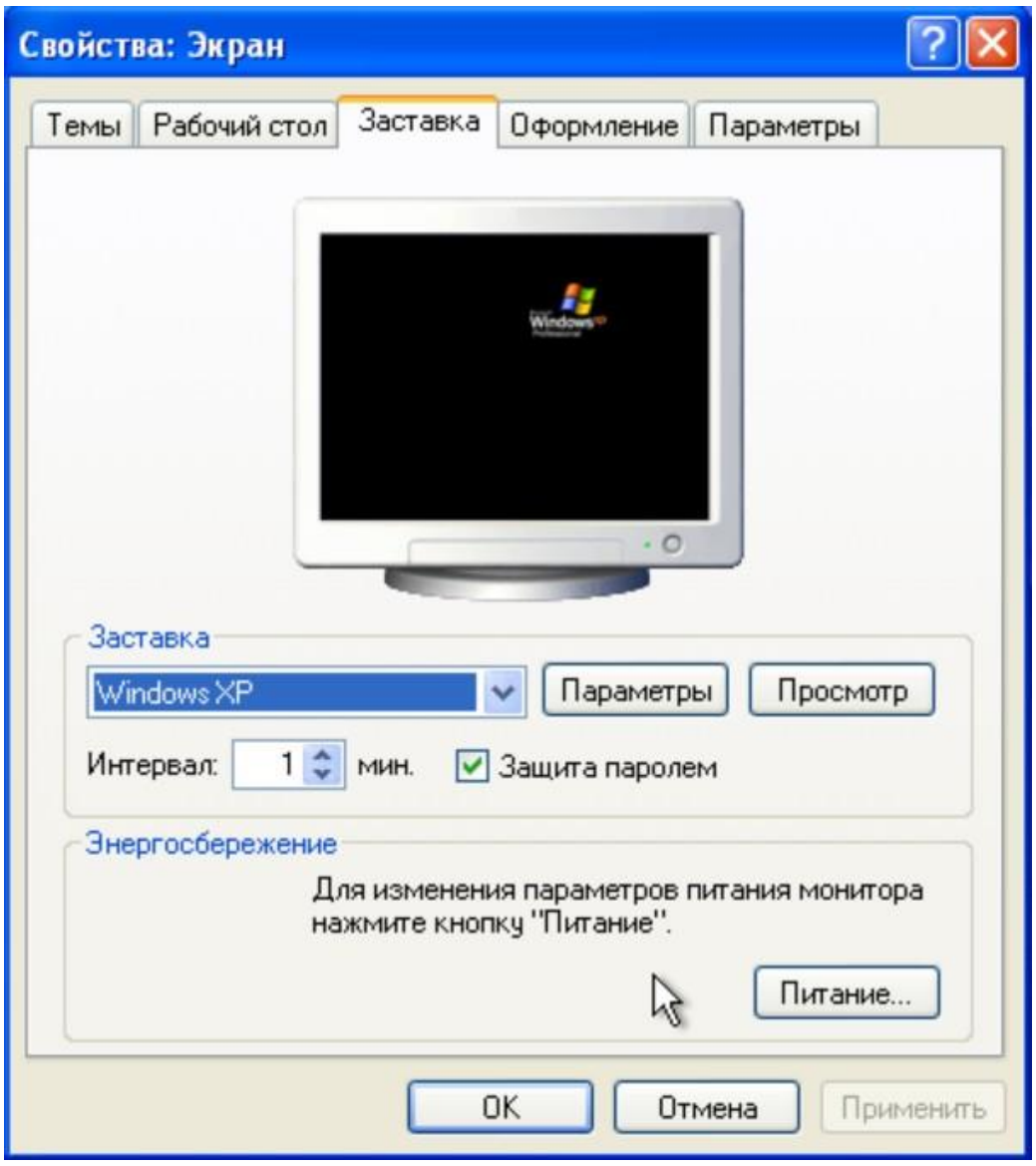

Рисунок № 10 – настройка блокировки экрана (Windows XP)

По истечению времени равного одному интервалу появится заставка:

Рисунок № 11 – заставка блокировки экрана (Windows XP)

При нажатии любой клавиши появится форма. Аналогичная форма появляется при нажатии комбинации клавиш описанной выше:

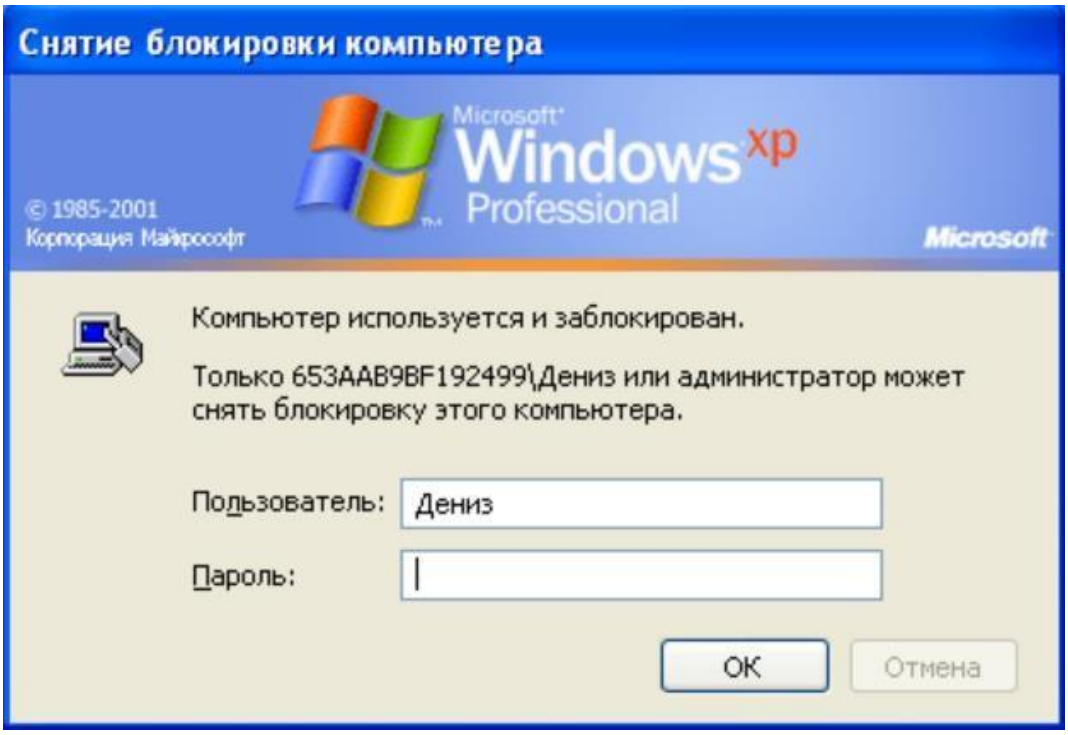

Рисунок № 12 – форма входа пользователя (Windows XP)

Также можно включить запрашивание пароля при выходе из спящего режима как дополнительную функцию. Делается это следующим образом.

Переходим в раздел «*Параметры*», во вкладке «*Схемы управления питанием*» задаем время, во вкладке «*Дополнительно*» ставим галочку «*Запрашивать пароль при выходе из ждущего режима*»:

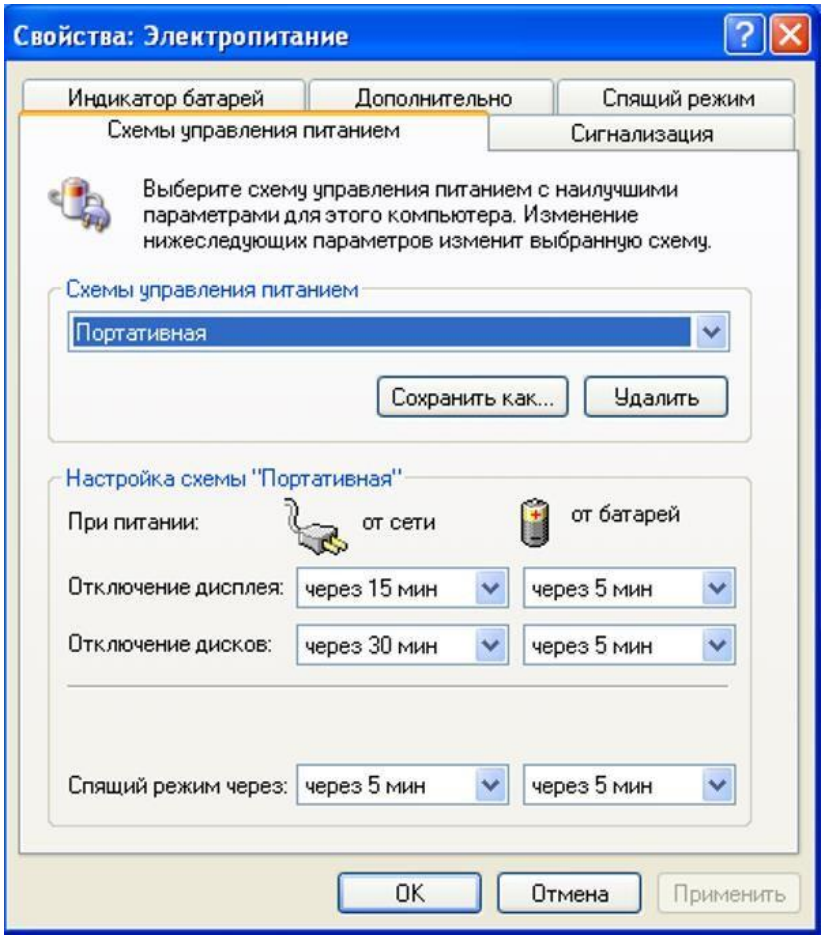

Рисунок № 13 – схема управления питанием (Windows XP)

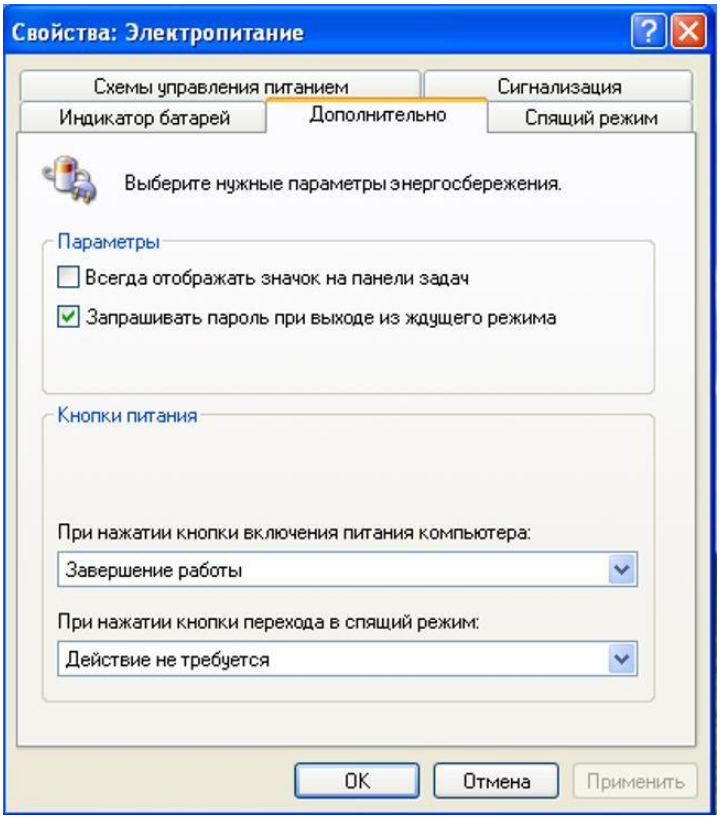

Рисунок № 14 – дополнительно (Windows XP)

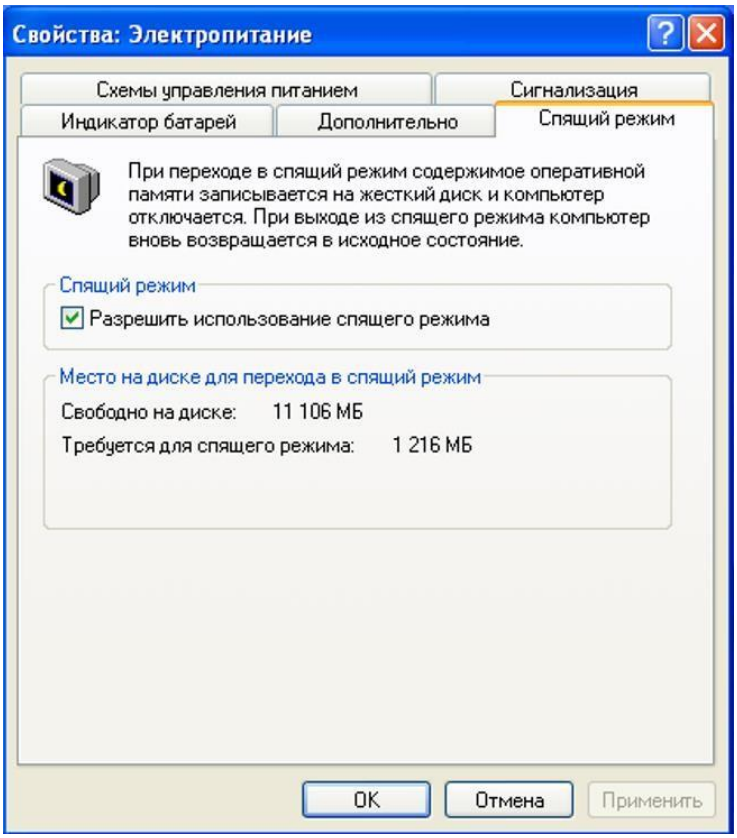

Рисунок № 15 – спящий режим (Windows XP)

При выходе из спящего режима будет аналогичная форма, как на рисунке № 12.

6. Открыть (или создать) произвольный документ в текстовом процессоре Word. Изучить порядок использования паролей для защиты документов в Microsoft Word и включить в отчет соответствующие сведения. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. Завершить работу с Word.

Наряду с операционной платформой *Windows* особо востребованным программным приложением корпорации является пакет разнонаправленных программ *Microsoft Office*, позволяющий создавать, редактировать, распространять и успешно взаимодействовать с различными типами документов. Несмотря на тот факт, что пользователи гарантированно уже используют пароль для защиты своей учетной записи и файлов в операционной системе *Windows* от несанкционированного доступа, существует множество причин, по которым также может дополнительно потребоваться установить пароль для защиты документов *Microsoft*.

Например, пользователям может потребоваться поделиться документом с конфиденциальной информацией и убедиться, что только один доверенный получатель имеет к нему доступ, или рабочий процесс пользователей организован таким образом, что к компьютерному устройству, на котором храниться документ, могут иметь физический доступ многие сторонние пользователи, и необходимо закрыть при помощи пароля свободное взаимодействие.

В *Microsoft Word* возможно установить различные режимы защиты документа:

1) Защита от **несанкционированного просмотра** (*File => Info => Protect document*). Парольная защита на открытие документа;

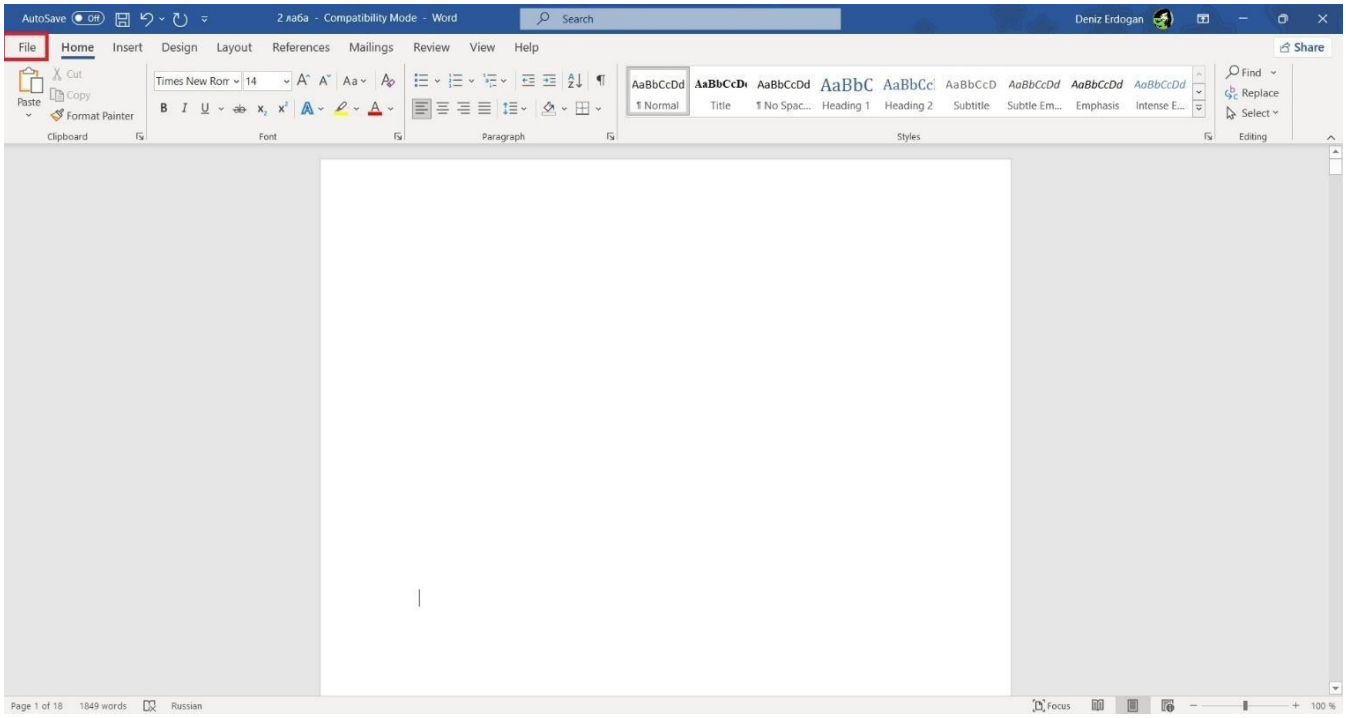

Рисунок № 16 – пункт File (Windows 11)

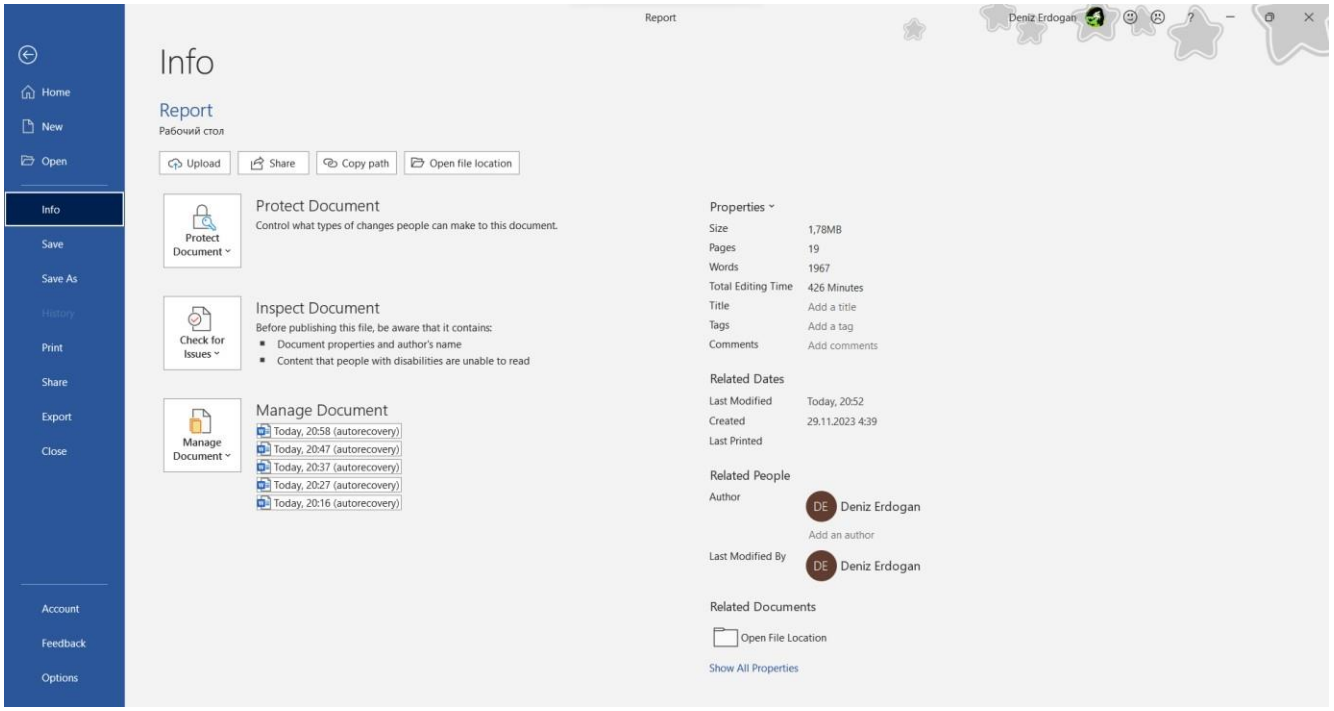

Рисунок № 17 – пункт Info (Windows 11)

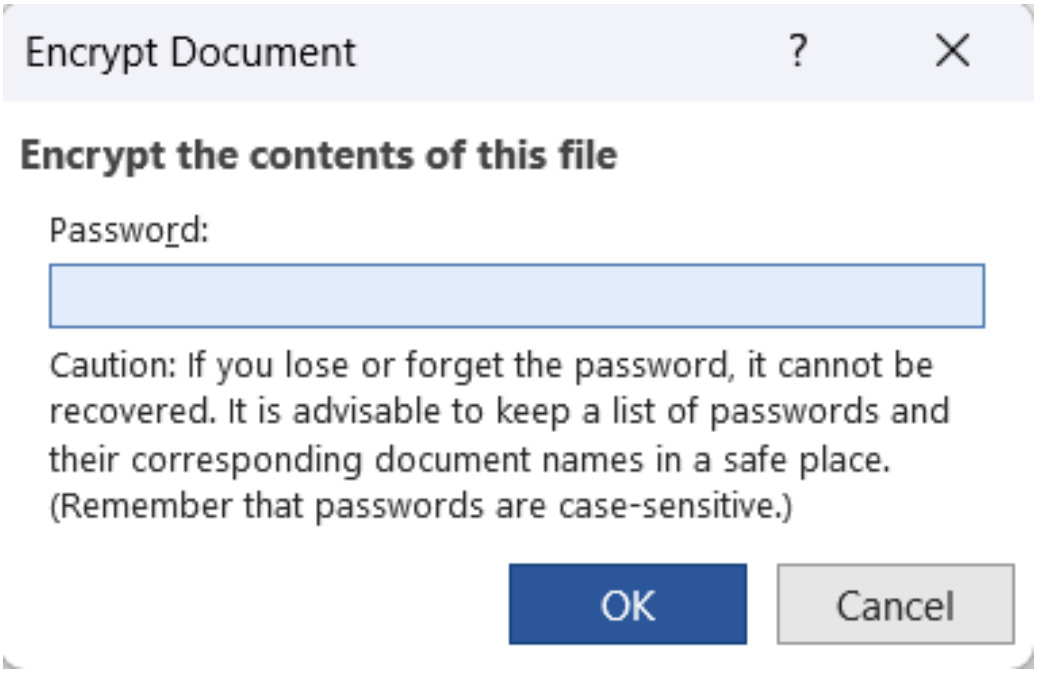

Рисунок № 18 – широфвание документа (Windows 11)

2) Защита от **несанкционированного редактирования (**Review => *Restrict Editing* => (*Formatting restrictions*/*Editing restrictions*/*Start enforcement*)). Здесь возможны несколько вариантов:
   a) защита всего содержимого от редактирования. Парольная защита на сохранение измененного документа;
   b) защита части содержимого от редактирования. Парольная защита на редактирование указанной части документа;
   c) защита всего содержимого от редактирования, кроме полей форм. Парольная защита на редактирование всей текстовой части документа, кроме использованных в документе полей форм.

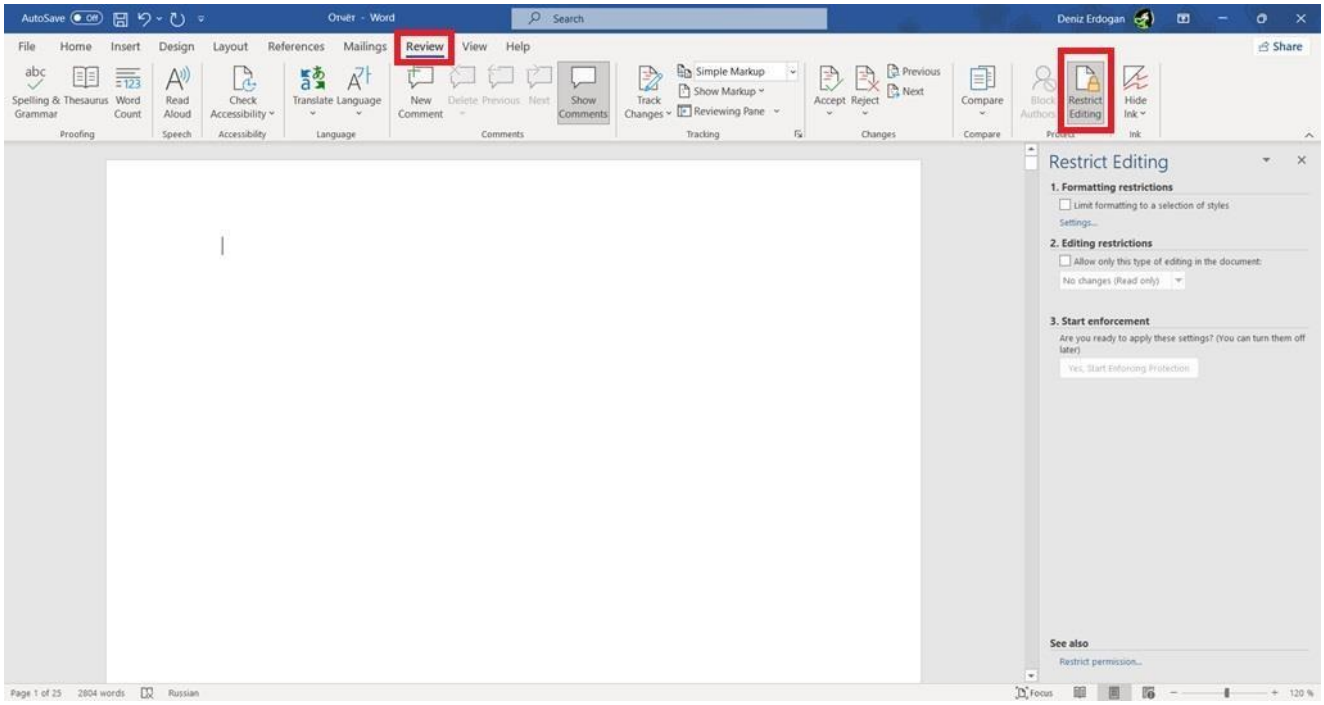

Рисунок № 19 – ограничение редактирования (Windows 11)

7. Открыть (или создать) произвольную таблицу Excel. Изучить порядок использования паролей для защиты документов в табличном процессоре Microsoft Excel и включить в отчет соответствующие сведения. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. Завершить работу с Excel.

В электронных таблицах, создаваемых при помощи *Microsoft Excel*, часто хранится важная информация, которая должна быть скрыта от лишних глаз или случайного редактирования. Специально для таких случаев разработчики программного обеспечения предлагают защиту.

Предусмотрено несколько уровней защиты, позволяющих управлять доступом к данным и их изменением.

1. Можно ограничить доступ к книге (файлу), например, **несанкционированное открытие** книги и/или сохранение в нем изменений.

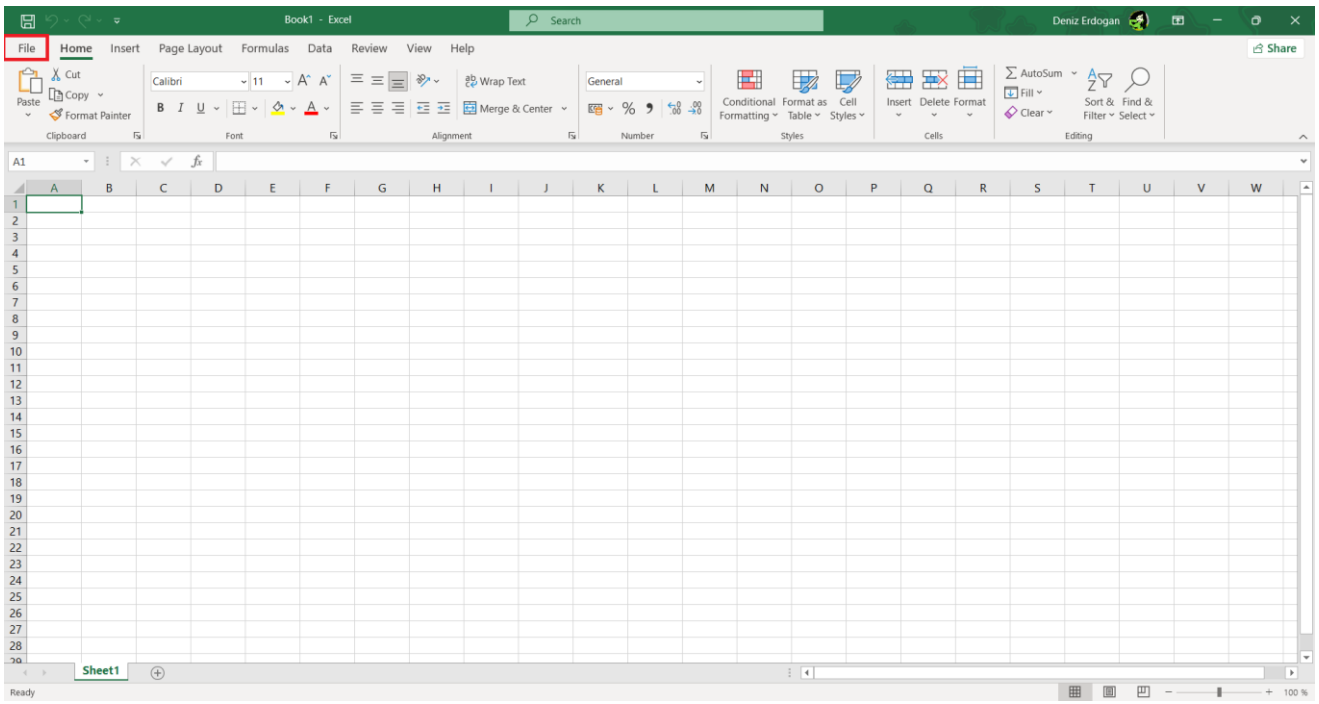

Рисунок № 20 – раздел File (Windows 11)

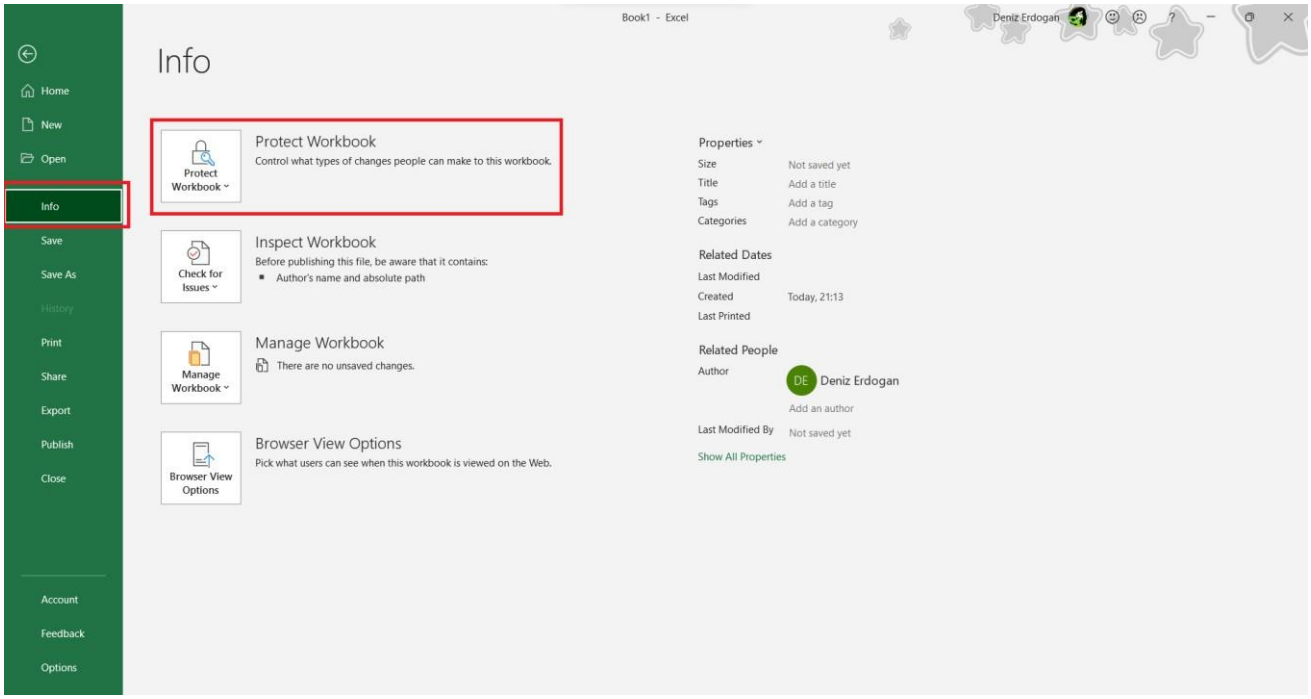

Рисунок № 21 – раздел Info (Windows 11)

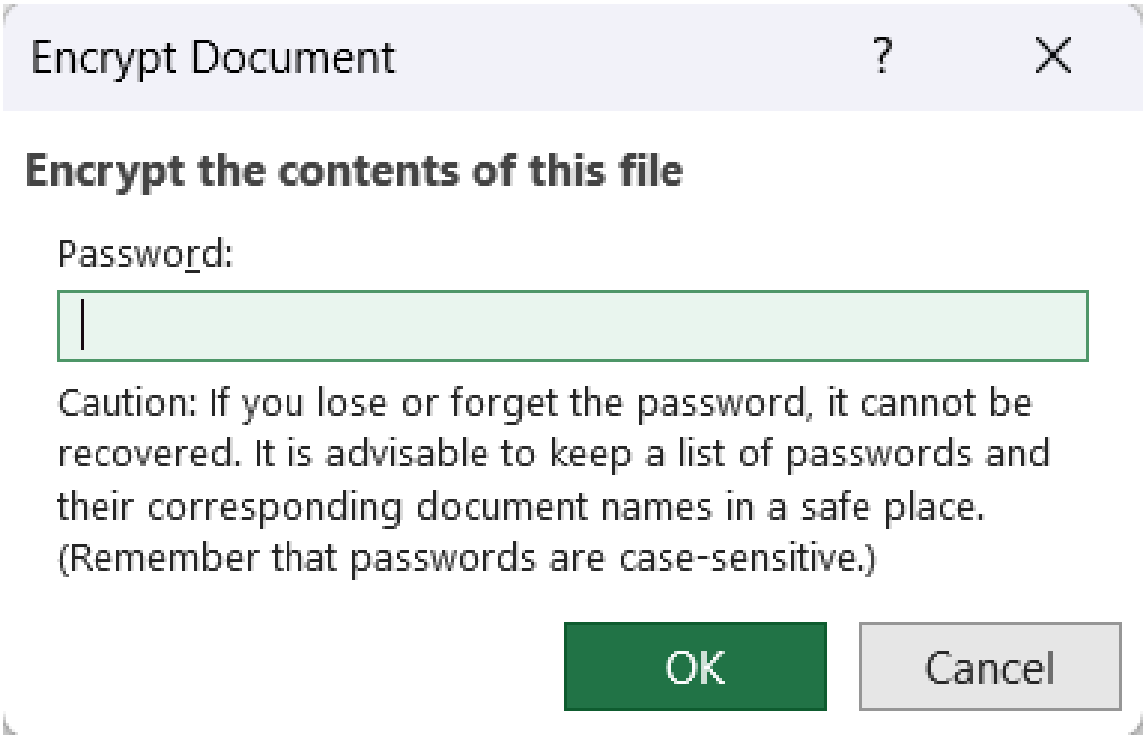

Рисунок № 22 – раздел Шифрования файла (Windows 11)

2. Можно применить защиту к элементам книги, **ограничив просмотр** отдельных листов и/или изменение данных на листе.
3. Можно **защитить элементы** листа, например, ячейки с формулами, запретив доступ к ним всем пользователям или предоставить доступ отдельным пользователям к определенным диапазонам.

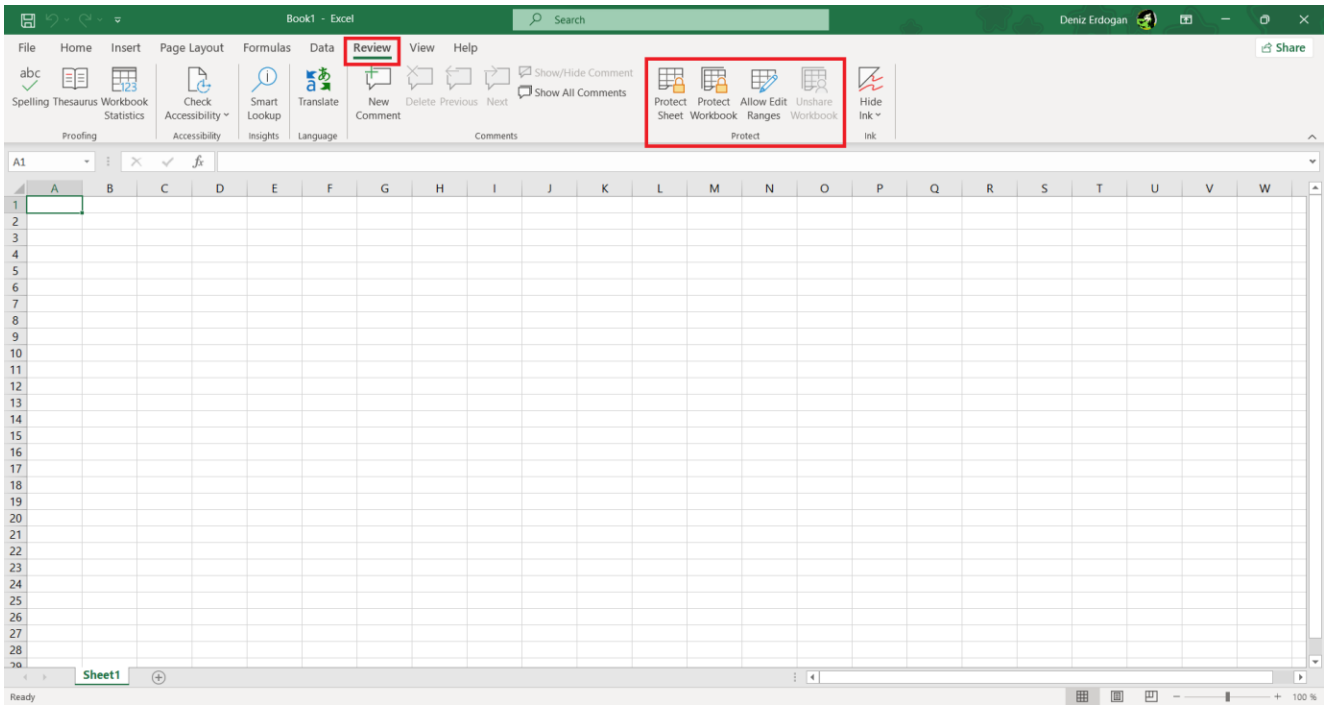

Рисунок № 23 – раздел Protect (Windows 11)

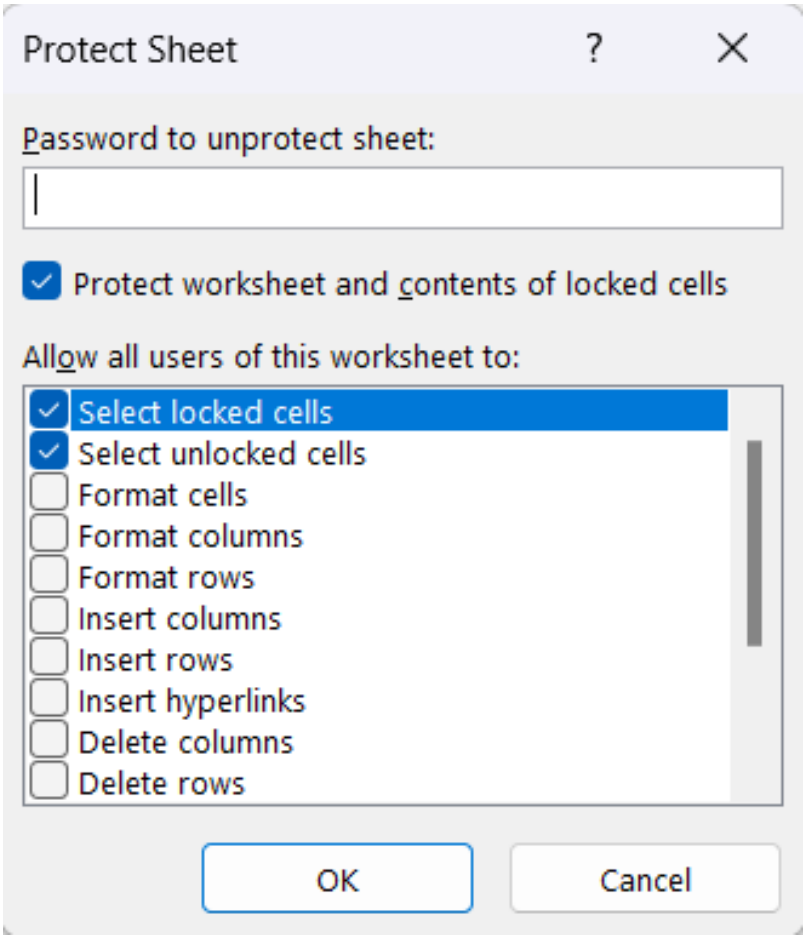

Рисунок № 24 – раздел Protect Sheet (Windows 11)

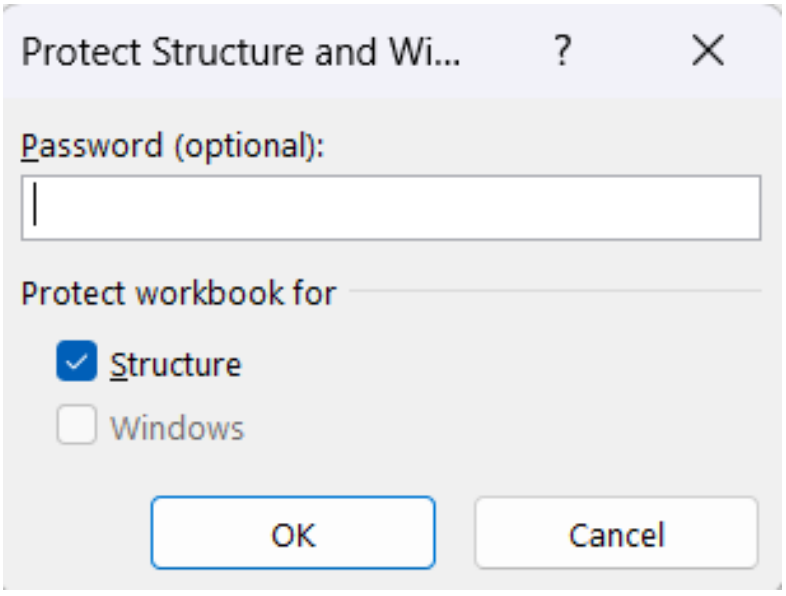

Рисунок № 25 – раздел Protect Structure and Widgets (Windows 11)

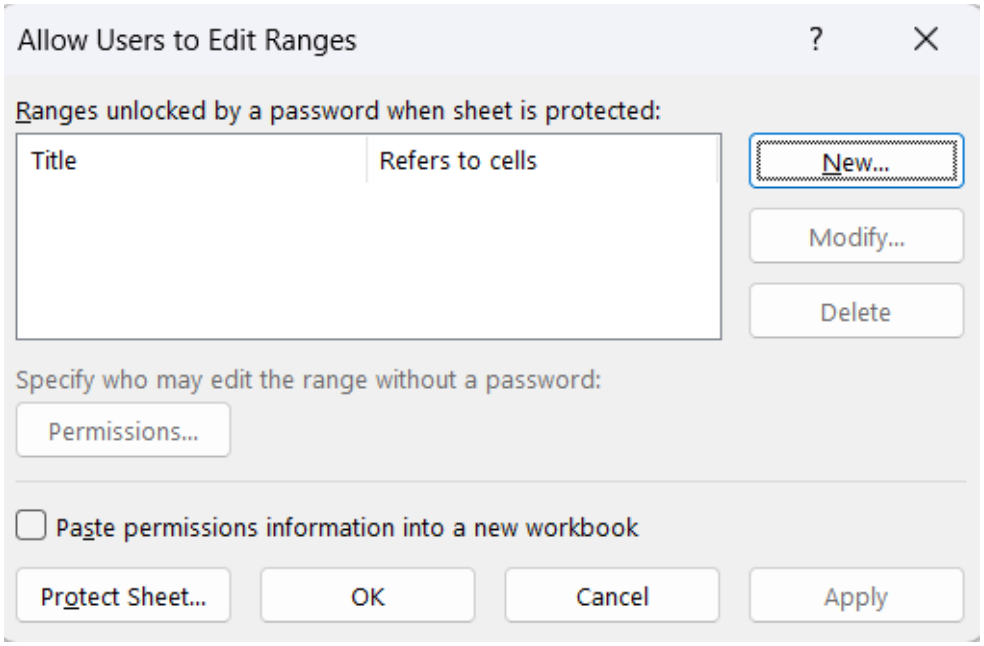

Рисунок № 26 – раздел Allow Users to Edit Ranges (Windows 11)

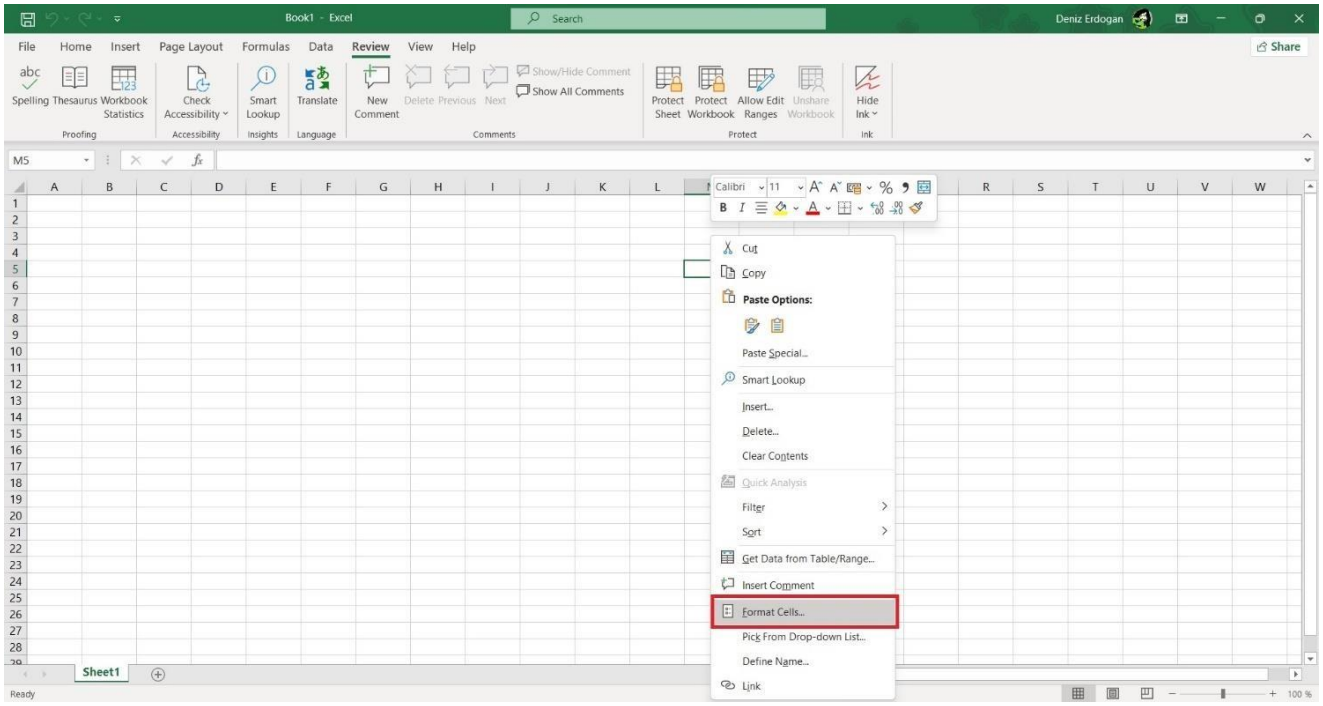

Рисунок № 27 – настройка ячейки Format Cells (Windows 11)

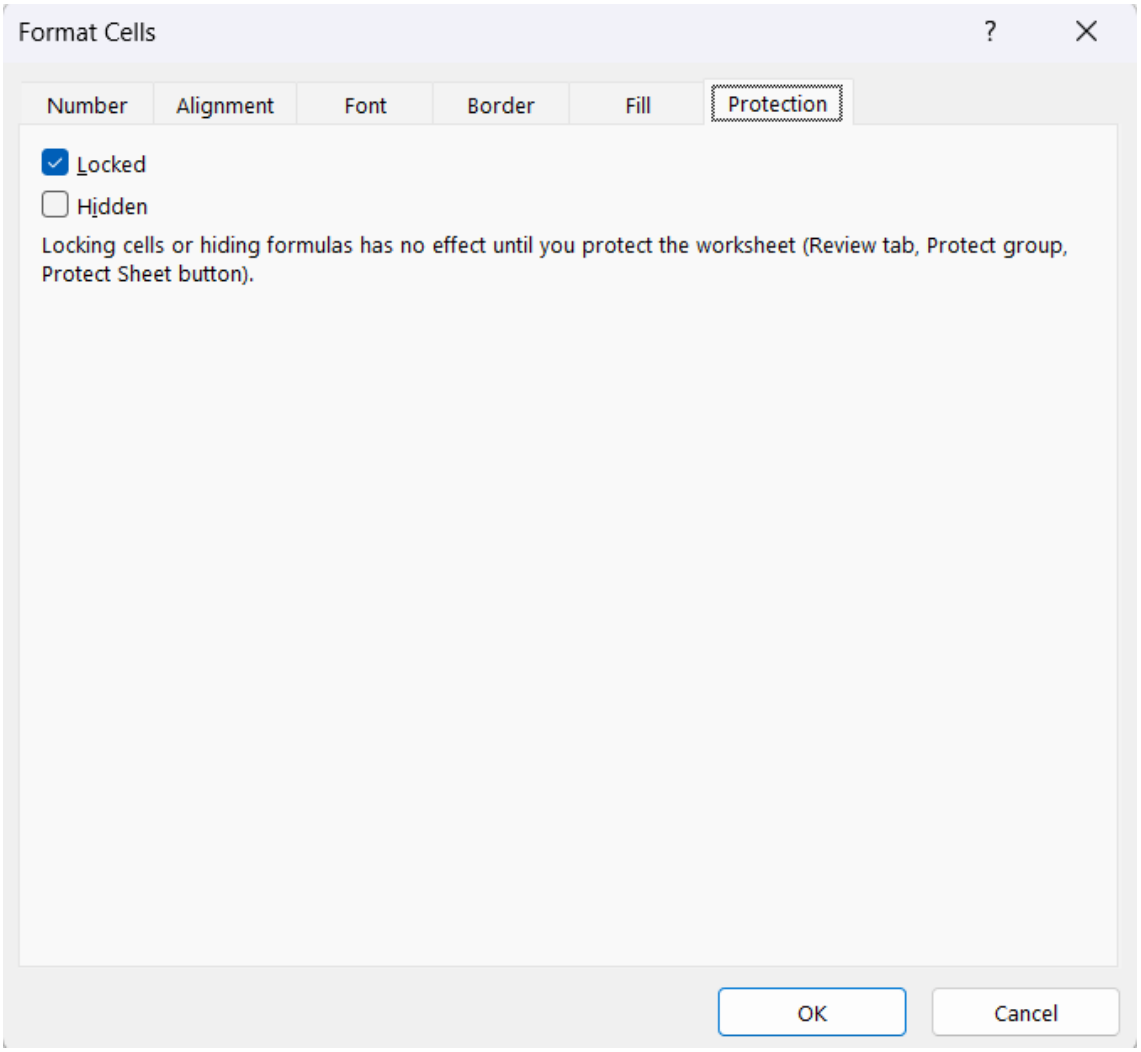

Рисунок № 28 – раздел Format Cells (Windows 11)

Все уровни защиты являются не взаимоисключающими, а взаимодополняющими друг друга.

8. Скопировать в произвольную папку на локальном жестком диске файл whisper.zip из указанного преподавателем сетевого диска.

9. Запустить программу Setup для установки программы Whisper 32 (непосредственно из архива, скопированного в пункте 8, без его распаковки).

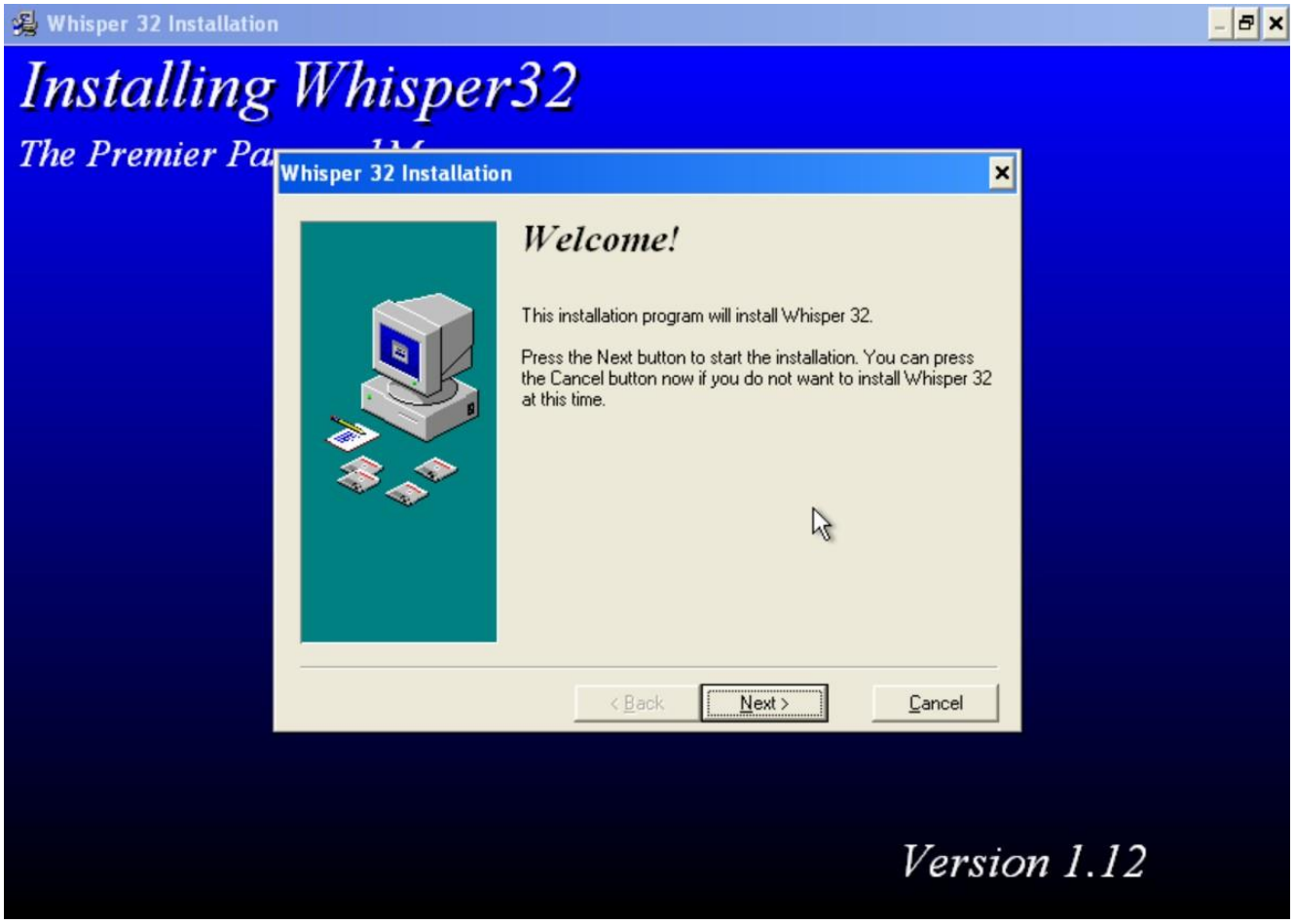

Рисунок № 29 – запуск программы Setup (Windows XP)

10. Запустить программу whisper.exe, предназначенную для создания и ведения базы данных паролей пользователя. Изучить назначение и основные функции программы и включить в отчет соответствующие сведения. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. Завершить работу с программой whisper.exe.

Для того, чтобы обеспечить надежную защиту системы, необходимо располагать полной информацией о паролях. Для хранения и обработки таких атрибутов пользователя, как пароли в ОС *Windows NT*, используется **SAM** (*Security Accounts Manager* — администратор учетных данных в системе защиты). *SAM* размещает всю информацию в базе данных *SAM*. Взломать систему безопасности *SAM* непросто, только если не знать обо всех местах, где можно найти базу данных *SAM*.

Существуют ПО для комфортной работы с *SAM*. Одна из таких программ *Whisper32*. **Whisper 32** - программа, предназначенная для:

- создания и ведения базы данных паролей пользователя:

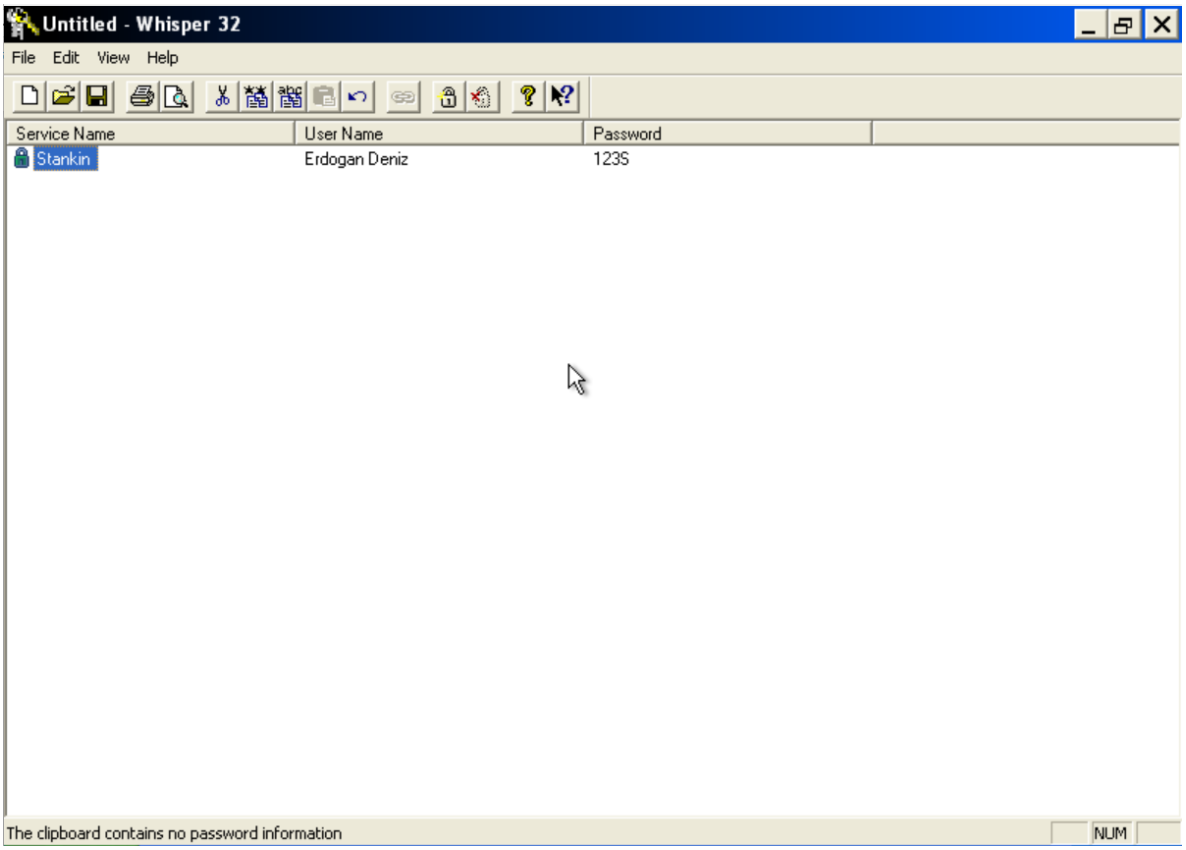

Рисунок № 30 – введение базы данных (Windows XP)

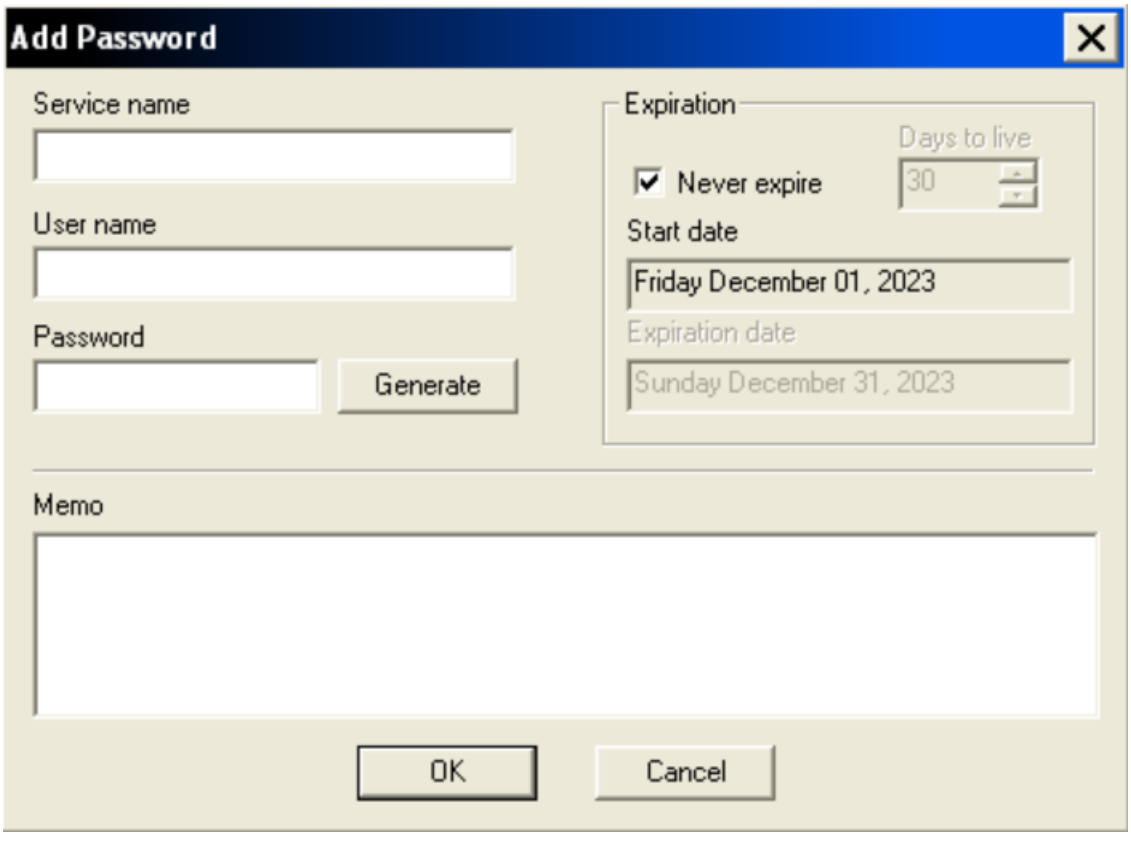

Рисунок № 31 – создание базы данных (Windows XP)

- хранения всех имён пользователей и паролей в одном защищенном паролем файле:

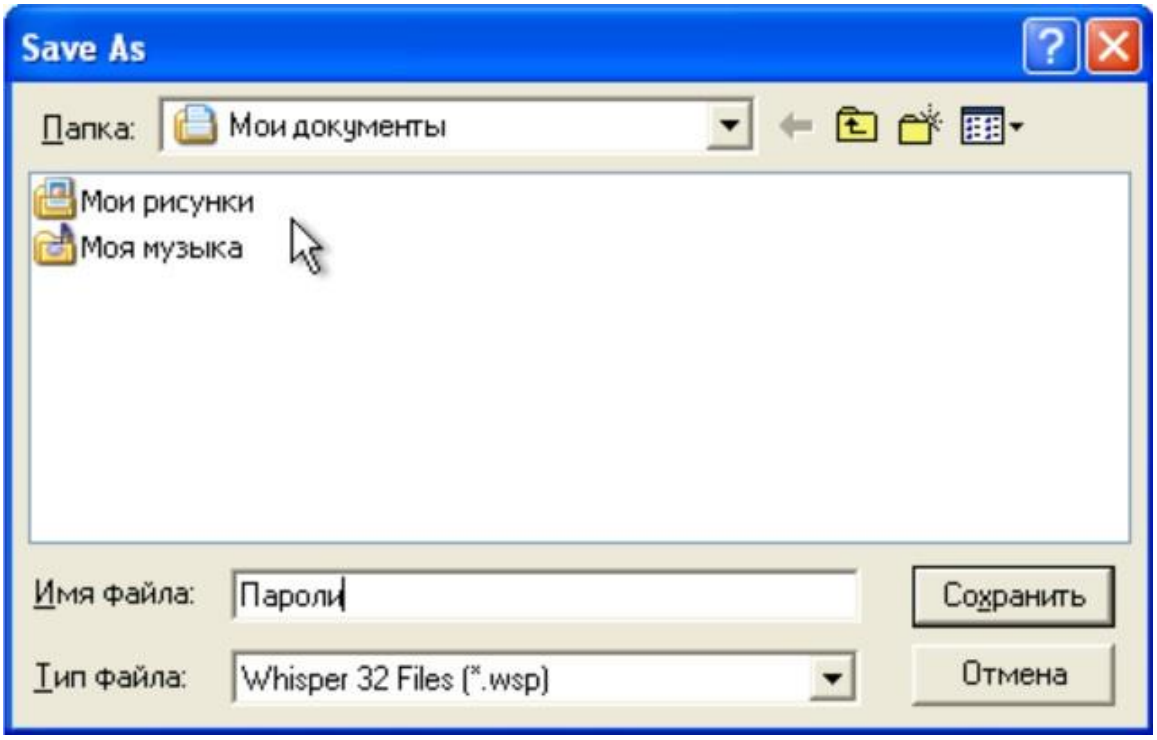

Рисунок № 32 – хранение паролей и пользователей в защищённом файле (Windows XP)

- распечатывания списка данных или копирования его в буфер обмена;
- скрытия полей с паролями;
- програмнного генерирования паролей. В форме генератора паролей нужно указать используемые символы и длину пароля:

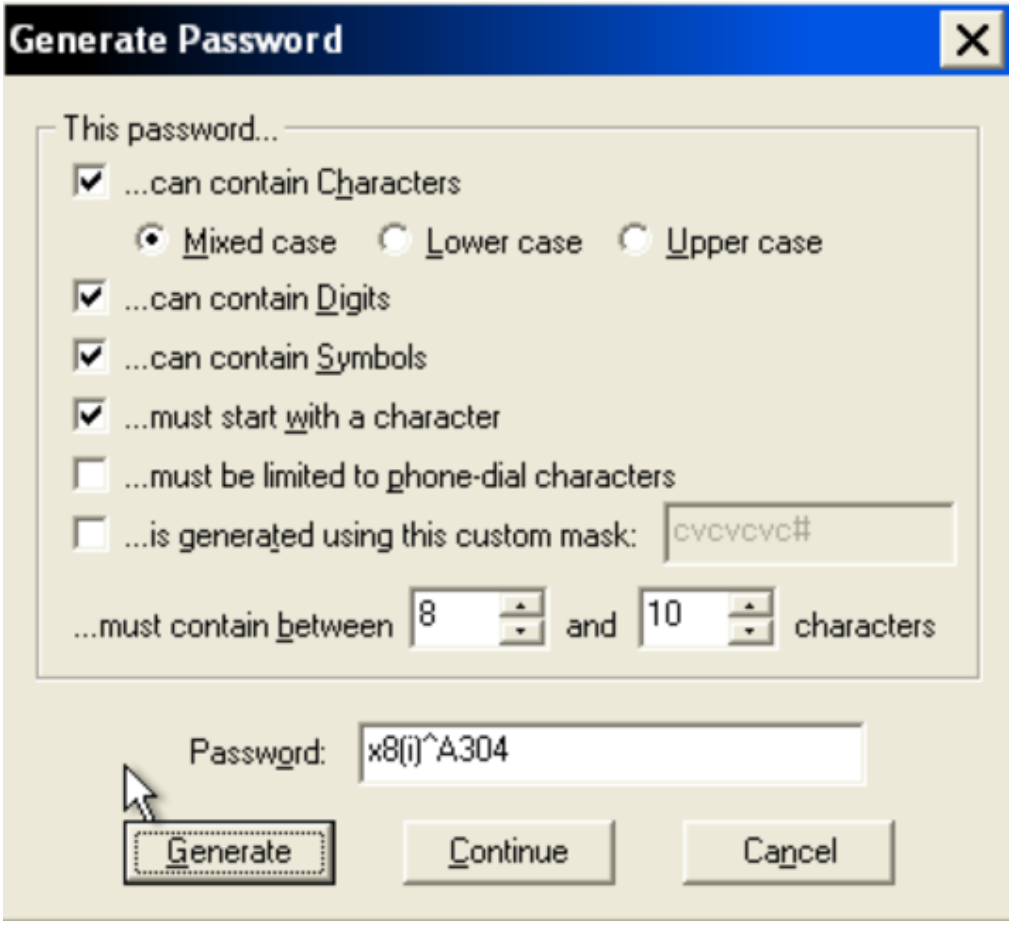

Рисунок № 33 – генерация пароля (Windows XP)

- указания срока действия пароля. По истечении этого периода программа выдаст сообщение об изменения пароля. Данная возможность обеспечивает дополнительную безопасность от несанкционированного доступа к личному кабинету на сайтах:

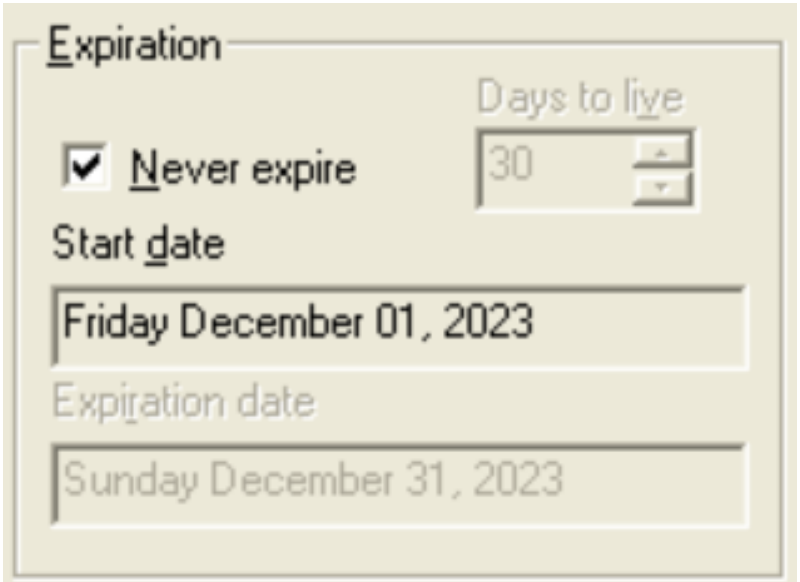

Рисунок № 34 – установление времени на пароль (Windows XP)

- в свойствах программы можно настроить автоматическое резервное копирование списка;
- изменить пароль:

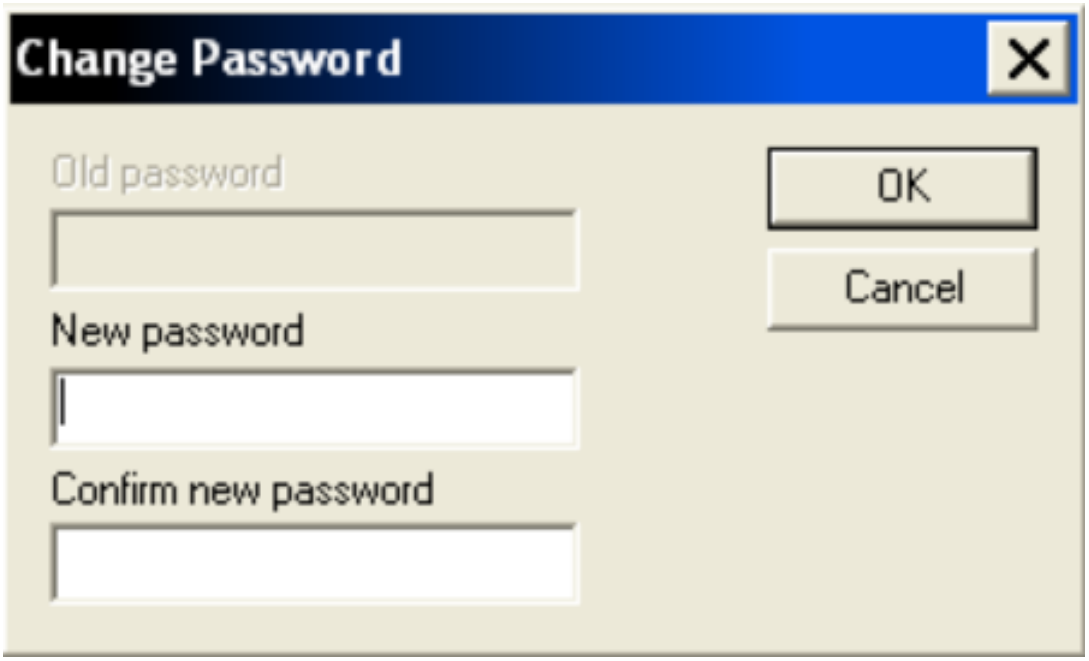

Рисунок № 35 – смена пароля (Windows XP)

11. Ознакомиться (на примере папок, созданных в папке c:\ Documents and Settings \ Имя пользователя \ Документы и в папке c:\ Documents and Settings \ All Users \ Документы) с порядком разграничения доступа к ресурсам в защищенных версиях операционной системы Windows (с помощью контекстного меню объекта и элементов управления соответствующих диалоговых окон). Если команда «Общий доступ и безопасность» недоступна (при работе в ОС Windows XP Professional), то выключить режим «Использовать простой общий доступ к файлам» на вкладке «Вид» окна свойств папки. Включить в отчет сведения об особенностях управления доступом к папкам и файлам в этих ОС. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта.

Для обеспечения безопасности данных и контроля доступа пользователей к системным и пользовательским ресурсам существуют разграничения доступа к ресурсам в ОС *Windows*.

Управление доступом заключается в предоставлении пользователям, группам и компьютерам определенных прав на доступ к объектам по сети или на компьютере. Группе пользователей или пользователю можно предоставить разрешения на чтение, запись, изменение или полный доступ к файлу или папке. Например, одному пользователю можно разрешить читать содержимое файла, другому - вносить изменения в файл, а всем остальным пользователям вообще запретить доступ к этому файлу. Целесообразно установить разрешения для групп, поскольку эту увеличивает быстродействие системы при проверке прав доступа к объекту.

Разрешения, назначаемые объекту, зависят от его типа. Например, разрешения, которые могут быть назначены для файла, отличаются от разрешений, допустимых для раздела реестра. Однако некоторые разрешения являются общими для большинства типов объектов (чтение, изменение, смена владельца, удаление).

Рассмотрим разрешения на примере папки “*Документы*” для одного пользователя:

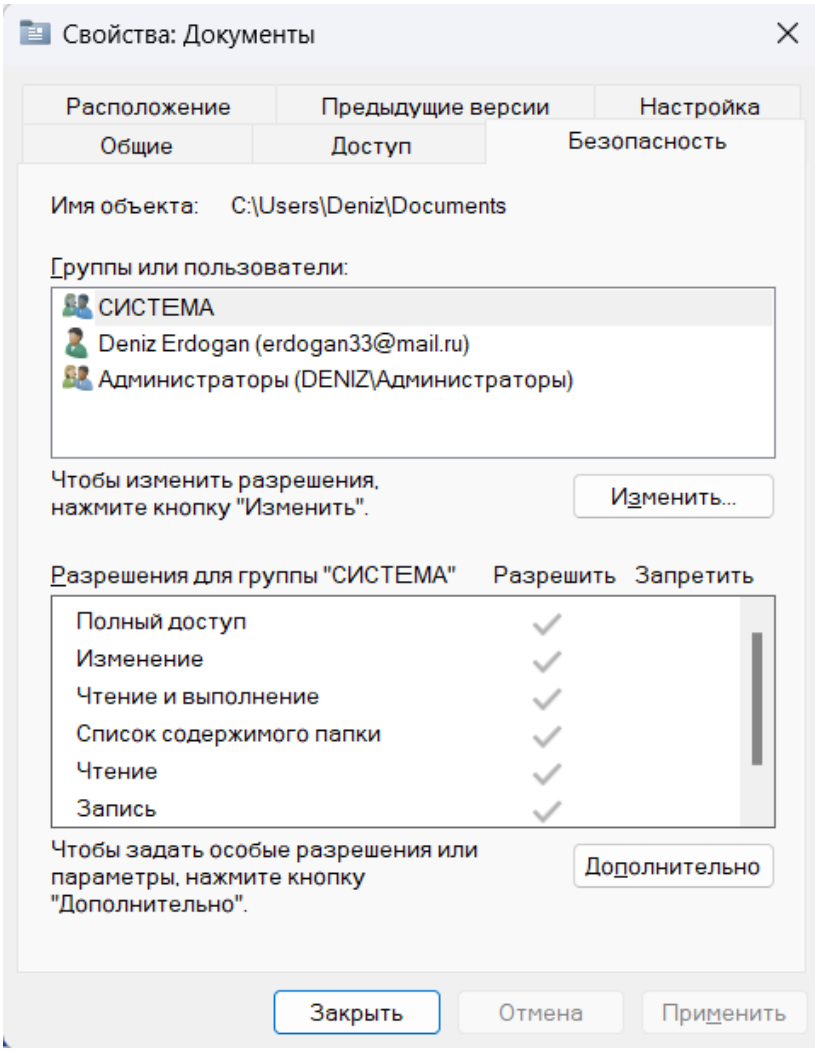

Рисунок № 36 – вкладка безопасности одного пользователя (Windows 11)

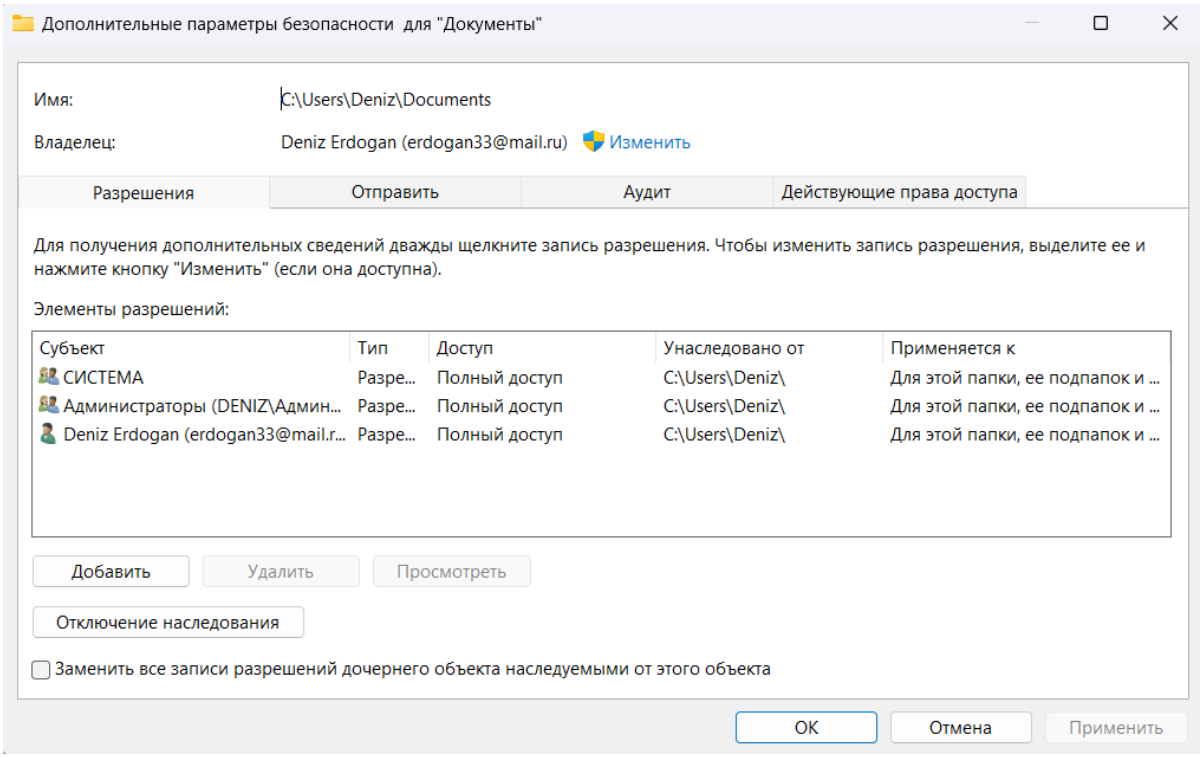

Рисунок № 37 – дополнительные параметры безопасности одного пользователя (Windows 11)

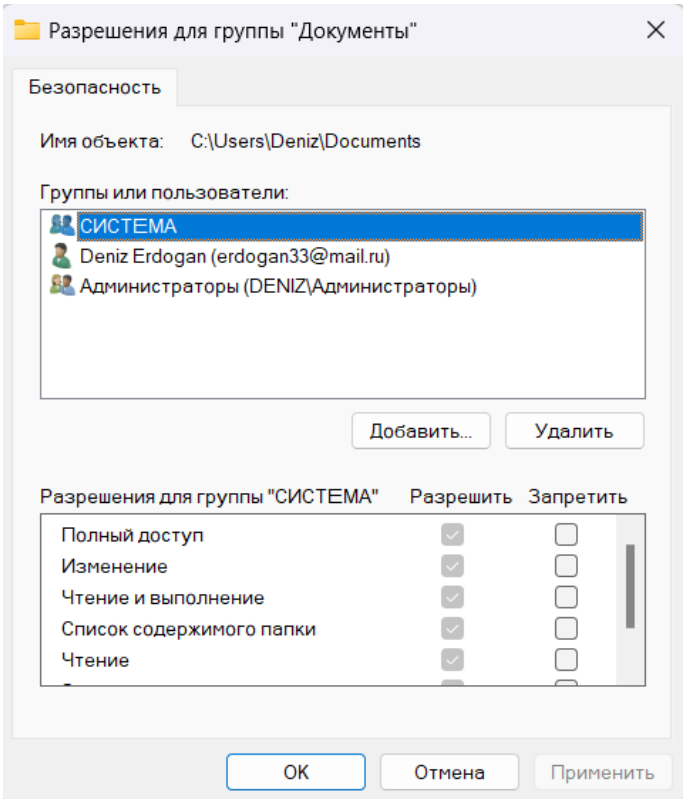

Рисунок № 38 – разрешение для группы папки одного пользователя (Windows 11)

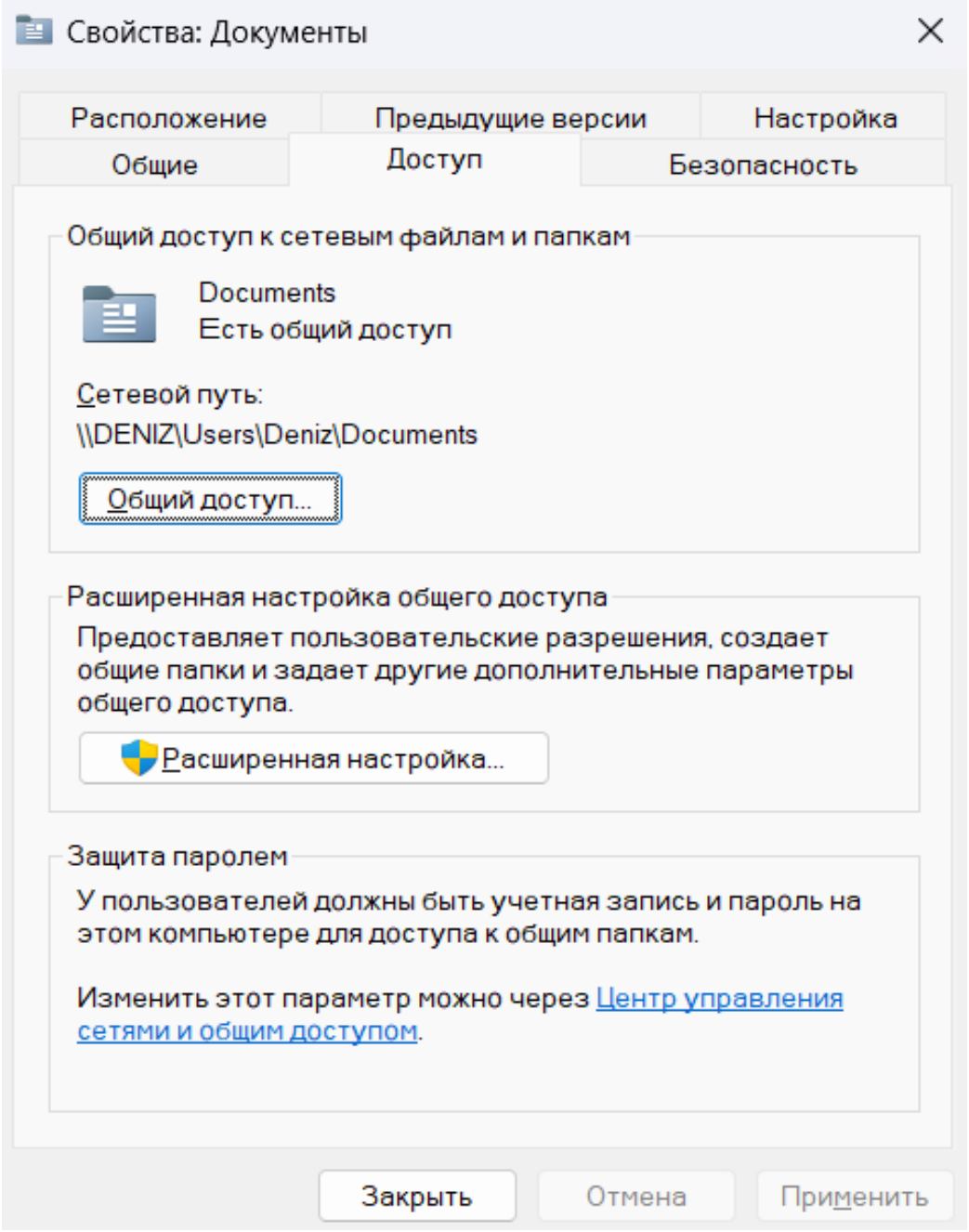

Рисунок № 39 – вкладка доступ одного пользователя (Windows 11)

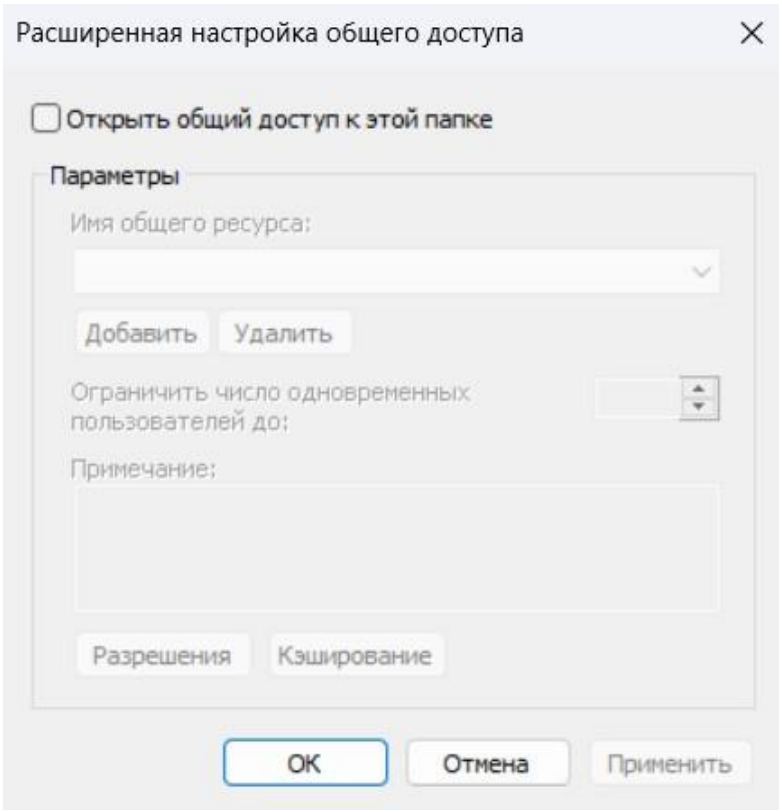

Рисунок № 40 – расширенные настройки общего доступа одного пользователя (Windows 11)

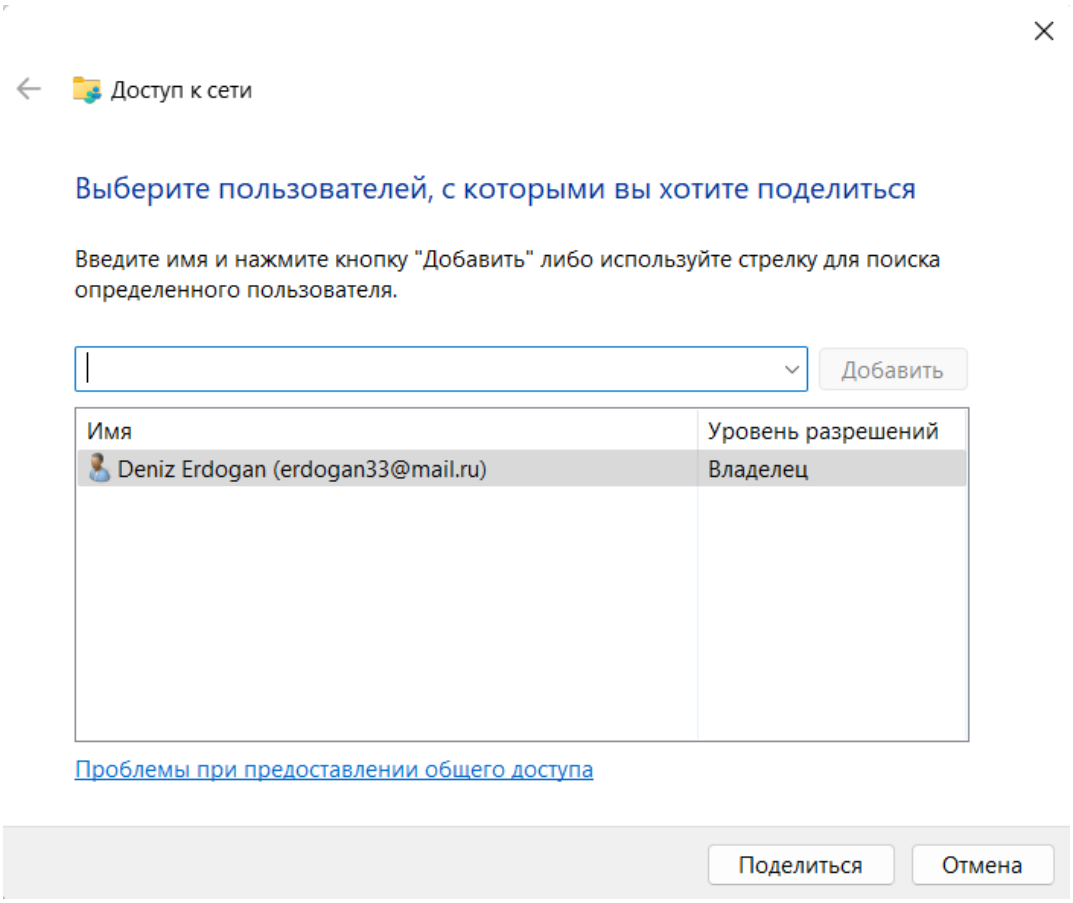

Рисунок № 41 – расширенные настройки общего доступа одного пользователя (Windows 11)

Теперь рассмотрим разрешения на примере папки “Документы” для всех пользователей:

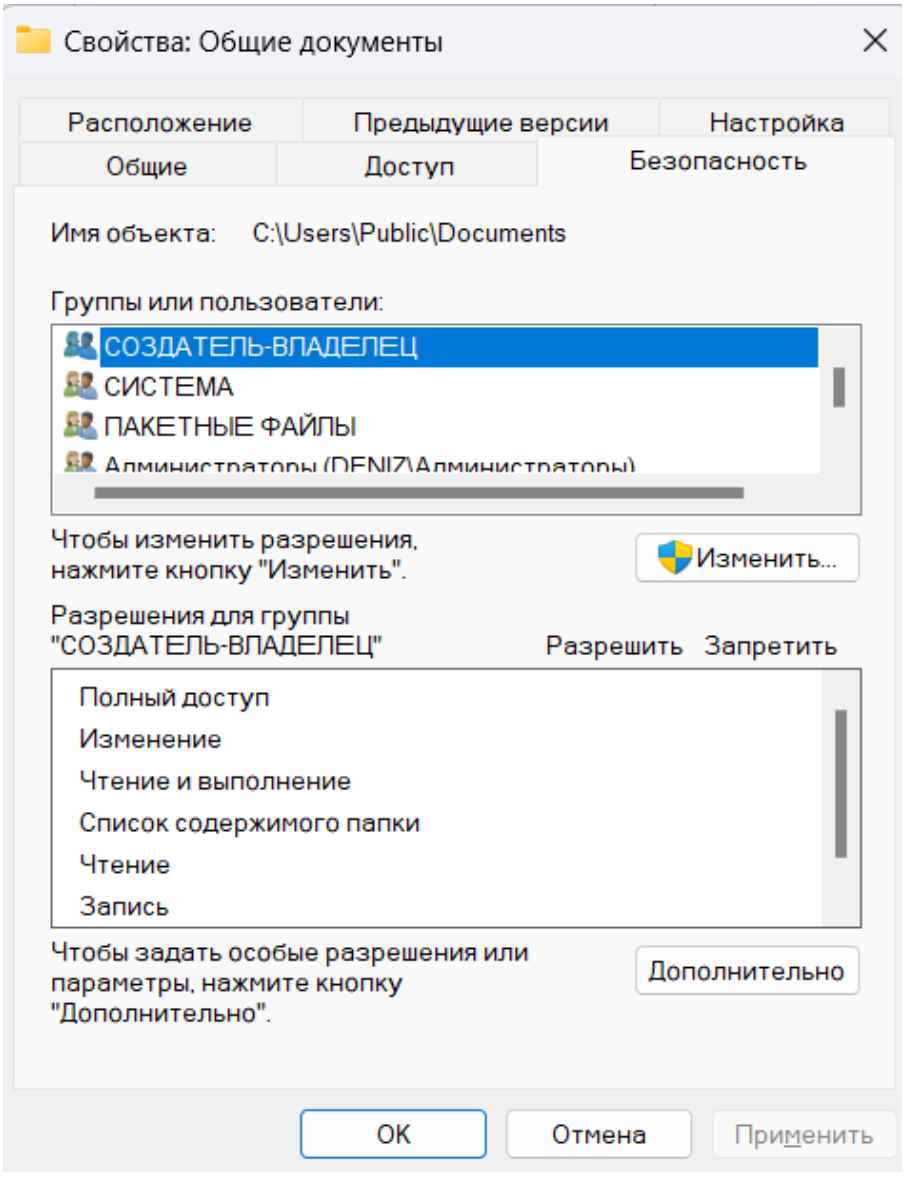

Рисунок № 42 – вкладка безопасности всех пользователей (Windows 11)

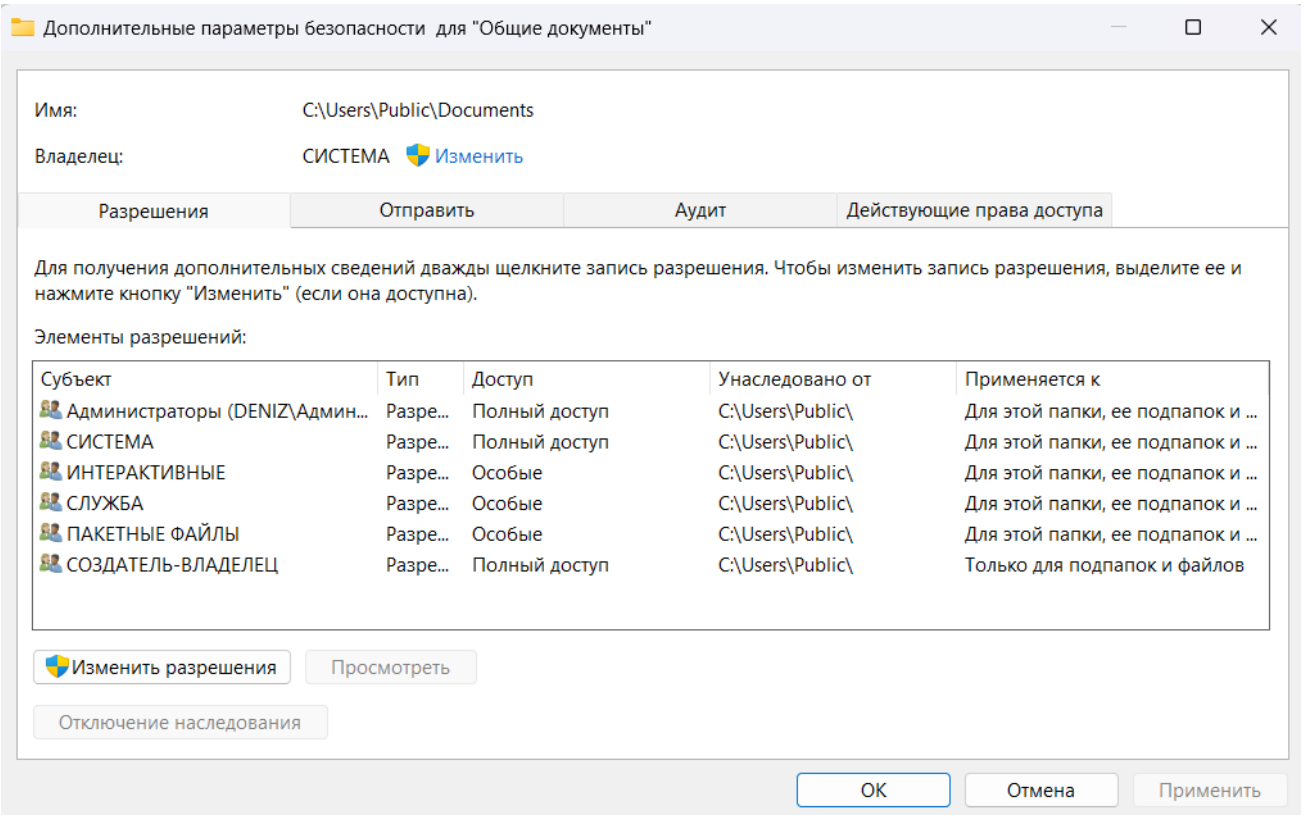

Рисунок № 43 – дополнительные параметры безопасности всех пользователей (Windows 11)

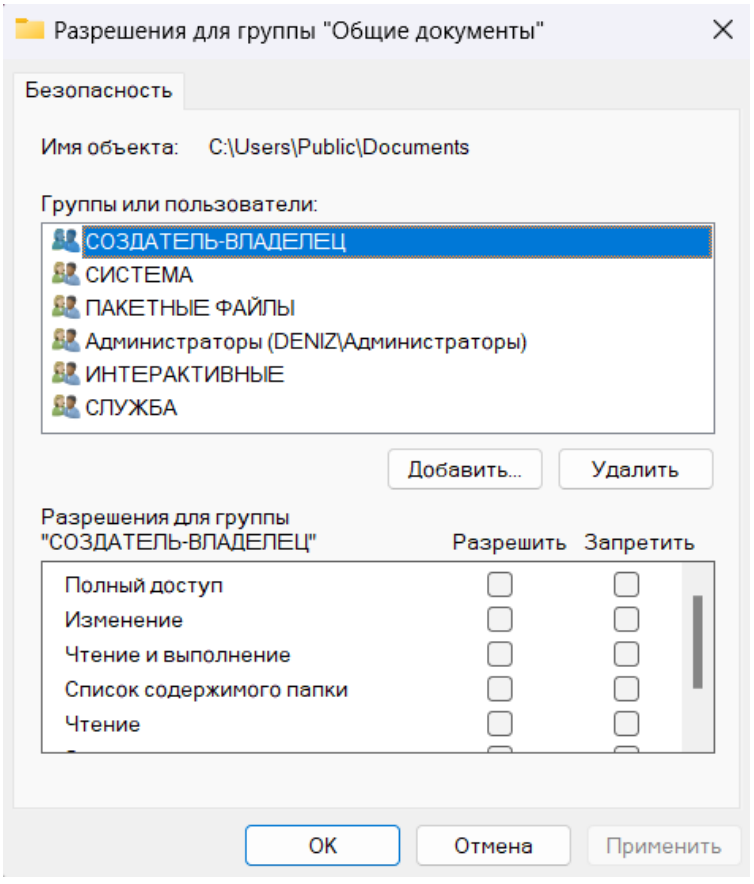

Рисунок № 44 – разрешение для группы папки всех пользователей (Windows 11)

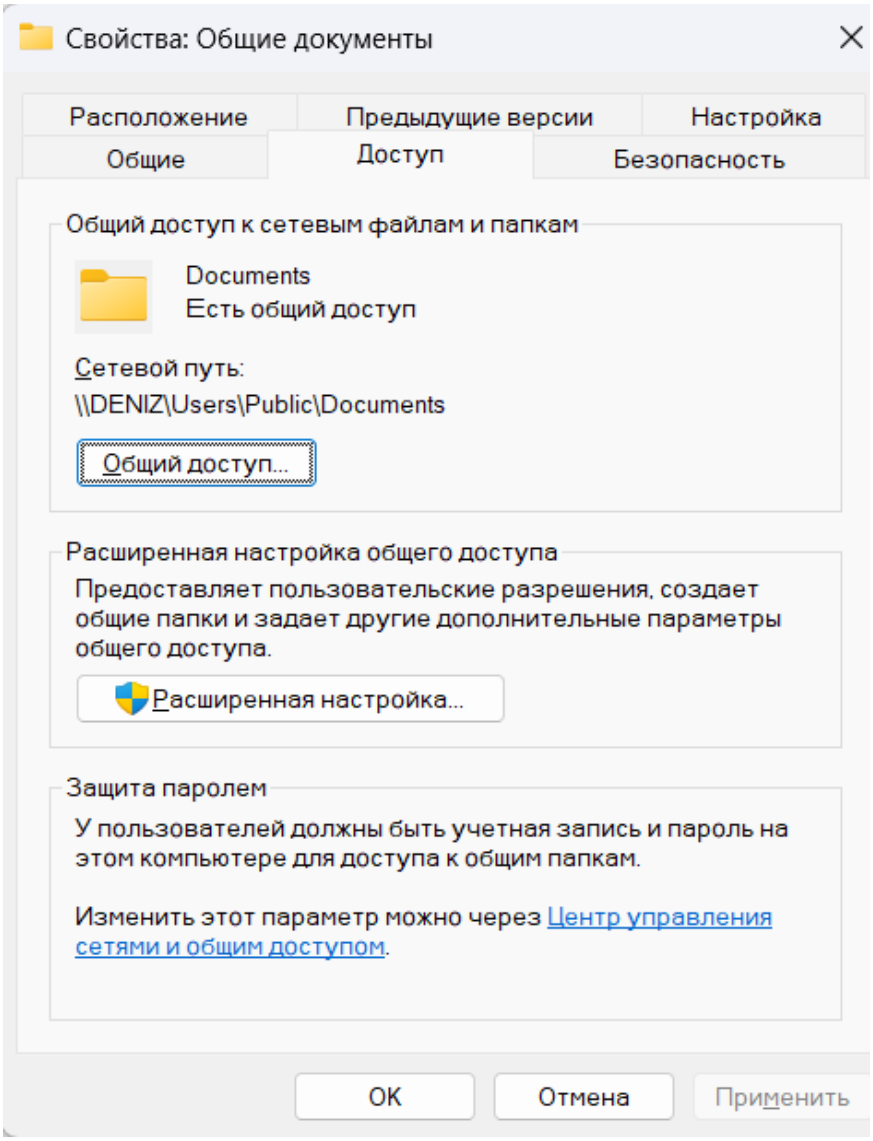

Рисунок № 45 – вкладка доступ всех пользователей (Windows 11)

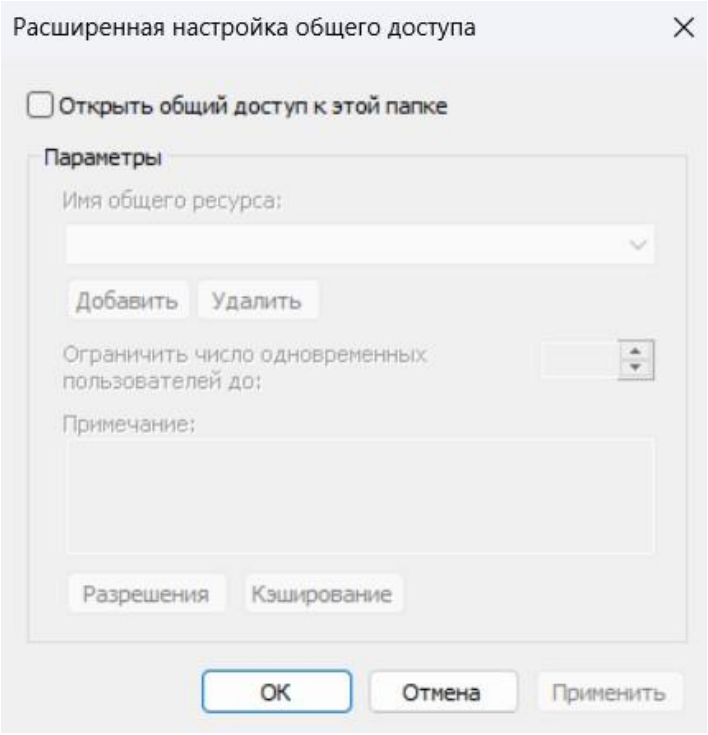

Рисунок № 46 – расширенные настройки общего доступа всех пользователей (Windows 11)

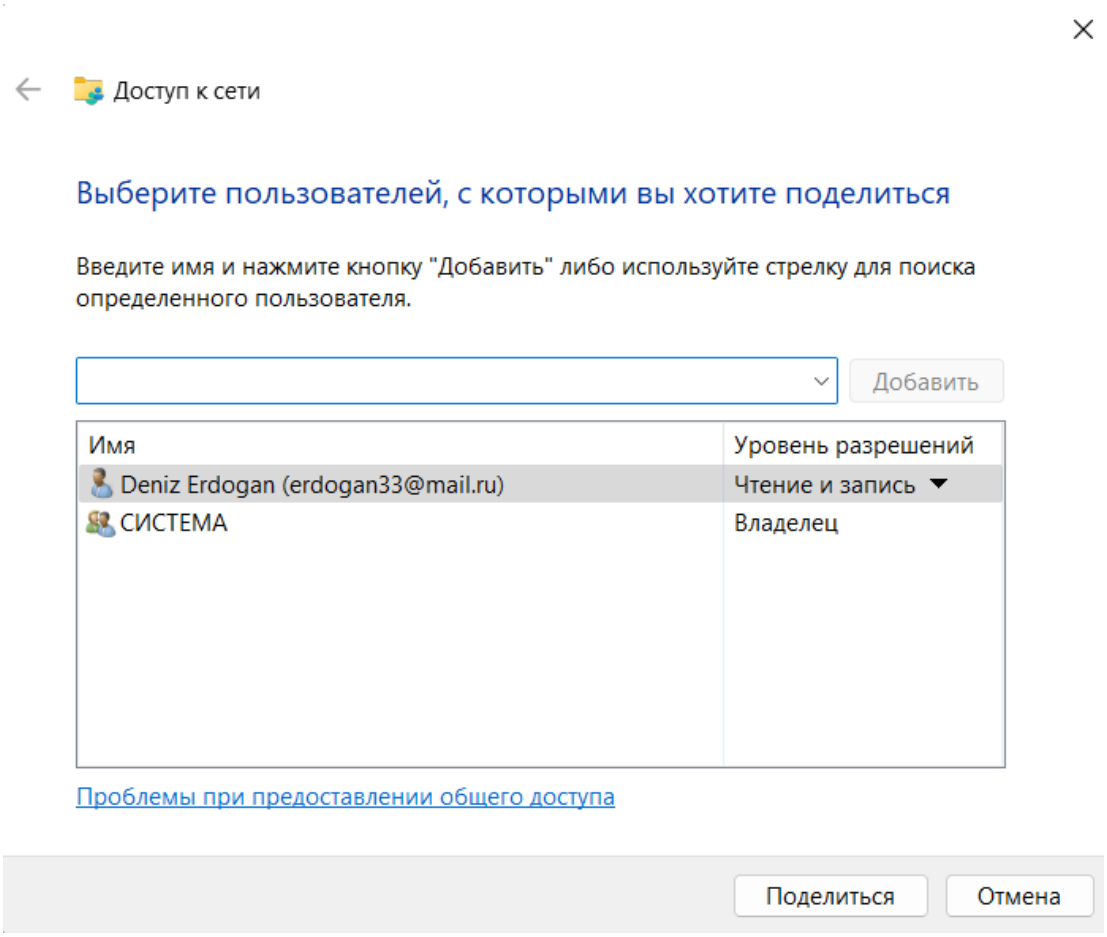

Рисунок № 47 – расширенные настройки общего доступа всех пользователей (Windows 11)

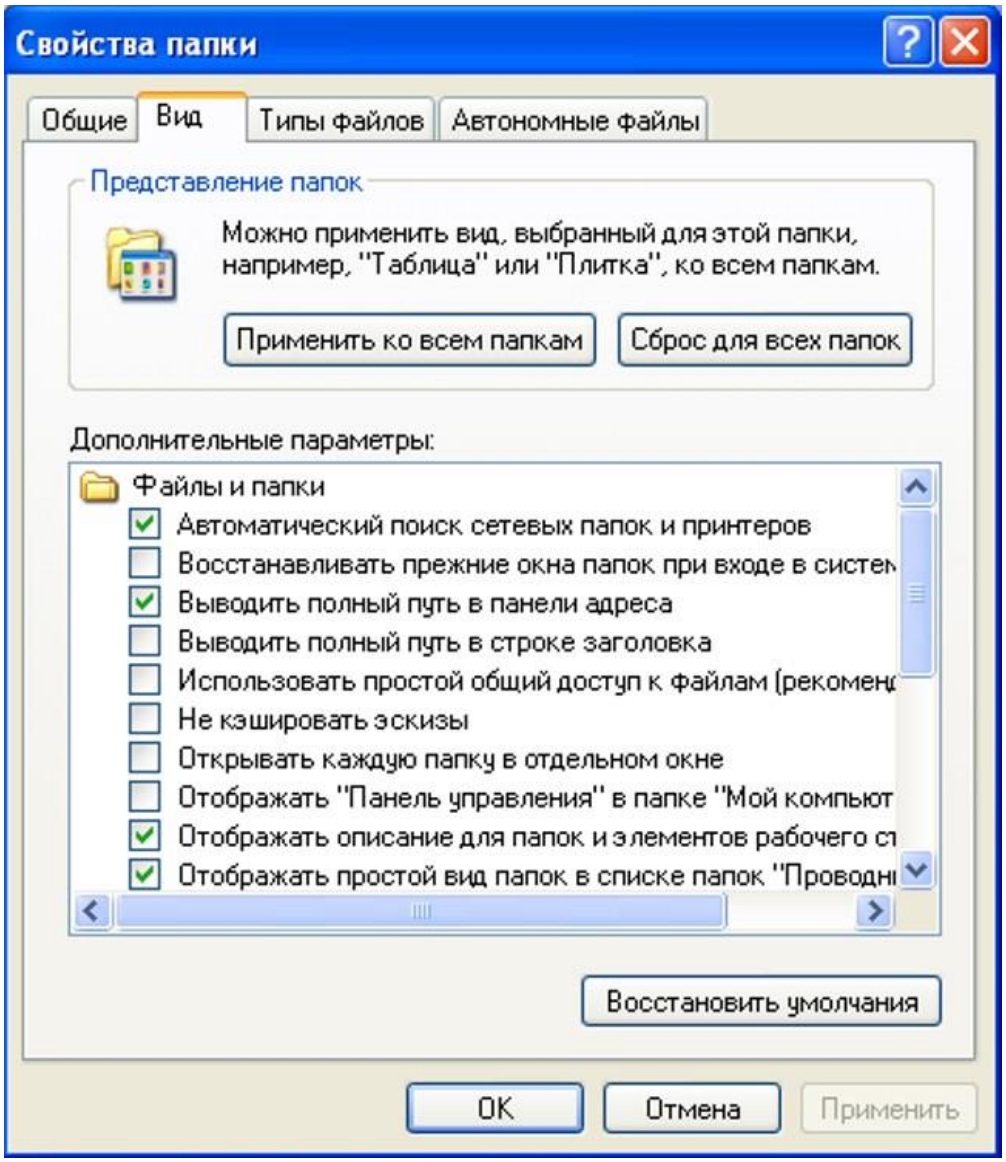

Рисунок № 48 – свойство папки одного пользователя (Windows XP)

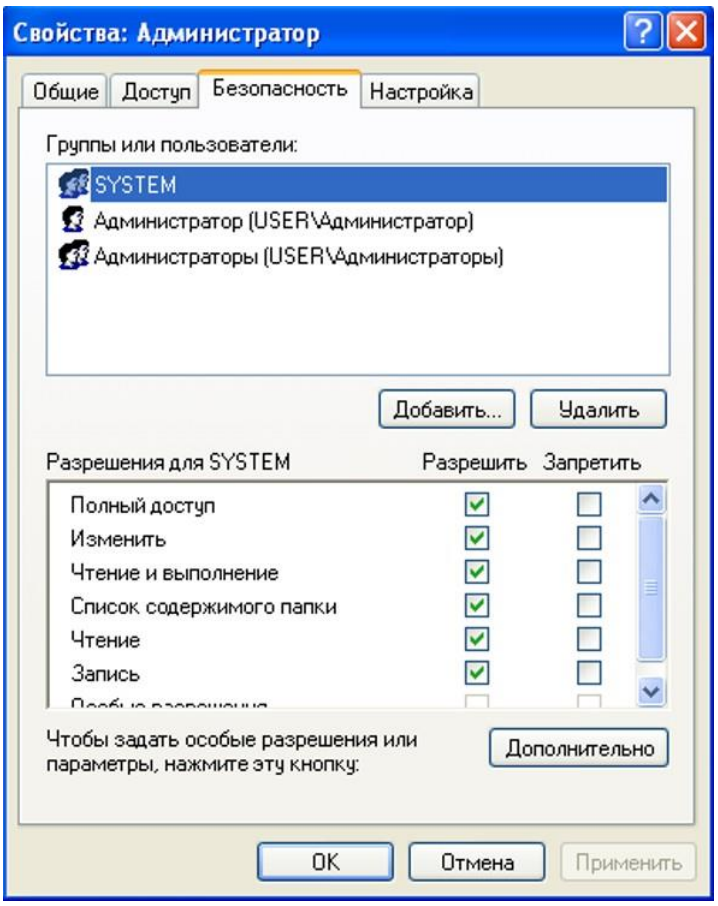

Рисунок № 49 – безопасность папки одного пользователя (Windows XP)

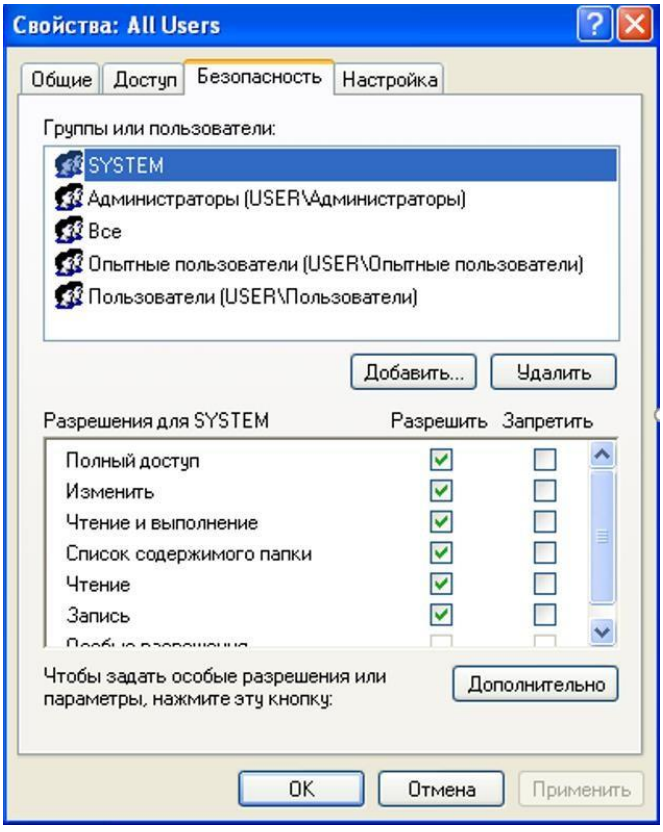

Рисунок № 50 – безопасность папки всех пользователей (Windows XP)

12. Ознакомиться (с помощью Панели управления Windows и редактора реестра) с порядком разграничения доступа к принтерам и разделам реестра. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта.

По умолчанию все пользователи могут посылать документы на печать на принтер. У каждого принтера существует три основных разрешения печати.

Печать — это разрешение позволяет пользователю или группе отправлять документы на принтер.

Управление принтерами — это разрешение позволяет пользователю или группе изменять свойства принтера, включая разрешения печати.

Управление документами — пользователи или группы, обладающие этим разрешением, могут приостанавливать, перезапускать или удалять любые документы в очереди принтера, независимо от их принадлежности.

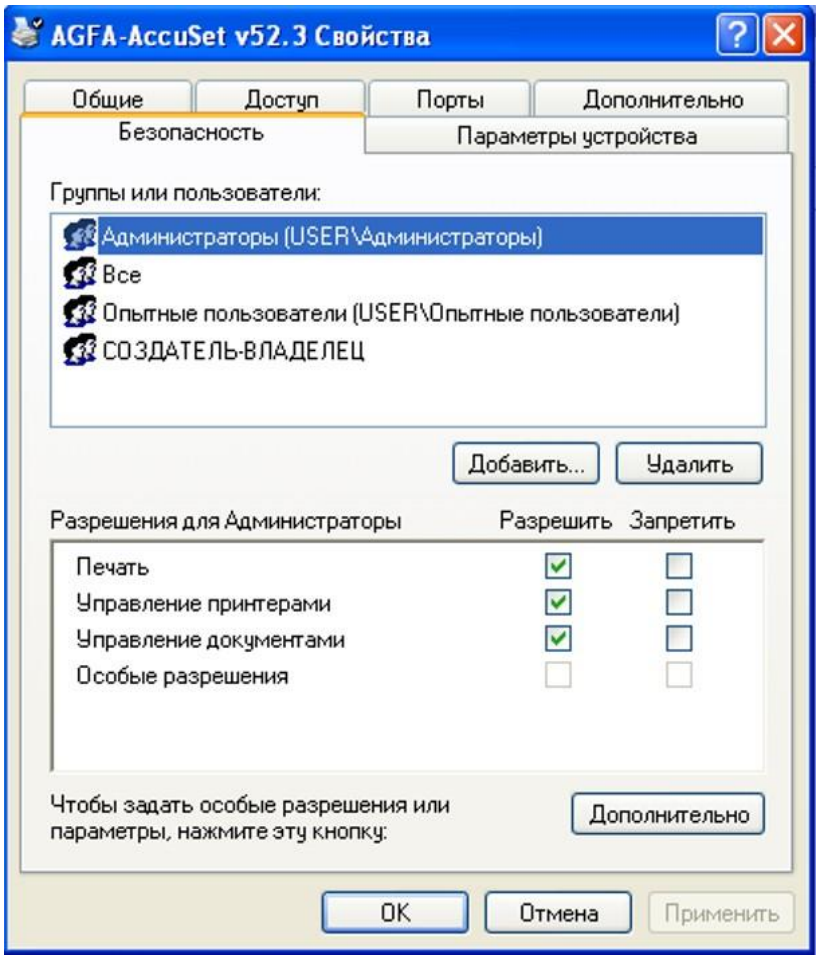

Рисунок № 51 – окно установки параметров безопасности для принтера (Windows XP)

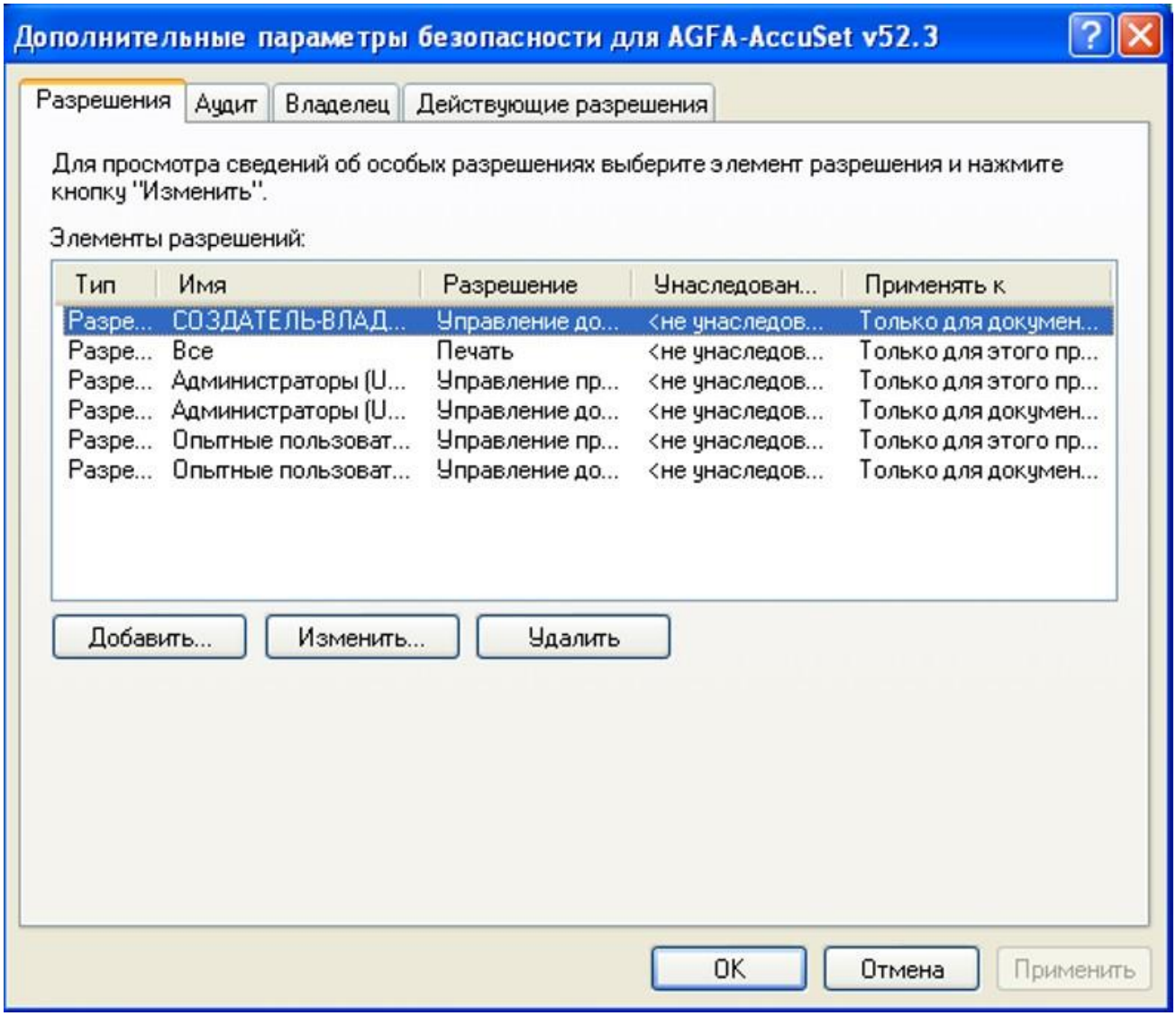

Рисунок № 52 – окно установки разрешений для принтера (Windows XP)

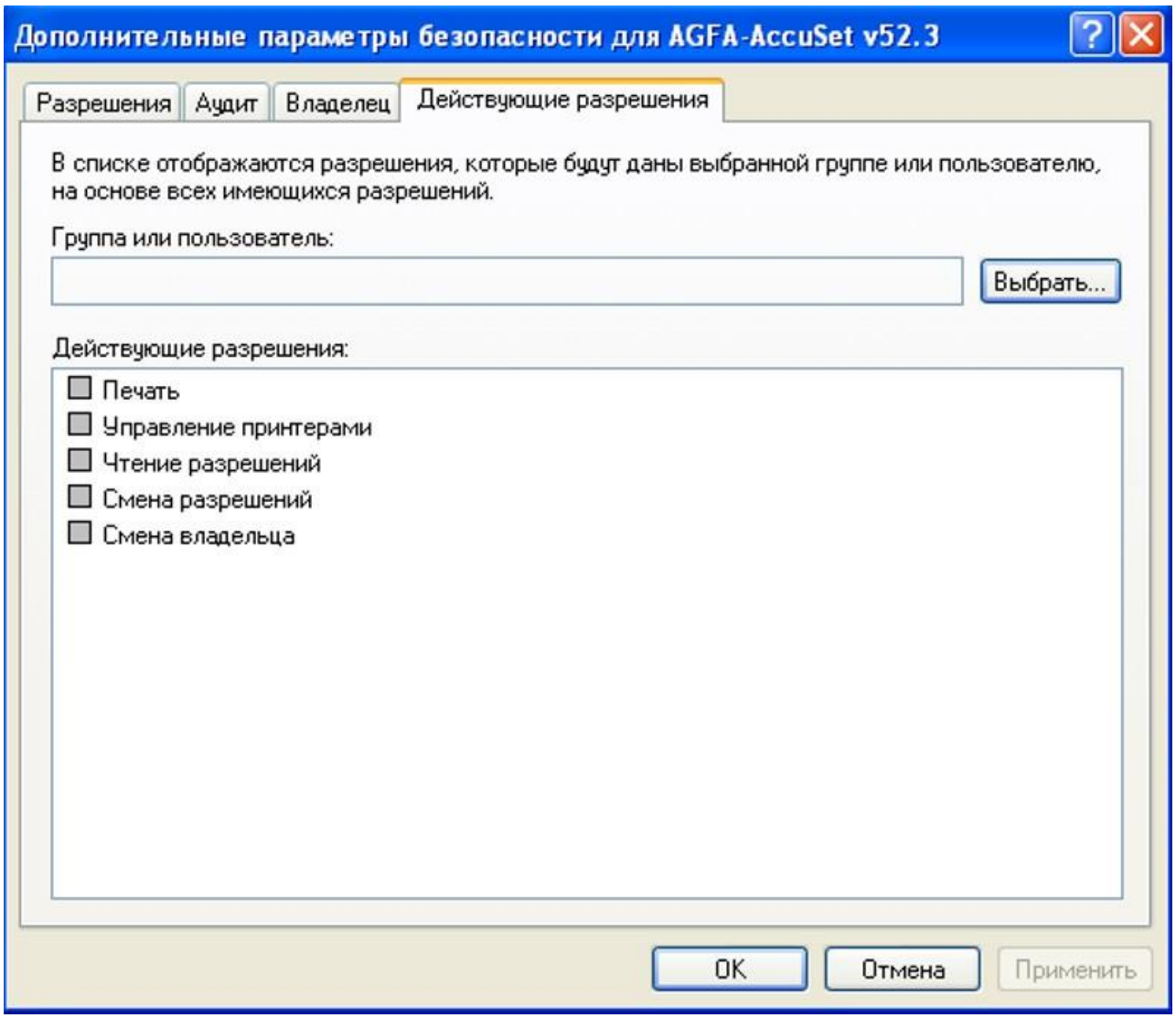

Рисунок № 53 – окно с действующими разрешения для принтера (Windows XP)

Для каждого раздела реестра можно настроить разрешения доступа на изменение, чтение, запись во вкладке «*Безопасность*». Настройки разделов реестра прав владельца и прав доступа работают по такому же принципу, как и аналогичные команды «*Проводника*» по установке прав доступа к файлам и каталогам.

Флажок	**Назначаемые права**
Запрос значения (*Query Value*)	Дает право чтения значимых элементов из раздела реестра
Задание значения (*Set Value*)	Дает право модифицировать значимый элемент в разделе реестра
Создание подраздела (*Create Subkey*)	Дает право создавать подразделы в

	выбранном разделе реестра
Перечисление подразделов (*Enumerate Subkey*)	Дает право идентифицировать подразделы выбранного раздела реестра
Уведомление (*Notify*)	Дает право установить аудит на разделы реестра
Создание связи (*Create Link*)	Дает право создавать символические ссылки в конкретном подразделе реестра
Удаление (*Delete*)	Дает право удаления выделенного раздела
Запись DAC (*Write DAC*)	Дает право получать доступ к разделу и создавать/модифицировать для него Список управления доступом (*Access Control List*, ACL)
Смена владельца (*Write Owner*)	Дает право присвоения прав владельца данного раздела
Чтение разрешений (*Read Control*)	Дает право просматривать параметры безопасности, установленные для данного раздела

Таблица № 1 - права доступа к разделу реестра

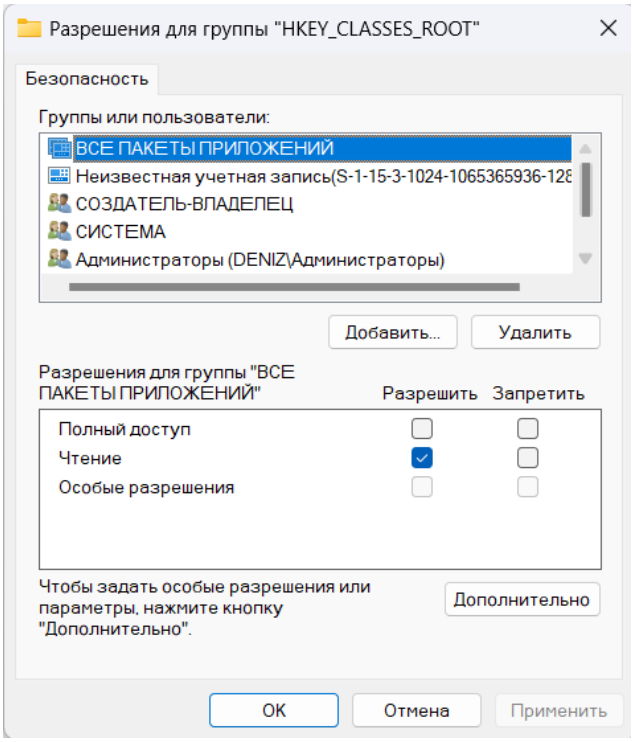

Рисунок № 54 – окно установки параметров безопасности раздела реестра (Windows 11)

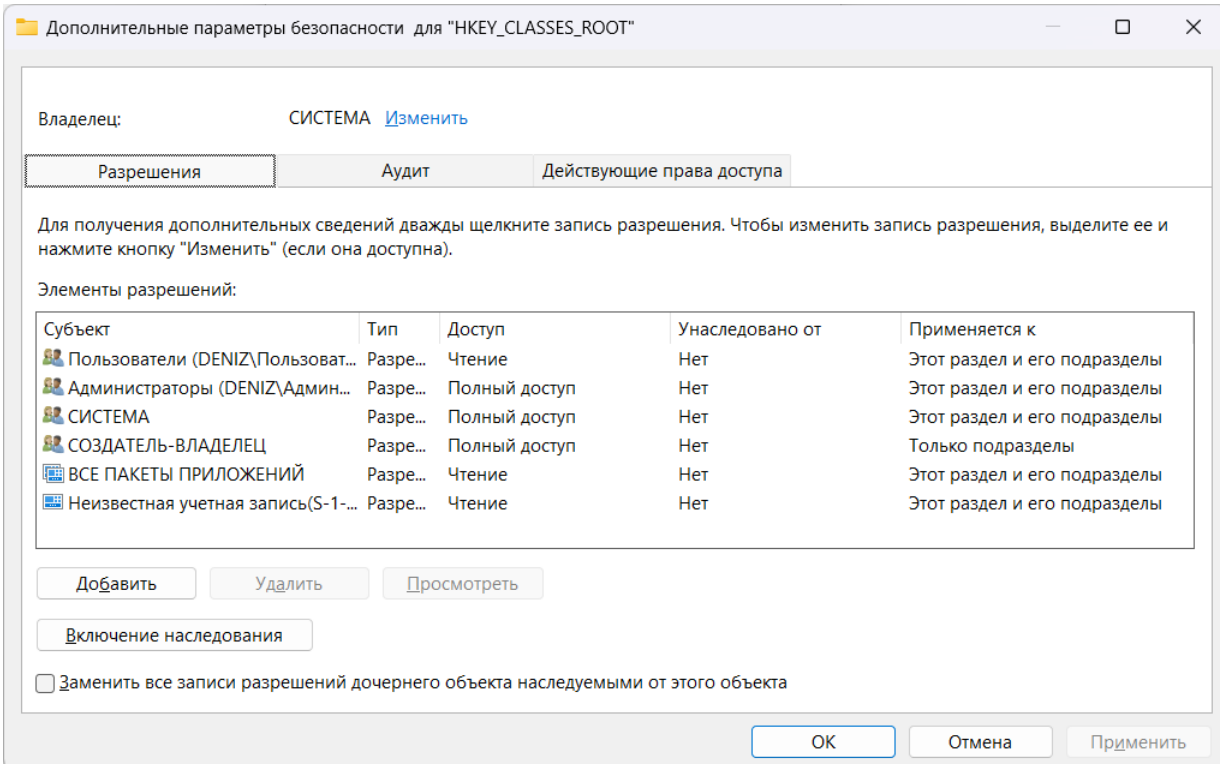

Рисунок № 55 – окно разрешений раздела реестра (Windows 11)

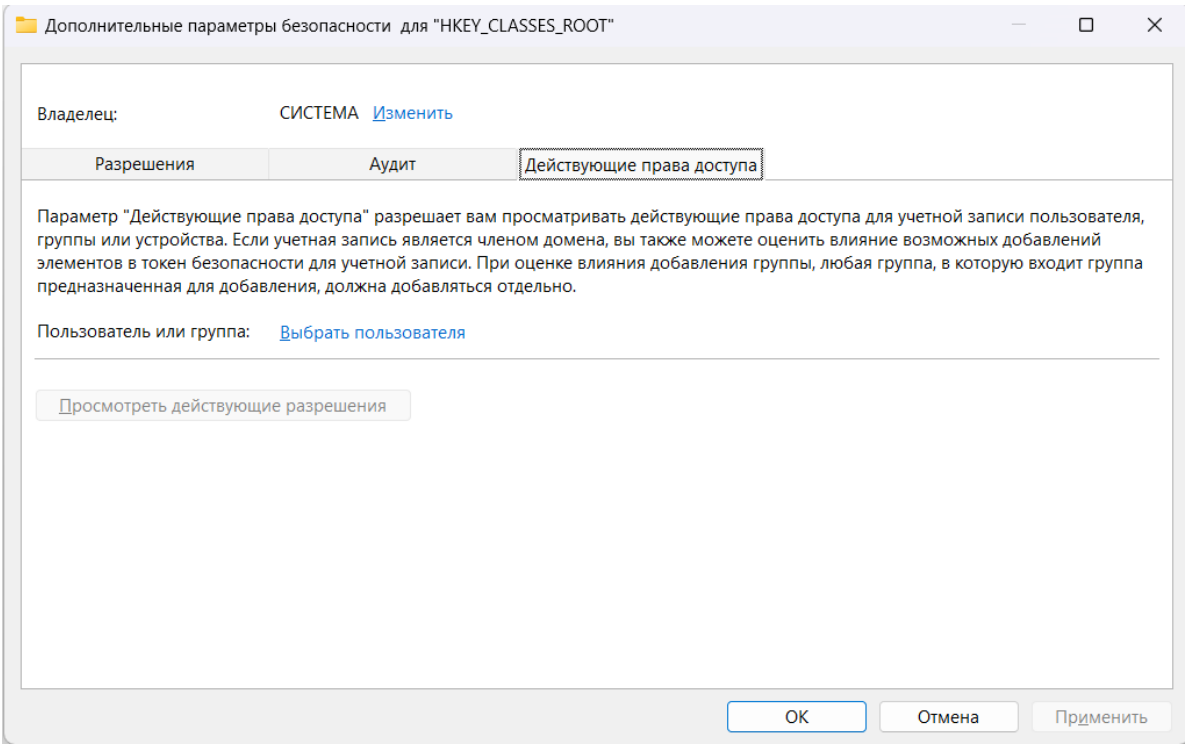

Рисунок № 56 – окно действующий разрешений раздела реестра (Windows 11)

13. Ознакомиться (с помощью функции Панели управления Администрирование | Управление компьютером) с порядком создания и изменения учетных записей пользователей и групп в защищенных версиях операционной системы Windows. Включить в отчет соответствующие сведения. Включить в электронную версию отчета копии соответствующих экранных форм.

Для управления локальными учетными записями пользователей предусмотрен один главный инструмент — *Computer Management*, который можно открыть из диспетчера серверов, выбрав в меню *Tools* пункт *Computer Management*. Оснастка «*Локальные пользователи и группы*» — это инструмент *MMC*. Он служит для создания пользователей и групп, хранимых локально на компьютере, и управления ими.

Запускать оснастку *Локальные пользователи и группы* может любой пользователь.

Выполнять администрирование учетных записей могут только администраторы и члены группы *Опытные пользователи*.

Основные действия по администрированию локальных пользователей:

- создание локальной учетной записи пользователя;
- сброс пароля для локальной учетной записи пользователя;
- отключение или активация локальной учетной записи пользователя;
- удаление локальной учетной записи пользователя;
- переименование локальной учетной записи пользователя;
- назначение сценария входа для локальной учетной записи пользователя;
- назначение домашней папки локальной учетной записи пользователя.

Основные действия по администрированию локальных групп:

- создание локальной группы;
- добавление члена в локальную группу;
- идентификация членов локальной группы;
- удаление локальной группы.

Сразу после установки системы *Windows* папка Пользователи содержит две встроенные учетные записи — *Администратор* и *Гость*. Они создаются автоматически при установке *Windows*. Ниже даны описания свойств обеих встроенных учетных записей:

- **Администратор** — эту учетную запись используют при установке и настройке рабочей станции или сервера, являющегося членом домена. Она не может быть

уничтожена, блокирована или удалена из группы *Администраторы*, ее можно только переименовать;

- **Гость** — эта учетная запись применяется для регистрации в компьютере без использования специально созданной учетной записи. Учетная запись *Гость* не требует ввода пароля и по умолчанию блокирована. Она является членом группы *Гости*. Ей можно предоставить права доступа к ресурсам системы точно так же, как любой другой учетной записи;
- **Администраторы** — ее члены обладают полным доступом ко всем ресурсам системы. Это единственная встроенная группа, автоматически предоставляющая своим членам весь набор встроенных прав;
- **Операторы архива** — члены этой группы могут архивировать и восстанавливать файлы в системе независимо от того, какими правами эти файлы защищены. Кроме того, операторы архива могут входить в систему и завершать ее работу, но они не имеют права изменять настройки безопасности;
- **Гости** — эта группа позволяет выполнить регистрацию пользователя с помощью учетной записи *Гость* и получить ограниченные права на доступ к ресурсам системы. Члены этой группы могут завершать работу системы;
- **Опытные пользователи** — члены этой группы могут создавать учетные записи пользователей, но они имеют право модифицировать настройки безопасности только для созданных ими учетных записей. Кроме того, они могут создавать локальные группы и модифицировать состав членов созданных ими групп. То же самое они могут делать с группами *Пользователи*, *Гости* и *Опытные пользователи*. Члены группы *Опытные пользователи* не могут модифицировать членство в группах *Администраторы* и *Операторы архива*. Они не могут быть владельцами файлов, архивировать или восстанавливать каталоги, загружать и выгружать драйверы устройств и модифицировать настройки безопасности и журнал событий;
- **Репликатор** — членом группы *Репликатор* должна быть только учетная запись, с помощью которой можно зарегистрироваться в службе репликации контроллера домена. Ее членами не следует делать рабочие учетные записи;
- **Пользователи** — члены этой группы могут выполнять большинство пользовательских функций, например, запускать приложения, пользоваться локальным или сетевым принтером, завершать работу системы или блокировать рабочую станцию. Они также могут создавать локальные группы и регулировать состав их членов. Они не могут получить доступ к общему каталогу или создать локальный принтер.

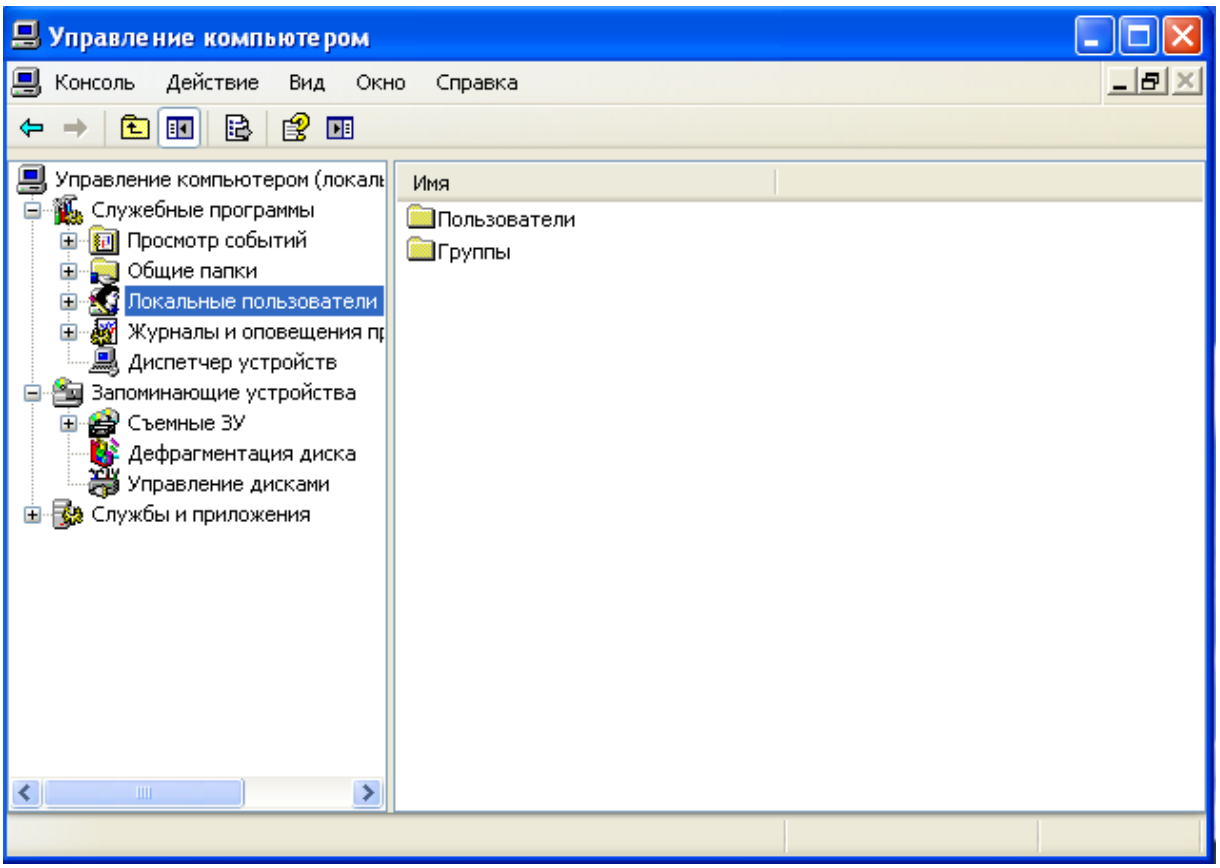

Рисунок № 57 – локальные пользователи в реестре (Windows XP)

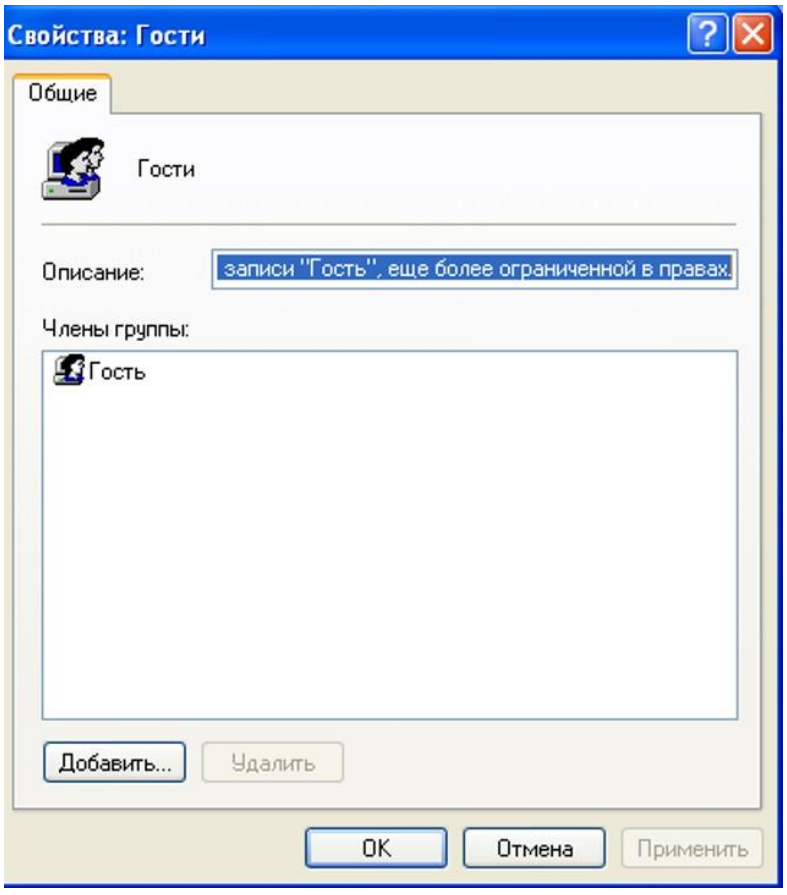

Рисунок № 58 – свойство группы (Windows XP)

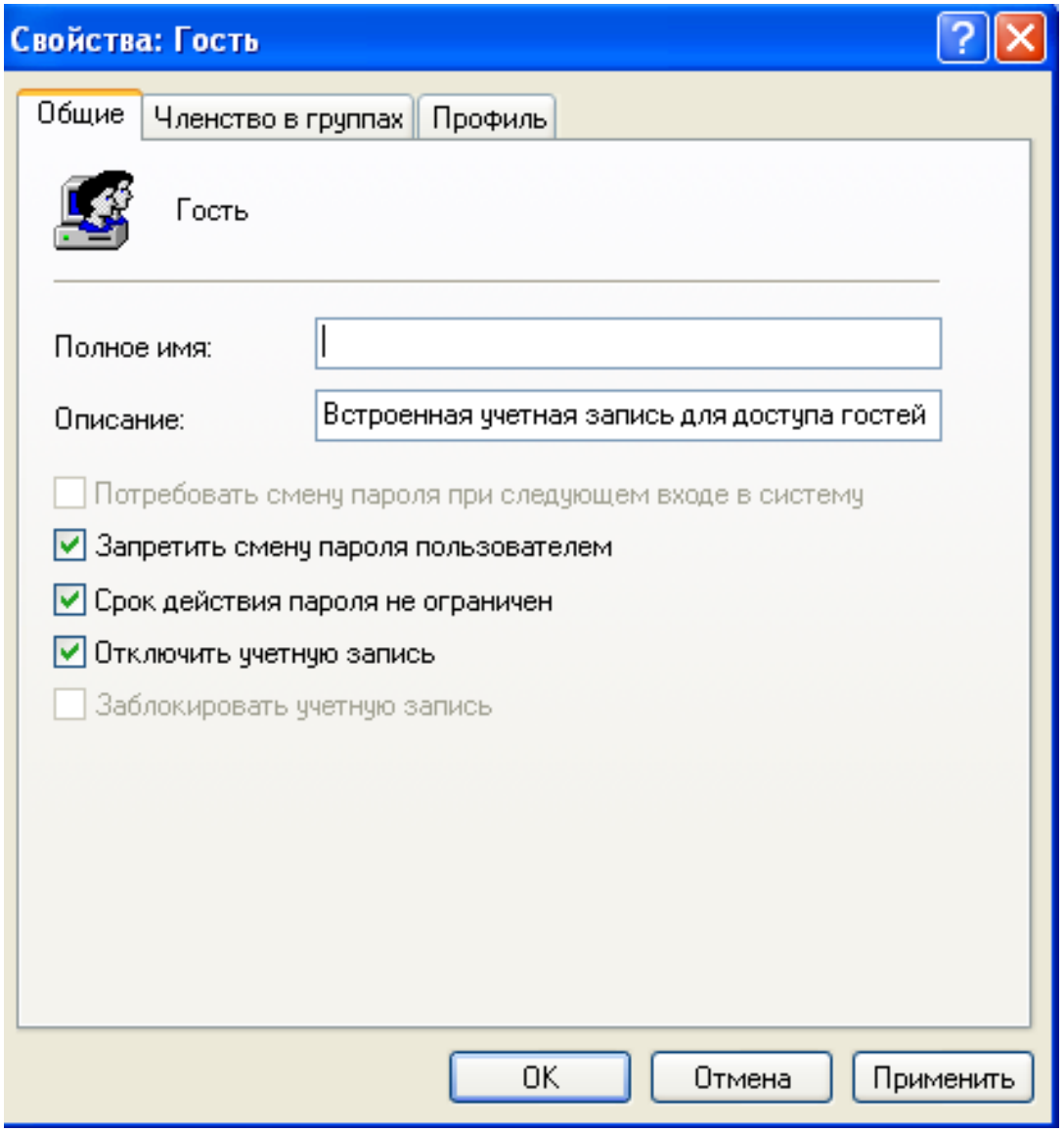

Рисунок № 59 – свойство пользователя (Windows XP)

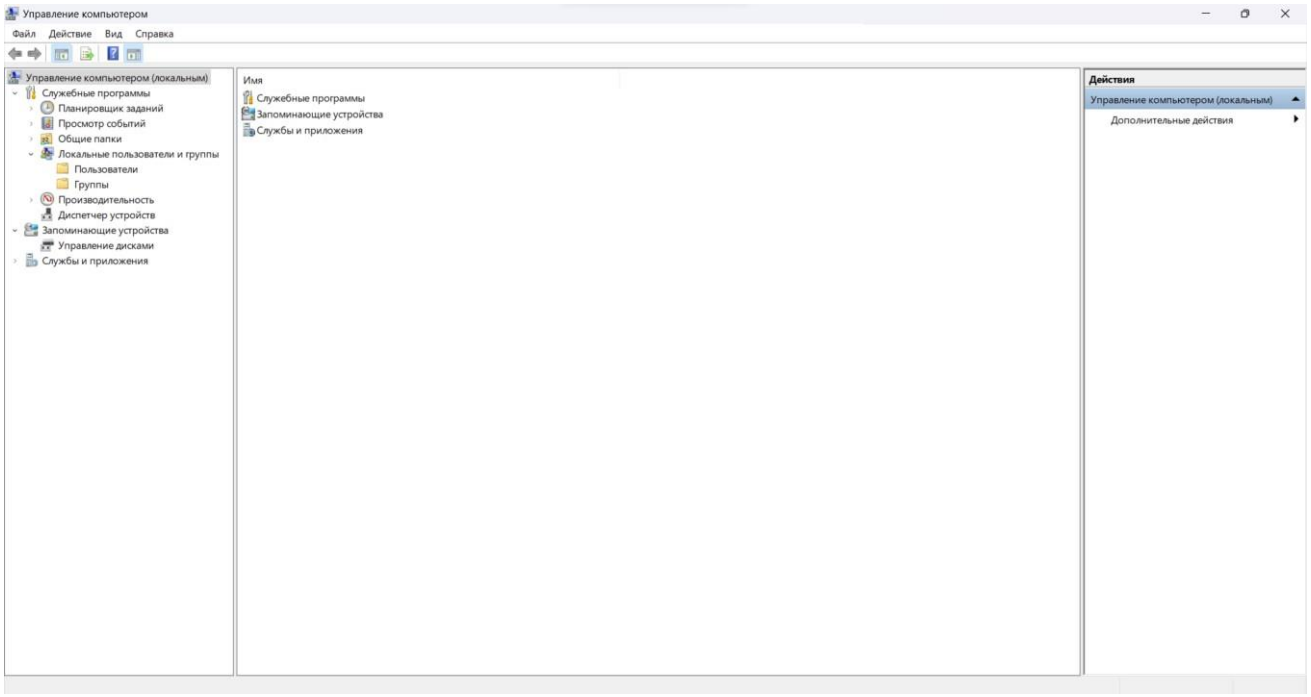

Рисунок № 60 – управление компьютером (Windows 11)

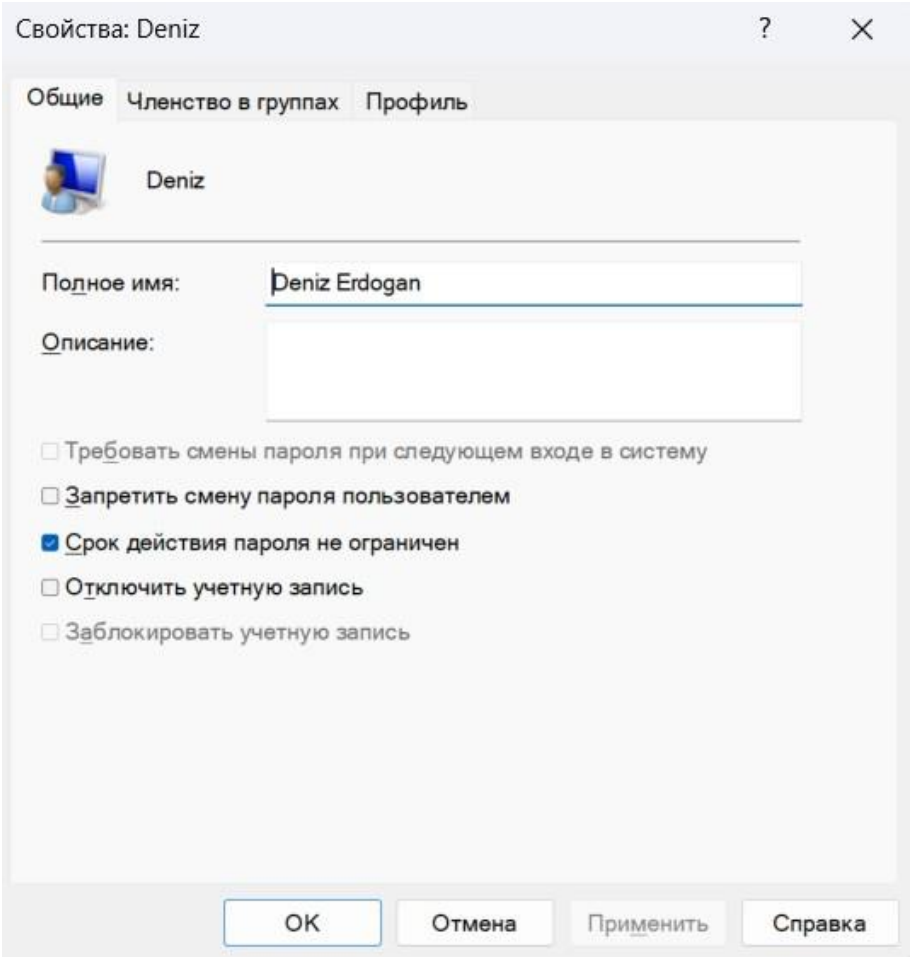

Рисунок № 61 – свойство пользователя (Windows 11)

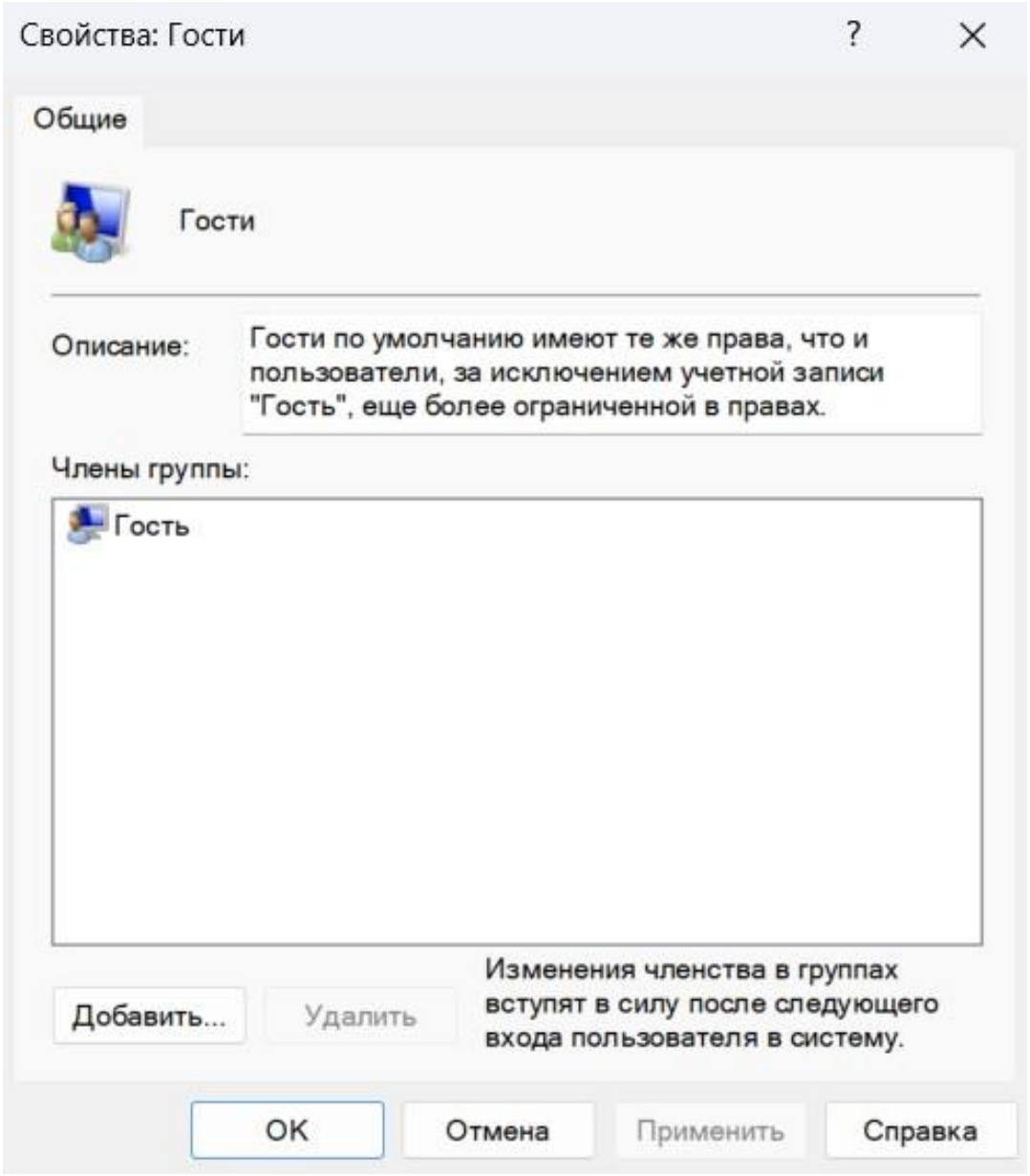

Рисунок № 62 – свойство группы (Windows 11)

14. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Локальные политики | Назначение прав пользователя) с порядком назначения прав пользователям и группам. Включить в отчет соответствующие сведения. Включить в электронную версию отчета копии соответствующих экранных форм.

Назначение прав пользователям и группам устанавливается настройкой локальной политики.

Параметр	Пояснение
Запретить вход в систему через службы удаленных рабочих столов	Этот параметр безопасности определяет, каким пользователям и группам будет запрещено входить в систему как клиенту служб удаленных рабочих столов.
Запретить локальный вход	Этот параметр безопасности определяет, каким пользователям будет отказано во входе в систему. Этот параметр политики заменяет параметр "*Разрешить локальный вход в систему*", если к учетной записи применяются обе политики.
Отказать в доступе к этому компьютеру из сети	Этот параметр безопасности определяет, каким пользователям будет отказано в доступе к компьютеру из сети. Этот параметр заменяет параметр политики "*Разрешить доступ к компьютеру из сети*", если к учетной записи пользователя применяются об политики.
Разрешить вход в систему через службы удаленных рабочих столов	Этот параметр безопасности определяет, у каких пользователей или групп есть разрешение на вход в систему в качестве клиента служб удаленных рабочих столов.
Управление аудитом и журналом безопасности	Этот параметр безопасности определяет, какие пользователи могут указывать параметры аудита доступа к объектам для отдельных ресурсов, таких как файлы, объекты *Active Directory* и разделы реестра. Данный параметр безопасности не разрешает пользователю включить аудит доступа к файлам и объектам в целом. Для включения такого аудита нужно настроить параметр доступа к объекту "*Аудит*" в пути

	"*Конфигурация компьютера\Параметры Windows\Параметры безопасности\Локальные политики\Политики аудита*".

Таблица № 2 – основные права пользователя

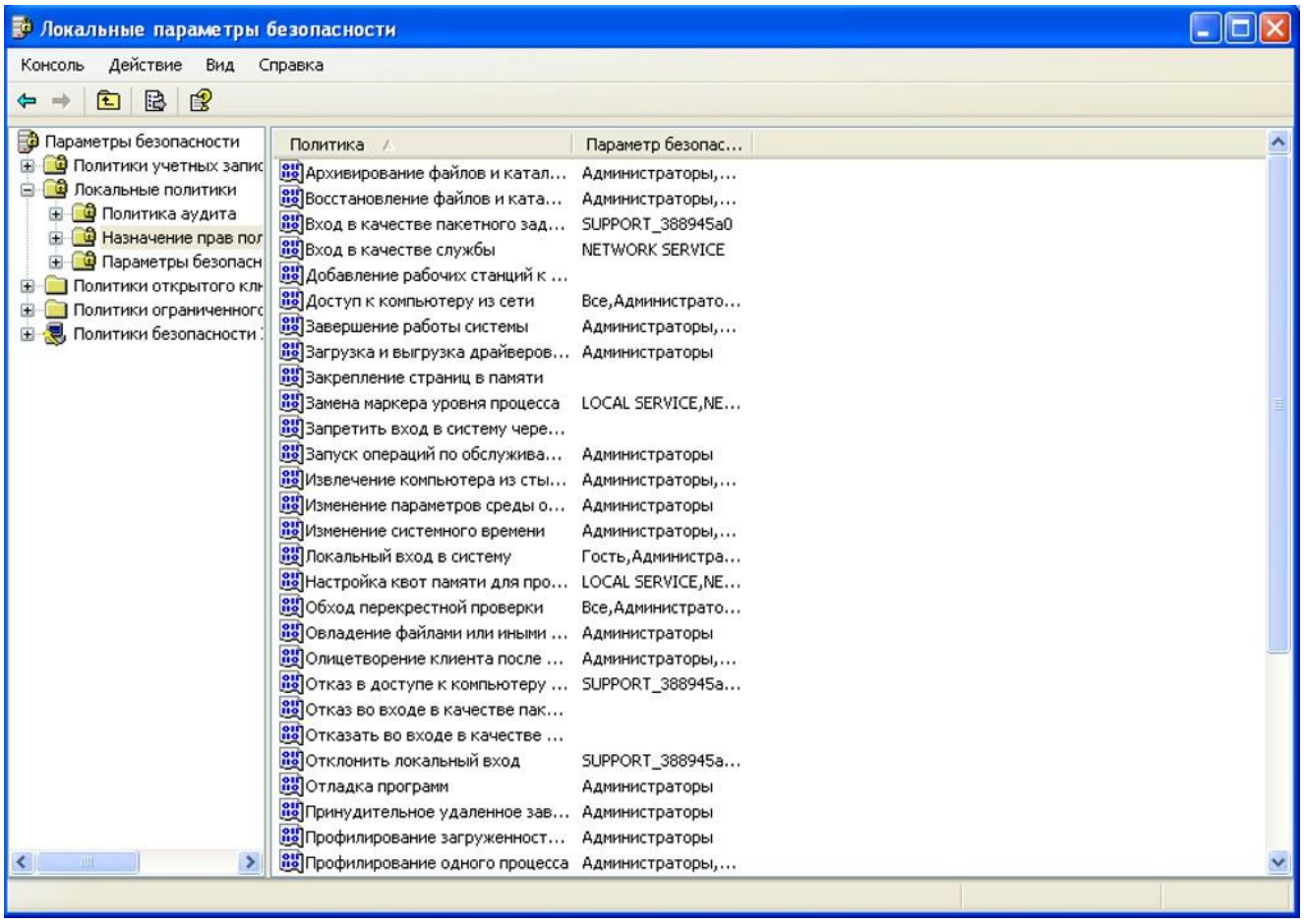

Рисунок № 63 – окно назначения прав пользователя (Windows XP)

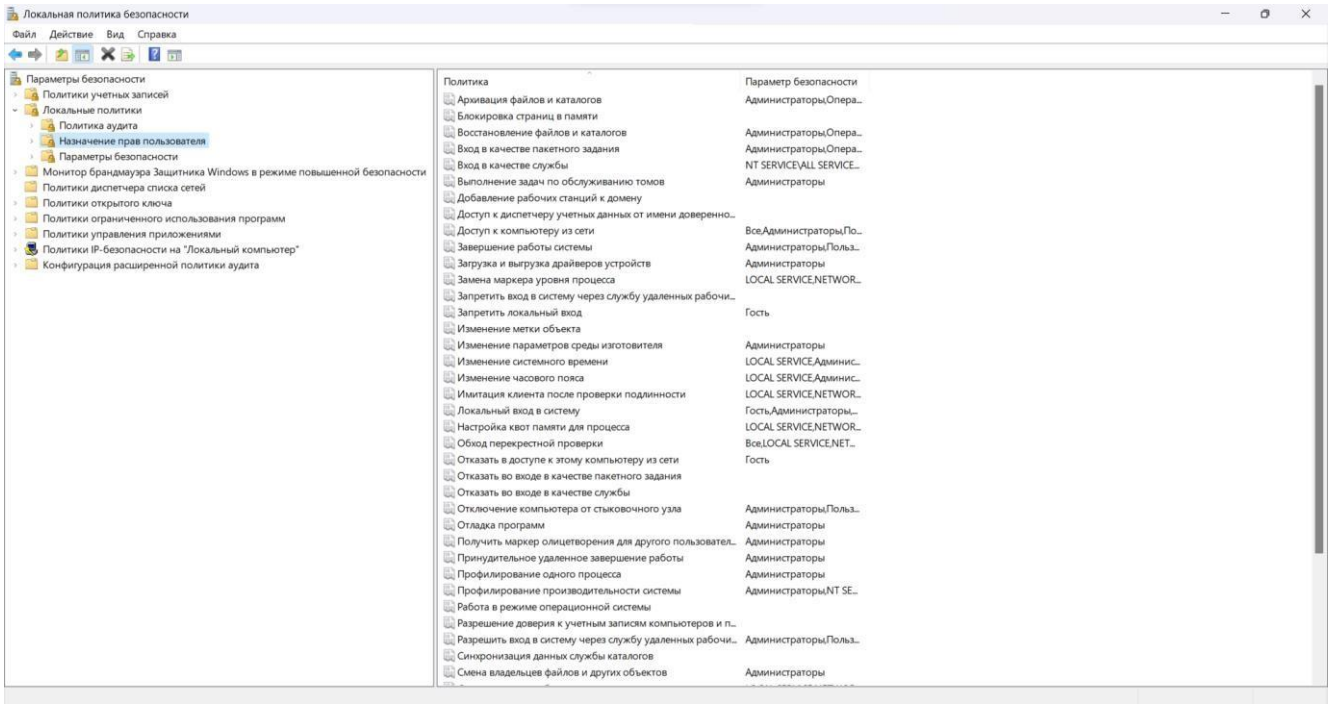

Рисунок № 64 – окно назначения прав пользователя (Windows 11)

15. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Политики учетных записей | Политика паролей) с порядком определения параметров безопасности для парольной аутентификации. Включить в отчет соответствующие сведения. Включить в электронную версию отчета копии соответствующих экранных форм.

Политики паролей операционной системы *Windows* позволяют довольно гибко настроить ограничения по выбору паролей для пользователей Windows. Политики паролей позволяют настроить минимальную длину паролей, их сложность и многие другие параметры.

К данным политикам относятся:

1. **Аудит минимальной длины пароля** - этот параметр безопасности определяет минимальную длину пароля, для которой создаются события предупреждения аудита длины пароля. Этот параметр может иметь значение от 1 до 128. Параметр следует включать и настраивать только при определении возможного воздействия увеличения минимальной длины пароля в вашей среде.
    - Если этот параметр не определен, события аудита не создаются;

- Если этот параметр определен и не превышает минимальное значение параметра минимальной длины пароля или равно ему, события аудита не создаются;
- Если этот параметр определен и превышает значение параметра минимальной длины пароля, а длина нового пароля учетной записи меньше значения этого параметра, создается событие аудита.

2. **Вести журнал паролей** - 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;
   - ✓ Эта политика позволяет администраторам улучшать безопасность, гарантируя, что старые пароли не будут повторно использоваться постоянно.
3. **Максимальный срок действия пароля -** этот параметр безопасности определяет период времени (в днях), в течение которого можно использовать пароль, пока система не потребует от пользователя сменить его.
   - ✓ Срок действия пароля может составлять от 1 до 999 дней;
   - ✓ Значение 0 соответствует неограниченному сроку действия пароля;
   - ✓ Если значение максимального срока действия пароля составляет от 1 до 999 дней, то значение минимального срока действия пароля должно быть меньше максимального;
   - ✓ Если значение максимального срока действия пароля равно 0, то минимальный срок действия пароля может принимать любые значения в диапазоне от 0 до 998 дней.
4. **Минимальная длина пароля** - этот параметр безопасности определяет минимальное количество знаков, которое должно содержаться в пароле пользователя.
   - ✓ Максимальное значение для этого параметра зависит от значения параметра "Ослабить ограничение минимальной длины пароля";
   - ✓ Если параметр "Ослабить ограничение минимальной длины пароля" не определен, этому параметру можно присвоить значение от 0 до 14;
   - ✓ Если параметр "Ослабить ограничение минимальной длины пароля" определен и отключен, этому параметру можно присвоить значение от 0 до 14;

- ✓ Если параметр "Ослабить ограничение минимальной длины пароля" определен и включен, этому параметру можно присвоить значение от 0 до 128;
- ✓ Если присвоить этому параметру значение 0, пароль не требуется.

5. **Минимальный срок действия пароля** - этот параметр безопасности определяет период времени (в днях), в течение которого необходимо использовать пароль, прежде чем пользователь сможет его изменить.
   - ✓ Можно установить значение от 1 до 998 дней либо разрешить изменять пароль сразу, установив значение 0 дней;
   - ✓ Минимальный срок действия пароля должен быть меньше максимального, кроме случая, когда максимальный срок равен 0 дней и, следовательно, срок действия пароля никогда не истечет;
   - ✓ Если максимальный срок действия пароля равен 0 дней, то минимальный срок может принимать любые значения в диапазоне от 0 до 998 дней;
   - ✓ Установите значение минимального срока действия пароля больше 0, если вы хотите включить ведение журнала паролей;
   - ✓ Без установки минимального срока действия пароля пользователь может изменять пароли повторно, пока не получит свой старый предпочитаемый пароль. На значение по умолчанию эта рекомендация не распространяется, благодаря чему администратор может назначить пользователю пароль, а затем потребовать, чтобы пользователь сменил его при входе в систему;
   - ✓ Если для журнала паролей установлено значение 0, пользователю не нужно выбирать новый пароль. По этой причине значение для журнала паролей по умолчанию равно 1.
6. **Ослабить ограничение минимальной длины пароля** - этот параметр определяет, можно ли увеличить минимальную длину пароля выше предыдущего ограничения в 14 символов.
   - Если этот параметр не определен, минимальной длине пароля можно присвоить максимальное значение не более 14;
   - Если этот параметр определен и отключен, минимальная длина пароля может быть не более 14;
   - Если этот параметр определен и включен, минимальная длина пароля может быть больше 14.

7. **Пароль должен отвечать требованиям сложности** - этот параметр безопасности определяет, должен ли пароль отвечать требованиям сложности.
    - ✓ Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям;
    - ✓ Не содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков;
    - ✓ Иметь длину не менее 6 знаков;
    - ✓ Содержать знаки трех из четырех перечисленных ниже категорий:
        - Латинские заглавные буквы (от A до Z);
        - Латинские строчные буквы (от a до z);
        - Цифры (от 0 до 9);
        - Отличающиеся от букв и цифр знаки (например, !, $, #, %).

Требования сложности применяются при создании или изменении пароля.

8. **Хранить пароли, используя обратимое шифрование** - этот параметр безопасности определяет, используется ли операционной системой для хранения паролей обратимое шифрование.
    - ✓ Эта политика обеспечивает поддержку приложений, использующих протоколы, требующие знание пароля пользователя для проверки подлинности. Хранение паролей с помощью обратимого шифрования - по существу то же самое, что и хранение паролей открытым текстом. По этой причине данная политика не должна применяться, пока требования приложения не станут более весомыми, чем требования по защите паролей;
    - ✓ Эта политика необходима при использовании проверки подлинности протокола *CHAP* через удаленный доступ или службу проверки подлинности в Интернете (IAS). Она также необходима при использовании краткой проверки подлинности в *IIS*.

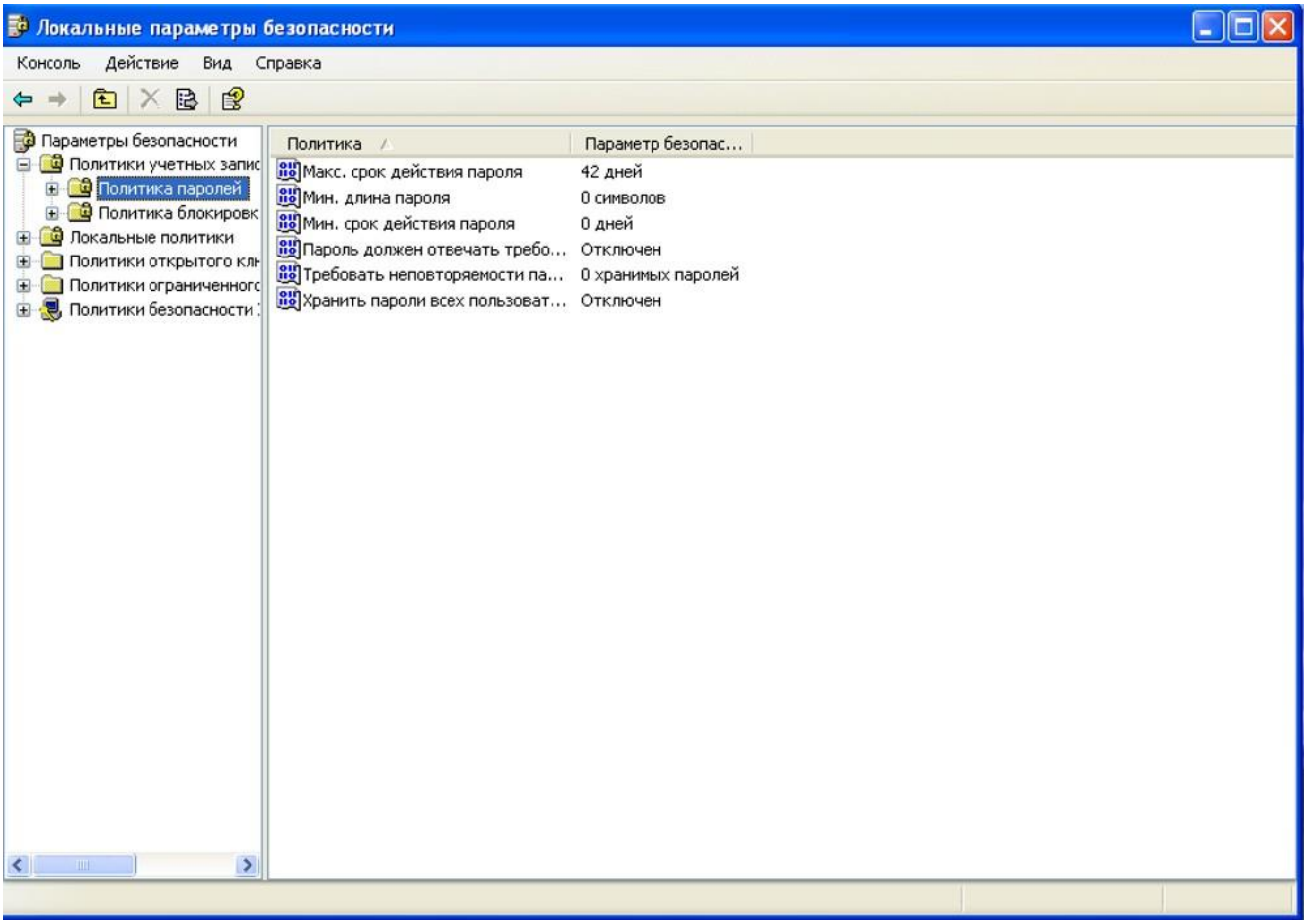

Рисунок № 64 – окно установки политики паролей (Windows XP)

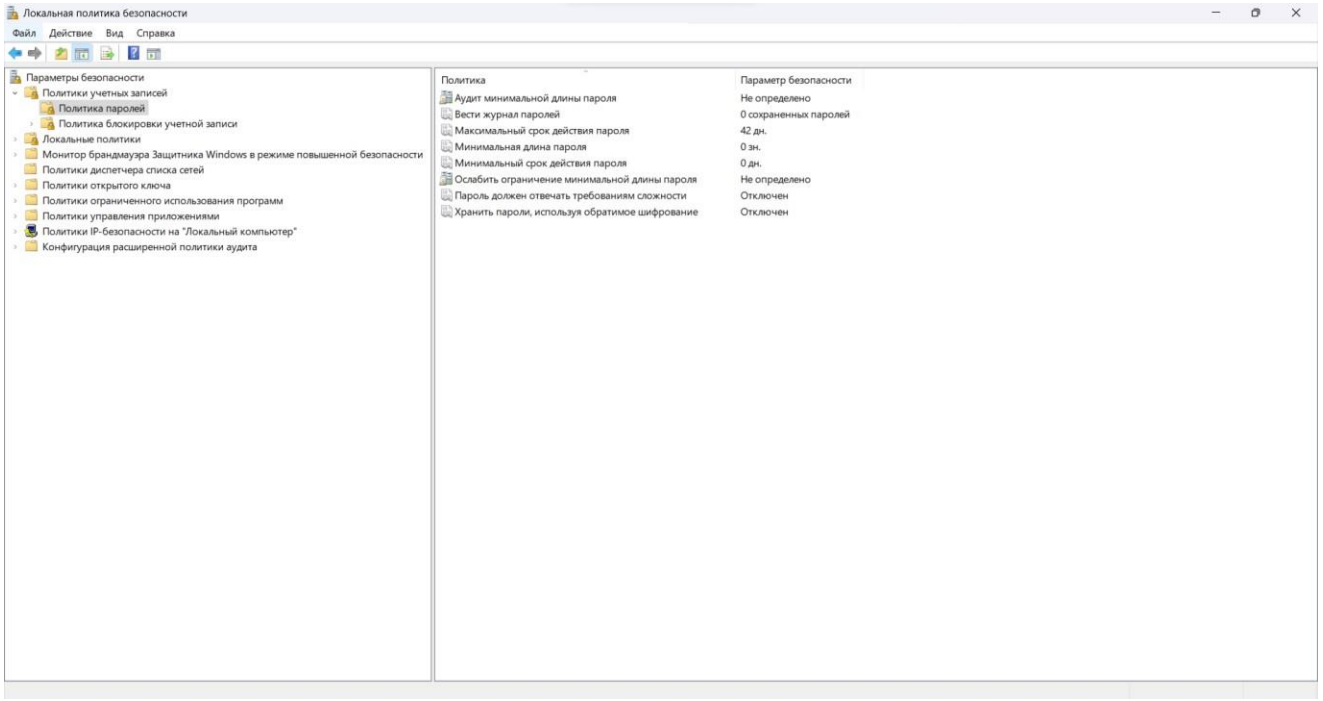

Рисунок № 65 – окно установки политики паролей (Windows 11)

16. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Политики учетных записей | Политика блокировки учетных записей) с порядком определения параметров безопасности для политики блокировки учетных записей. Включить в отчет соответствующие сведения. Включить в электронную версию отчета копии соответствующих экранных форм.

Параметры политики блокировки учетных записей:

1) **Время до сброса счетчика блокировки** - этот параметр безопасности определяет количество минут, которые должны пройти после неудачной попытки входа в систему до того, как счетчик неудачных попыток входа будет сброшен до 0.
   - ✓ Допустимые значения: от 1 до 99999 минут;
   - ✓ Если определено пороговое значение блокировки учетной записи, то время сброса должно быть меньше или равно длительности блокировки учетной записи.
2) **Пороговое значение блокировки** - этот параметр безопасности 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 этой учетной записи;
   - ✓ Количество неудачных попыток входа в систему может составлять от 0 до 999;
   - ✓ Если установить это значение равным 0, то учетная запись никогда не будет разблокирована;
   - ✓ Неудачные попытки ввода паролей на рабочих станциях или серверах-членах домена, заблокированных с помощью клавиш *CTRL+ALT+DELETE* или с помощью защищенных паролем заставок, считаются неудачными попытками входа в систему.
3) **Продолжительность блокировки учетной записи** - этот параметр безопасности определяет количество минут, в течение которых учетная запись остается заблокированной до ее автоматической разблокировки.
   - ✓ Допустимые значения: от 0 до 99999 минут;

- ✓ Если продолжительность блокировки учетной записи равна 0, то учетная запись будет заблокирована до тех пор, пока администратор не разблокирует ее;
- ✓ Если определено пороговое значение блокировки учетной записи, то длительность блокировки учетной записи должна быть больше или равна времени сброса.

4) **Разрешить блокировку учетной записи администратора** - этот параметр безопасности определяет, регулируется ли встроенная учетная запись администратора политикой блокировки учетных записей.

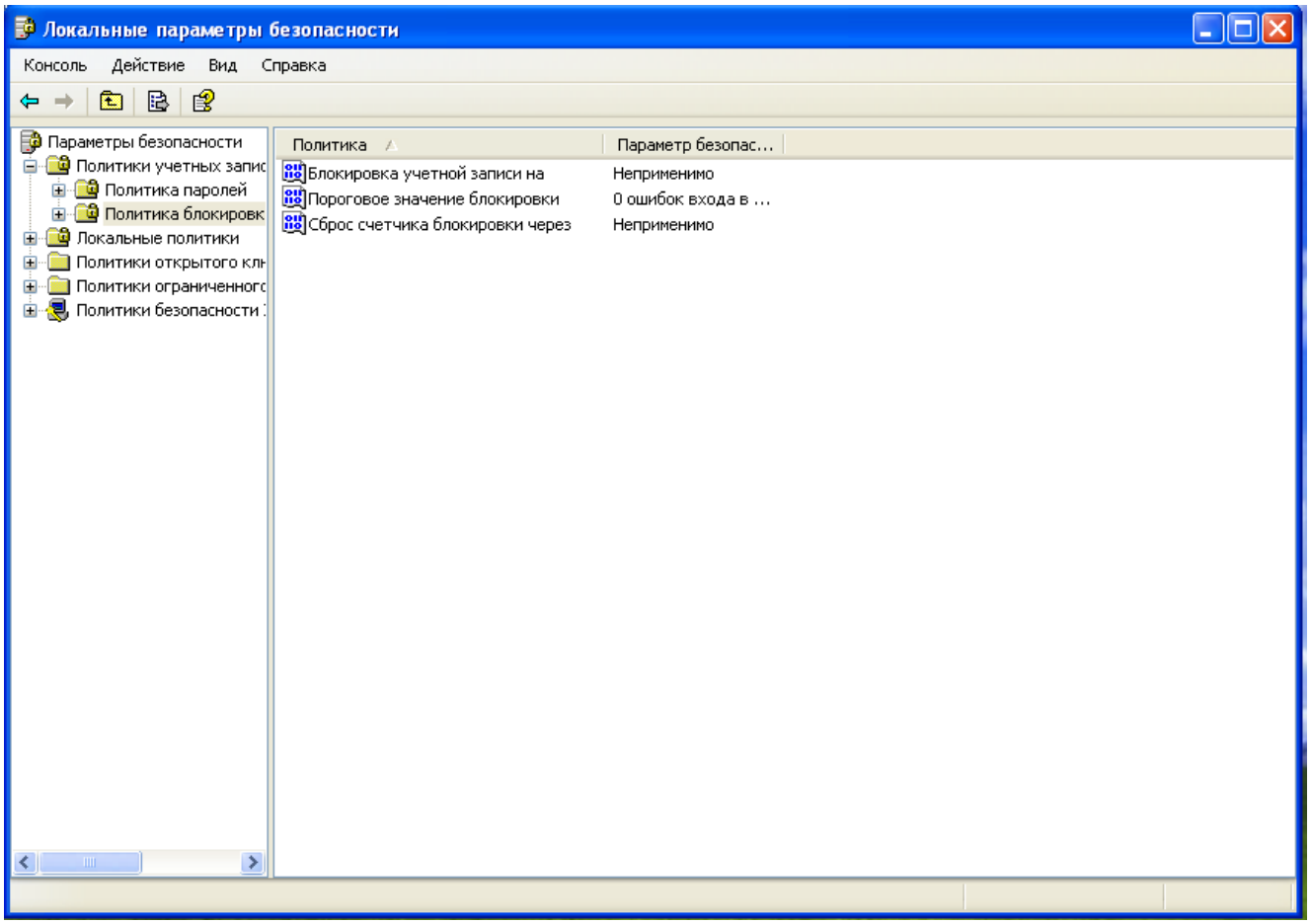

Рисунок № 66 – окно настройки политики блокировки учётных записей (Windows XP)

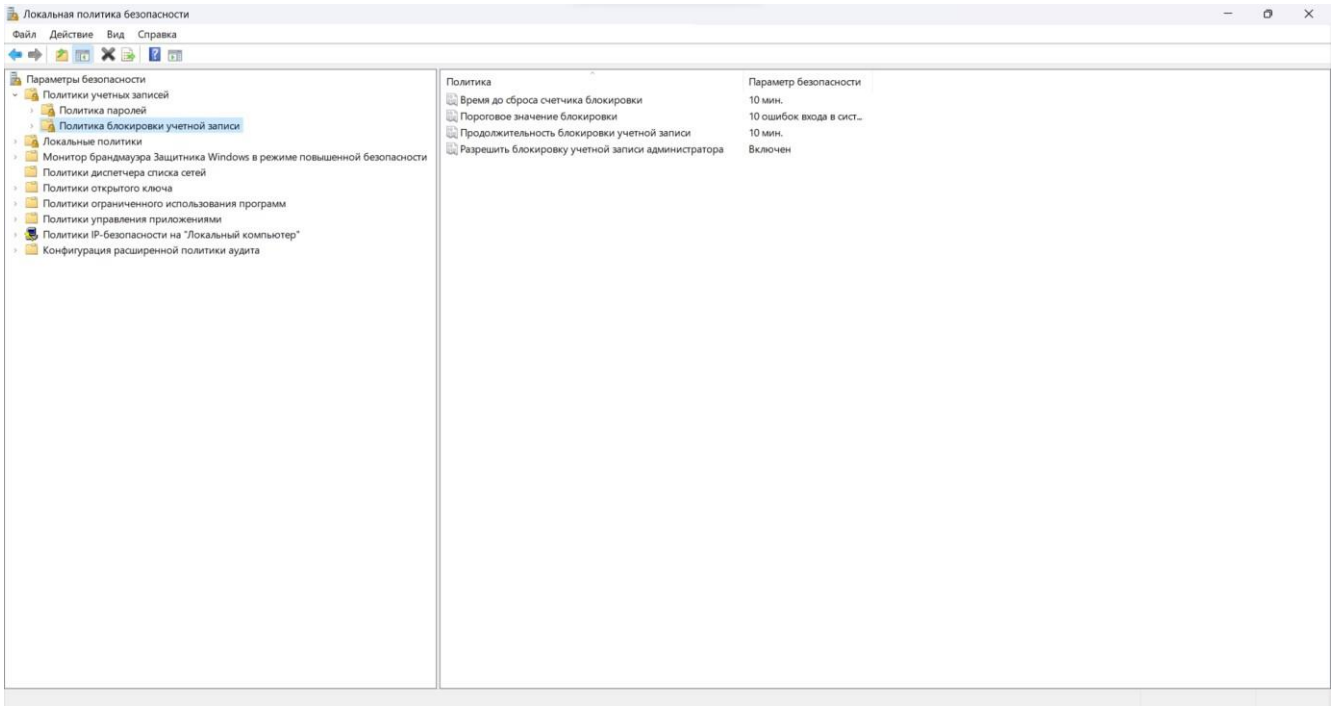

Рисунок № 67 – окно настройки политики блокировки учётных записей (Windows 11)

17. Включить в отчет ответы на контрольные вопросы, номера которых выбираются в соответствии с номером варианта.

Как реализована (в чем выражается) защита базы данных паролей программы whisper.exe?

Защита базы данных паролей в программе *Whisper.exe* реализуется через шифрование и кодирование хранящейся информации. Конкретные методы, используемые в *Whisper.exe*, могут включать в себя следующие подходы:

1. Использование криптографических алгоритмов для шифрования паролей перед их сохранением в базе данных. Это может включать алгоритмы симметричного шифрования, такие как *AES*, или более сложные алгоритмы, например криптосистемы с открытым ключом;
2. Применение хеширования паролей вместо их хранения в открытом виде. Хеширование создает необратимое и случайное отображение исходного пароля, которое затем сохраняется в базе данных вместо самого пароля;
3. Кодирование паролей с использованием надежных схем, таких как *bcrypt* или *PBKDF2*, для обеспечения дополнительного уровня защиты;

4. Защита базы данных паролем или сертификатом для предотвращения несанкционированного доступа;
5. Ограничение доступа к базе данных паролей на основе ролей и привилегий пользователей;
6. Регулярное резервное копирование базы данных для восстановления в случае потери или повреждения данных.

Какая модель разграничения доступа к объектам реализована в защищенных версиях операционной системы Windows?

В защищенных версиях операционной системы Windows, таких как Windows Server с функцией "*Role-Based Access Control*", реализована модель разграничения доступа к объектам. *RBAC* (ролевой контроль доступа) предоставляет механизм управления доступом на основе ролей пользователей или субъектов в системе.

В рамках *RBAC* пользователи или субъекты назначаются определенным ролям, и каждая роль имеет свои права доступа к объектам системы. Это обеспечивает более гибкий и централизованный способ управления доступом к ресурсам и данным. Администраторы могут легко изменять права доступа, назначать или отзывать роли для пользователей, и таким образом эффективно разграничивать доступ к различным объектам в системе.

RBAC является важным элементом безопасности в многих современных операционных системах и приложениях, и он помогает предотвращать несанкционированный доступ к данным и ресурсам, обеспечивая более точное управление доступом на уровне ролей и политик.

Какие установлены разрешения на доступ к разделу реестра HKEY_LOCAL_MACHINE и почему?

Установленные разрешения на доступ к разделу реестра *HKEY_LOCAL_MACHINE* зависят от настроек безопасности операционной системы. Обычно, этот раздел реестра является защищенным и доступ к нему имеют только администраторы системы или пользователи с правами администратора.

Причины установки ограниченных разрешений на доступ к *HKEY_LOCAL_MACHINE* включают:

1. Безопасность: *HKEY_LOCAL_MACHINE* содержит информацию о системной конфигурации, установленных программ и параметрах операционной системы. Ограниченный доступ к этому разделу реестра

предотвращает несанкционированные изменения или повреждение системных файлов;

2. Предотвращение вредоносных программ: Злоумышленники могут использовать доступ к *HKEY_LOCAL_MACHINE* для внесения изменений, отключения антивирусных программ или внедрения вирусов. Ограничение доступа помогает предотвратить такие атаки;
3. Разделение полномочий: Защищенный доступ к *HKEY_LOCAL_MACHINE* позволяет разделять полномочия между администраторскими учетными записями и учетными записями обычных пользователей. Это позволяет предотвратить несанкционированные изменения системы со стороны пользователей, не имеющих соответствующих полномочий.

В целом, установка ограниченных разрешений на доступ к *HKEY_LOCAL_MACHINE* помогает обеспечить безопасность и стабильность операционной системы, предотвращая несанкционированные изменения и атаки со стороны злоумышленников.

Кто управляет разрешениями на доступ к принтерам и почему?

Разрешения на доступ к принтерам управляются администраторами сети или системными администраторами. Они имеют эти полномочия, поскольку принтеры обычно подключены к сети, а необходимость доступа к ним может быть ограничена в целях безопасности или рационального использования ресурсов.

Администраторы имеют возможность назначать разрешения на доступ к принтерам для отдельных пользователей или групп пользователей, устанавливать ограничения на количественное использование принтеров и проводить другие настройки для эффективного управления печатными ресурсами.

Какие параметры могут быть установлены для политики блокировки учетных записей?

Для политики блокировки учетных записей Windows могут быть установлены следующие параметры:

- ✓ Период блокировки: определяет время, на протяжении которого учетная запись будет заблокирована после нескольких неудачных попыток входа;

- ✓ Количество неудачных попыток входа: определяет количество неудачных попыток входа, после которых учетная запись будет заблокирована;
- ✓ Длительность блокировки: определяет, на какой период времени учетная запись будет заблокирована после достижения максимального количества неудачных попыток входа;
- ✓ Сброс блокировки: определяет, будет ли блокировка автоматически сброшена после определенного периода времени или требуется вмешательство администратора для разблокировки учетной записи.

Эти параметры могут быть настроены через локальную политику безопасности (Local Security Policy) или через групповые политики (Group Policy) в доменной среде.

Кому может быть разрешен доступ по записи к базе учетных записей пользователей и почему?

Доступ по записи к базе учетных записей пользователей Windows может быть разрешен только администраторам или пользователям, у которых имеется соответствующие привилегии и разрешения. Это предотвращает возможность несанкционированного доступа или изменения учетных записей пользователей системы.

Обычным пользователям и ограниченным учетным записям не разрешается доступ к базе учетных записей пользователей Windows, чтобы обеспечить безопасность и сохранить интегритет учетных записей. Такие пользователи могут иметь права на выполнение только определенных операций, но не могут изменять или управлять учетными записями других пользователей.