МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ   
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САМАРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА»

(САМАРСКИЙ УНИВЕРСИТЕТ)

ИНСТИТУТ ИНФОРМАТИКИ И КИБЕРНЕТИКИ

Кафедра программных систем

Дисциплина

Основы информационной безопасности

# ОТЧЕТ

по лабораторной работе №1

Основные термины, определения и мероприятия по защите пользовательских данных.

Студент: Свистун С.И.

Группа: 6301-020302D

Преподаватель:

доцент Кафедры программных систем Додонов М. В.

Оценка: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Дата: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Самара 2025

**Контрольные вопросы**

1. **Информационная безопасность** — это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации.

**Безопасность данных** —такое состояние хранимых, обрабатываемых и принимаемых данных, при которых невозможно их случайное или преднамеренное получение, изменение или уничтожение.

**Защита данных** — совокупность целенаправленных действий и мероприятий по обеспечению безопасности данных. Таким образом, защита данных есть процесс обеспечения безопасности данных, а безопасность - состояние данных, конечный результат процесса защиты. Защита данных осуществляется с использованием методов (способов) защиты.

1. Методы защиты данных — это способы и приемы обеспечения безопасности, средства защиты — инструменты и технологии, реализующие эти методы, а механизмы защиты — это интеграция средств и методов для выполнения конкретных задач по защите данных.

**Методы** представляют собой теоретическое обоснование того, каким образом осуществляется защита данных. Это общие подходы, концепции и принципы, которые используются для достижения целей безопасности.

**Средства защиты** являются физическими или программными инструментами, воплощающими конкретные методы защиты.

**Механизмы защиты** объединяют ряд средств и методов в единую систему для решения конкретной задачи по обеспечению безопасности.

1. **Основные угрозы безопасности данных** включают:

* Случайные воздействия природной среды (ураган, пожар).
* Целенаправленные воздействия нарушителя (шпионаж, разрушение компонентов информационной системы, использование каналов утечки данных).
* Внутренние возмущающие факторы (отказы аппаратуры, ошибки в ПО, недостаточная подготовка персонала).

1. **Способы несанкционированного доступа к конфиденциальной информации** включают:

* Незаконное подключение (контактное и бесконтактное подключение к линиям связи).
* Высокочастотное навязывание (модуляция высокочастотных колебаний с целью перехвата разговоров).
* Перехват электромагнитных излучений (приём сигналов пассивными устройствами на безопасном расстоянии).

1. **Уязвимые места информационной системы** с точки зрения безопасности данных:

**Технические компоненты информационной системы**:

* Аппаратура (компьютеры, сервера, сетевое оборудование);
* Программное обеспечение (операционные системы, базы данных, прикладные программы);
* Информационно-коммуникационные каналы (телефонные линии, локальная сеть, Интернет).

**Недостатки технической инфраструктуры**:

* Низкий уровень изоляции помещений, позволяющий использовать визуальное наблюдение или прослушивание звуков;
* Прокладка коммуникаций таким образом, что появляется возможность перехвата электромагнитных излучений;
* Недостаточные меры по предотвращению несанкционированного физического доступа к помещениям и устройствам.

**Организационные недостатки**:

* Неправильное распределение ролей и полномочий среди сотрудников;
* Недостаточно строгие правила учета и хранения материальных носителей информации;
* Ослабленная процедура идентификации и аутентификации пользователей.

**Возможность утечек информации через каналы связи**:

* Электронные коммуникации, подверженные перехвату или проникновению (линии связи, электронная почта, Интернет-трафик);
* Телефонные линии и аналоговые каналы, доступные для подслушивания.

**Ненадлежащее хранение и обработка информации**:

* Отсутствие регулярного аудита безопасности данных;
* Хранение конфиденциальных данных на общедоступных серверах или устройствах;
* Обработка секретных данных в помещениях, не обеспеченных необходимой степенью конфиденциальности.

**Использование устаревших или недостаточно защищённых технологий**:

* Применение старых версий программного обеспечения, содержащих известные уязвимости;
* Игнорирование регулярных обновлений антивирусных продуктов и систем безопасности.

**Отсутствие адекватных мер противодействия внешним угрозам**:

* Неадекватная реакция на попытки проникновения извне (DDoS-атаки, фишинг, вирусные атаки);
* Невозможность оперативного реагирования на изменения условий эксплуатации и появления новых типов угроз.

1. **Основные методы защиты данных** включают:
2. **Управление ресурсами системы:** регуляция использования всех ресурсов информационной системы (аппаратура, операционные системы, программы, базы данных и т.д.) в пределах установленных технологических циклов обработки и передачи данных.
3. **Преграждение пути к данным:** физические препятствия, затрудняющие физический доступ нарушителя к защищённым ресурсам и информации.
4. **Маскировка данных:** криптографическое закрытие информации, зашифровка данных для предотвращения несанкционированного доступа.
5. **Регламентация процесса обработки данных:** разработка и реализация комплекса мероприятий, регламентирующих работу информационной системы и снижающих риск несанкционированного доступа путём установления чётких процедур и норм обработки данных.
6. **Побуждение:** создание моральной ответственности работников за соблюдение правил работы с конфиденциальной информацией.
7. **Принуждение:** введение правовых санкций (материальной, административной, уголовной ответственности) за нарушения правил работы с защищёнными данными.
8. **Основные средства защиты данных** включают:

**Формальные средства защиты:**

* Технические средства защиты.
* Программные средства защиты.
* Криптографические средства.
* Программные средства управления защитой.
* Средства поддержания работоспособности системы защиты.

**Неформальные средства защиты:**

* Организационные меры.
* Законодательные меры.
* Морально-этические нормы.

1. Анти-фишинговые фильтры, VPN-клиенты, Антивирусные программы, Брандмауэры (Firewall)
2. **Направления по обеспечению информационной безопасности для конечного пользователя** можно разделить на две основные категории:

**Защита информации от несанкционированного доступа (НСД):**

* Установка надежных паролей и регулярная их смена.
* Ограничение доступа посторонних лиц к устройству.
* Использование двухфакторной аутентификации (2FA).
* Работать исключительно с проверенными сайтами и службами.
* Устанавливать надежные антивирусные программы и регулярно их обновлять.
* Контроль над активностью сетевых соединений и доступом к важным ресурсам.

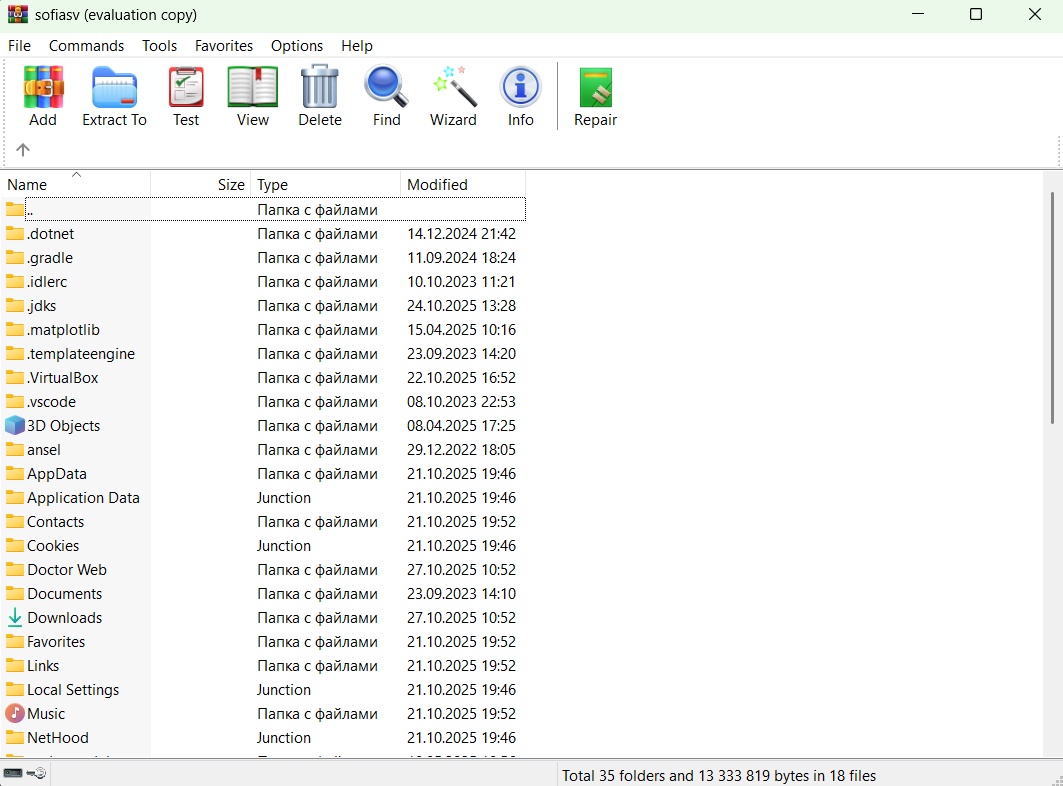
**Защита информации от потерь:**

* Регулярное резервное копирование данных на внешние носители (флешки, жесткие диски, облако).
* Организация автоматизированного резервного копирования ночью или в моменты минимальной нагрузки.
* Предупреждение случайного удаления данных через корзину или аналогичные механизмы.
* Поддержание резервных копий на постоянной основе.
* Защита от компьютерного вируса и прочих вредоносных программ.
* Минимизация риска сбоев техники благодаря обслуживанию и тестированию аппаратуры.

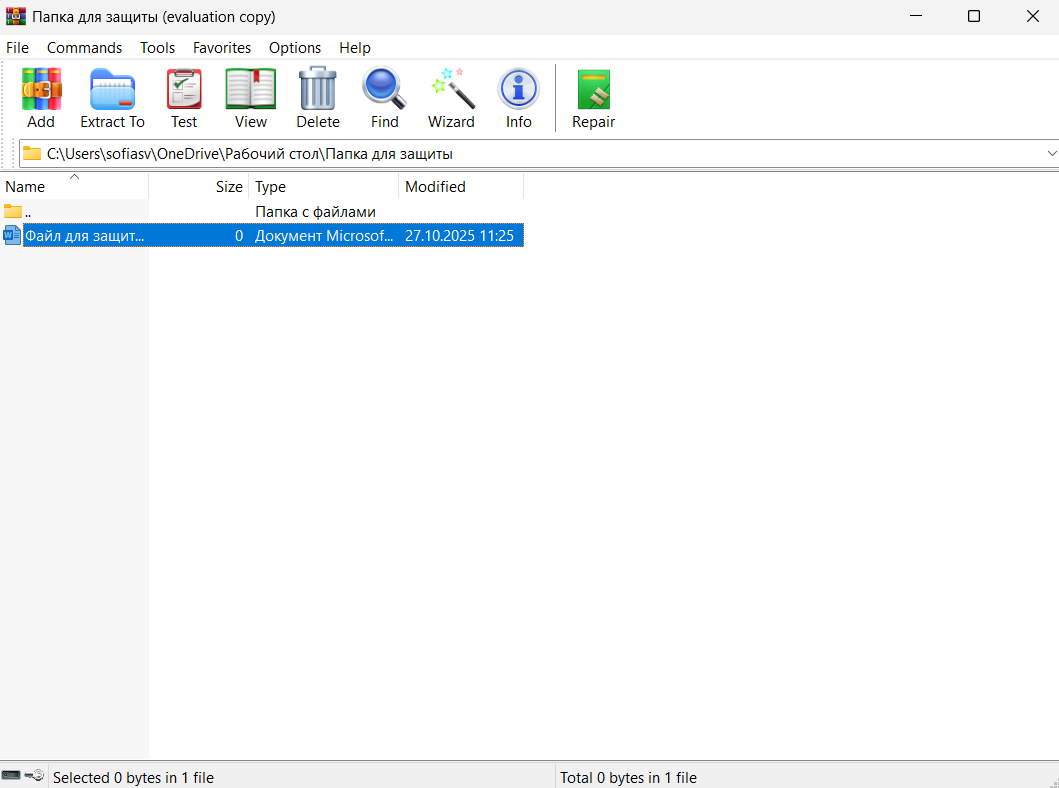
1. **Основные мероприятия по защите от компьютерных вирусов** включают:
2. **Предотвращение доступа посторонних лиц к компьютеру.** Пользователь должен ограничить доступ посторонних к своему компьютеру, поскольку чужой носитель (диски, USB-флешки) может содержать инфицированные файлы.
3. **Использование лицензированного программного обеспечения.** Следует избегать установки пиратского или неизвестного программного обеспечения, особенно игр, так как именно через них вирусы распространяются чаще всего.
4. **Мониторинг изменений в работе компьютера.** Необходимо следить за любыми изменениями в поведении компьютера: замедленной работой программ, появлением необычных сообщений или символов, зависаниями и ошибками. Раннее выявление симптомов позволит избежать значительных последствий.
5. **Хранение важной информации на защищенных носителях.** Рекомендуется размещать важные данные на съемных носителях, защищенных от записи, что предотвращает распространение вирусов даже при заражении основного жесткого диска.
6. **Постоянное использование антивирусных программ.** Компьютер необходимо периодически проверять специализированными антивирусными пакетами. Однако важно помнить, что антивирусные программы устаревают быстро, поэтому их необходимо постоянно обновлять.
7. **Основные мероприятия по защите информации от случайного удаления** включают:
8. Аккуратность и внимательность при работе с компьютером.
9. Размещение важной информации на защищённых от записи дисках.
10. Рациональное размещение файлов и систематическое удаление ненужных данных.
11. Быстрое восстановление случайно удалённой информации.
12. **Основные мероприятия по защите информации от сбоев в работе устройств** включают:
13. Периодическая проверка исправности оборудования.
14. Периодическая оптимизация (дефрагментация) диска для рационального размещения файлов на нем, ускорения работы и уменьшения его износа.
15. Наличие загрузочных (системных) дискет, с которых можно запустить компьютер (т.е. загрузить операционную систему) в случае сбоев с основным системным диском.

**Ход выполнения работы**

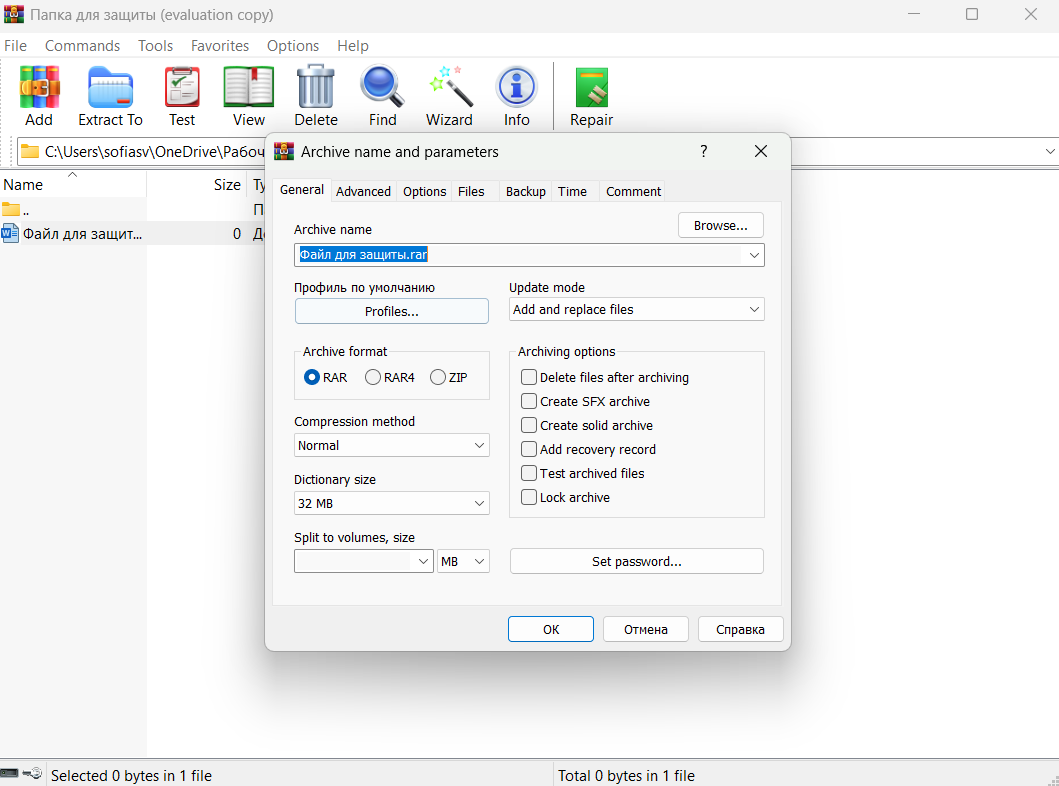
1. Запустите программу резервного копирования, например, «Архивация данных», WinRar, Хранитель V и т.п.



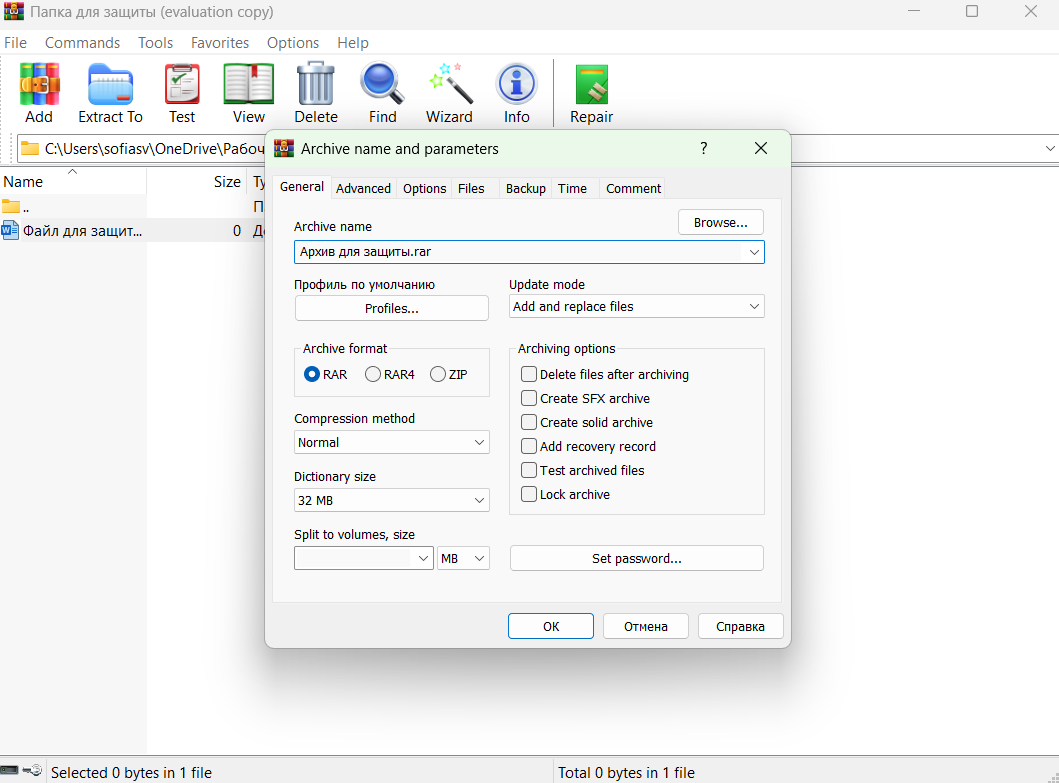
1. Выберите необходимые документы для резервного копирования



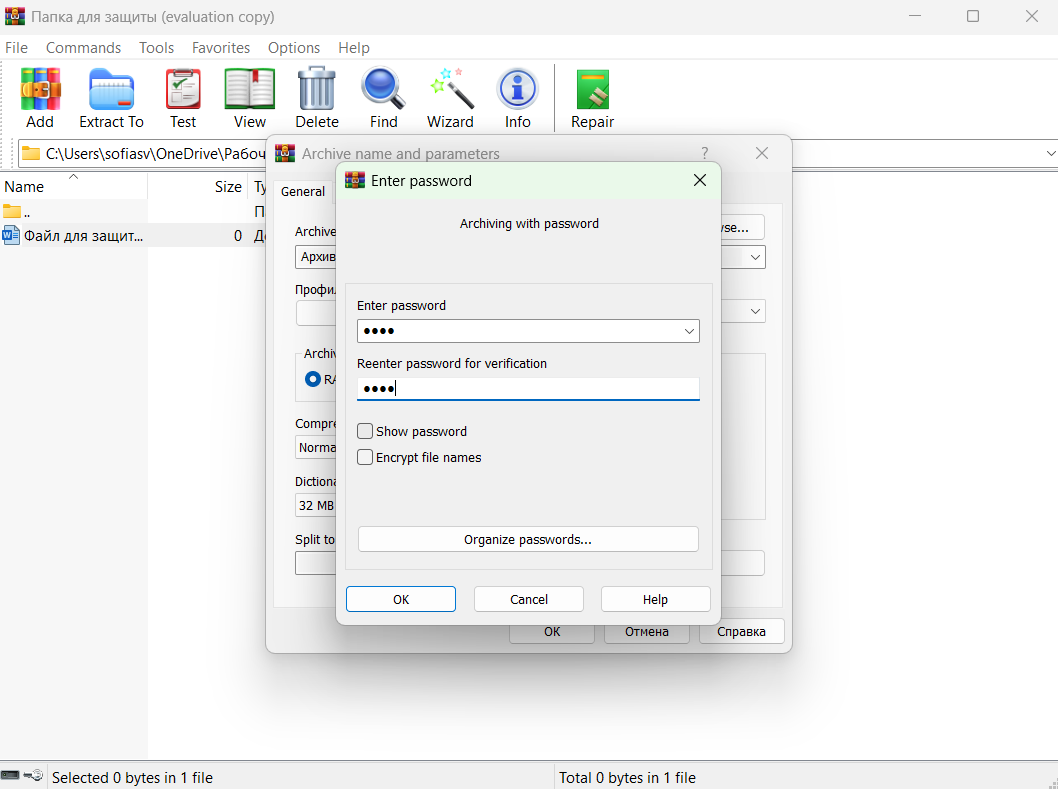
1. Нажмите кнопку «Добавить»



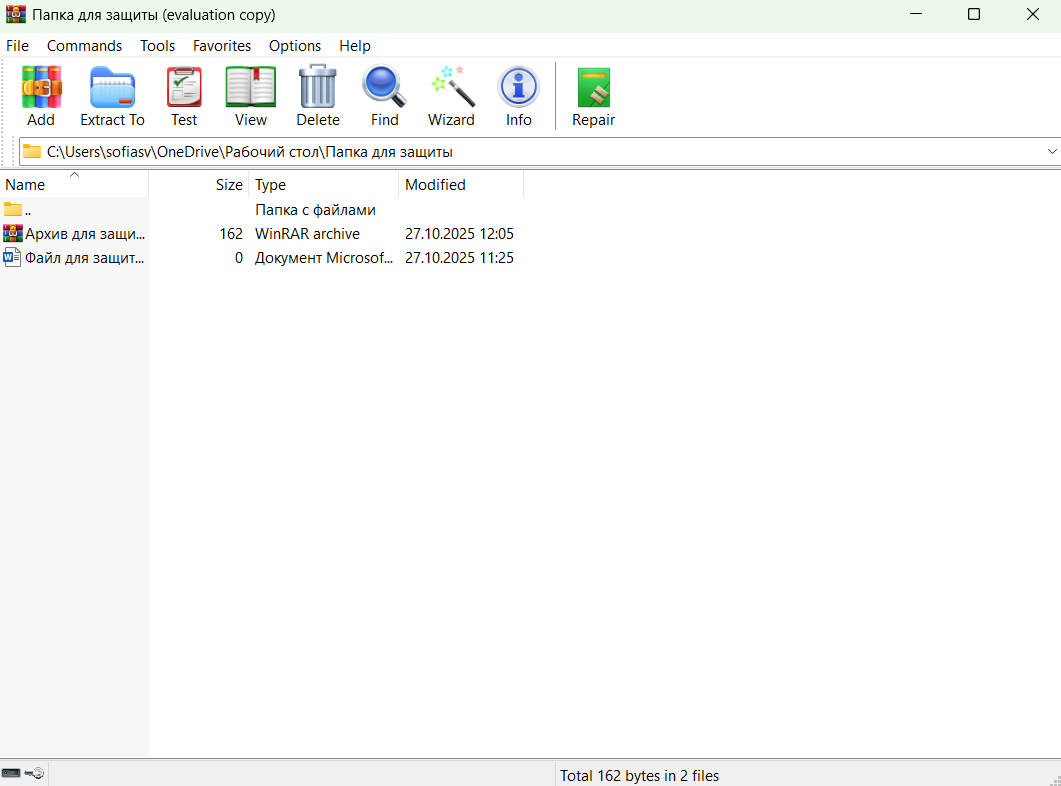
1. На вкладке «Общие» укажите имя архивного файла
2. Выберите необходимый метод сжатия



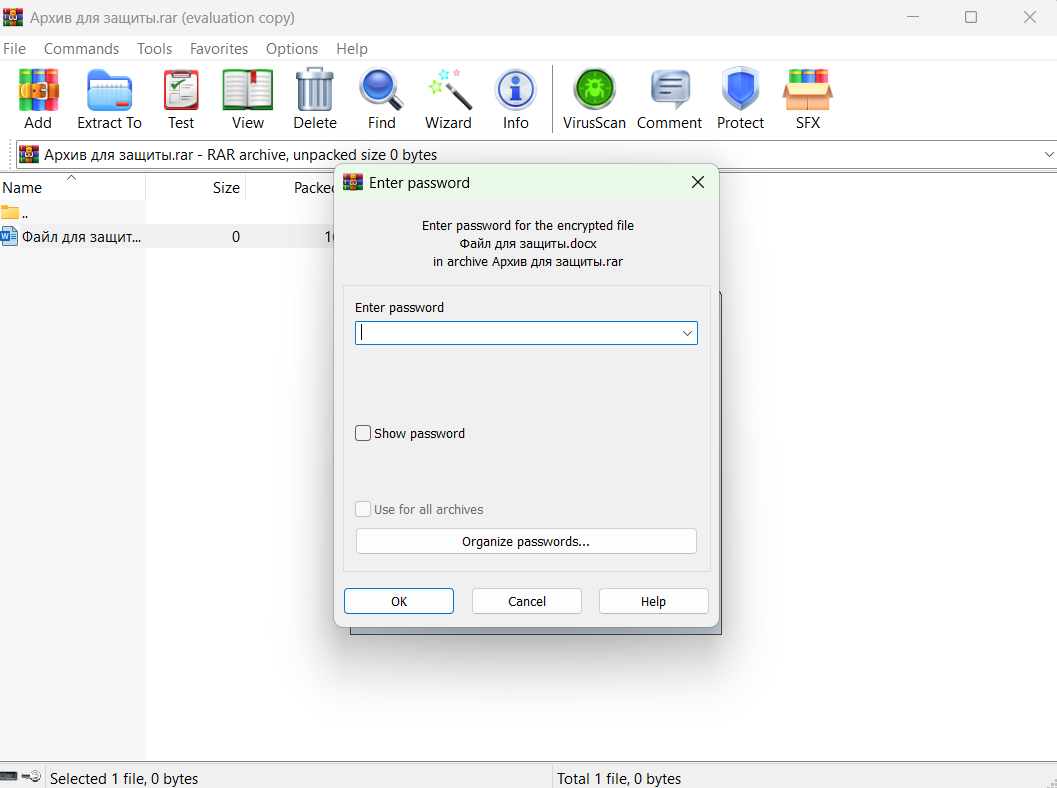
1. На вкладке «Дополнительно» нажмите кнопку «Установить пароль» и в открывшемся окне укажите пароль для выбранных файлов, добавляемых в указанный архив



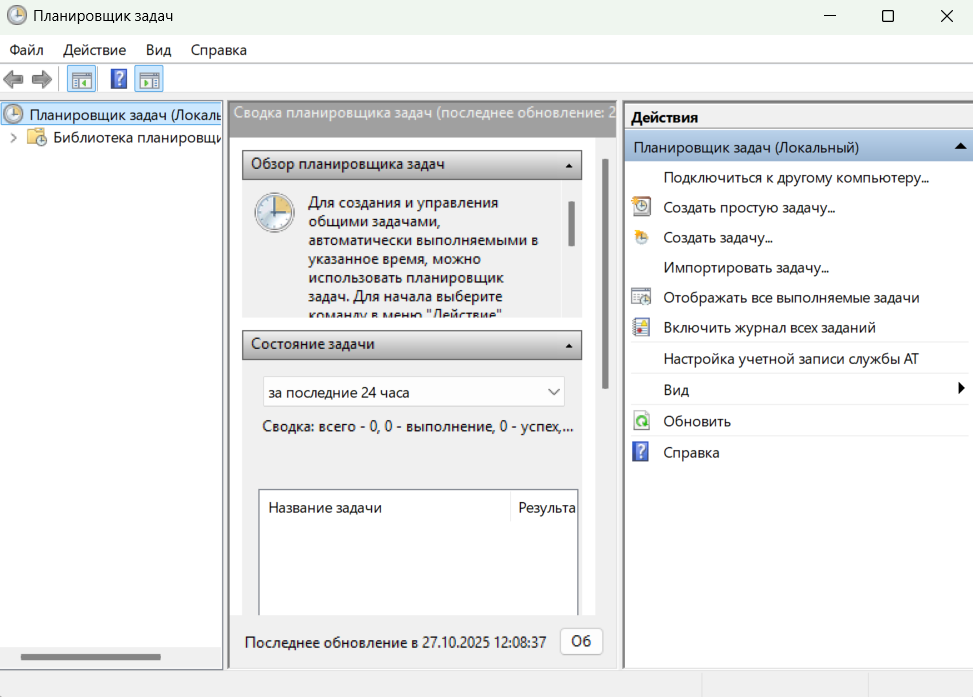
1. Ознакомьтесь с остальными параметрами, расположенными на вкладках «Общие», «Дополнительно», «Резервные копии», «Комментарии» окна «Имя и параметры архива» программы WinRar. Задайте необходимые параметры.
2. Нажмите кнопку «OK», после чего в заданный архив будут добавлены выбранные файлы



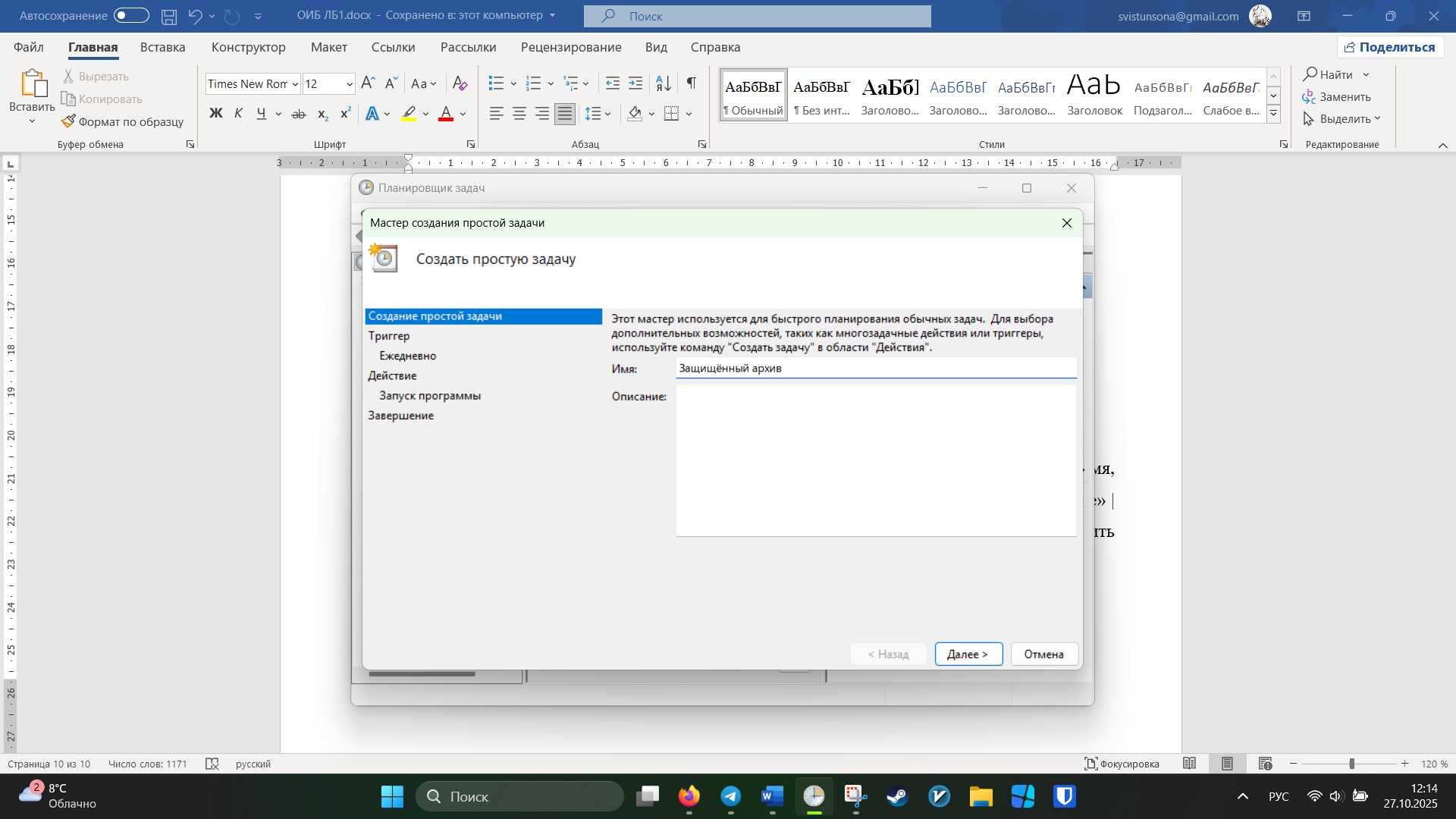
1. Убедитесь, что для просмотра содержимого добавленных файлов архива, необходимо ввести пароль

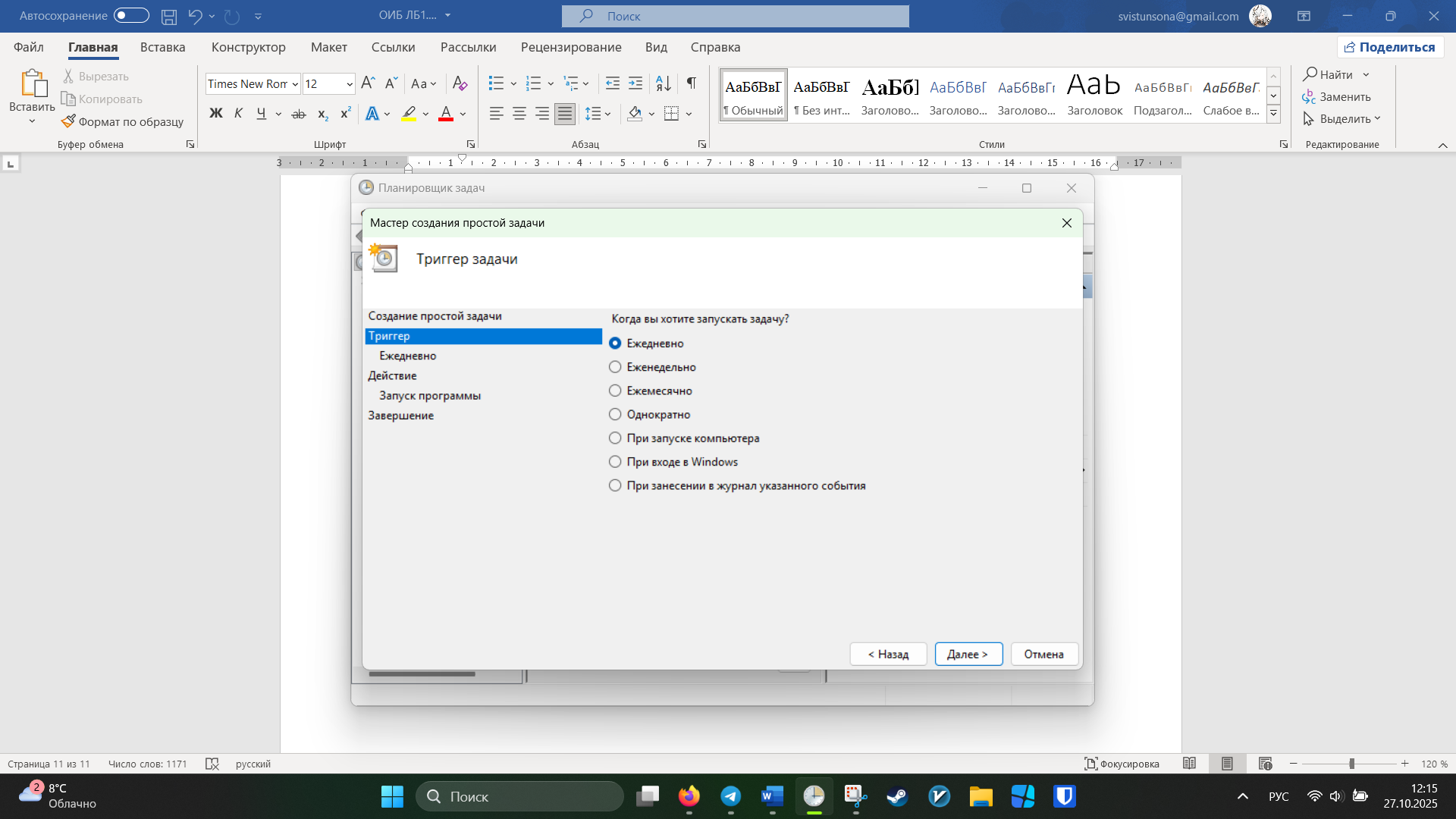


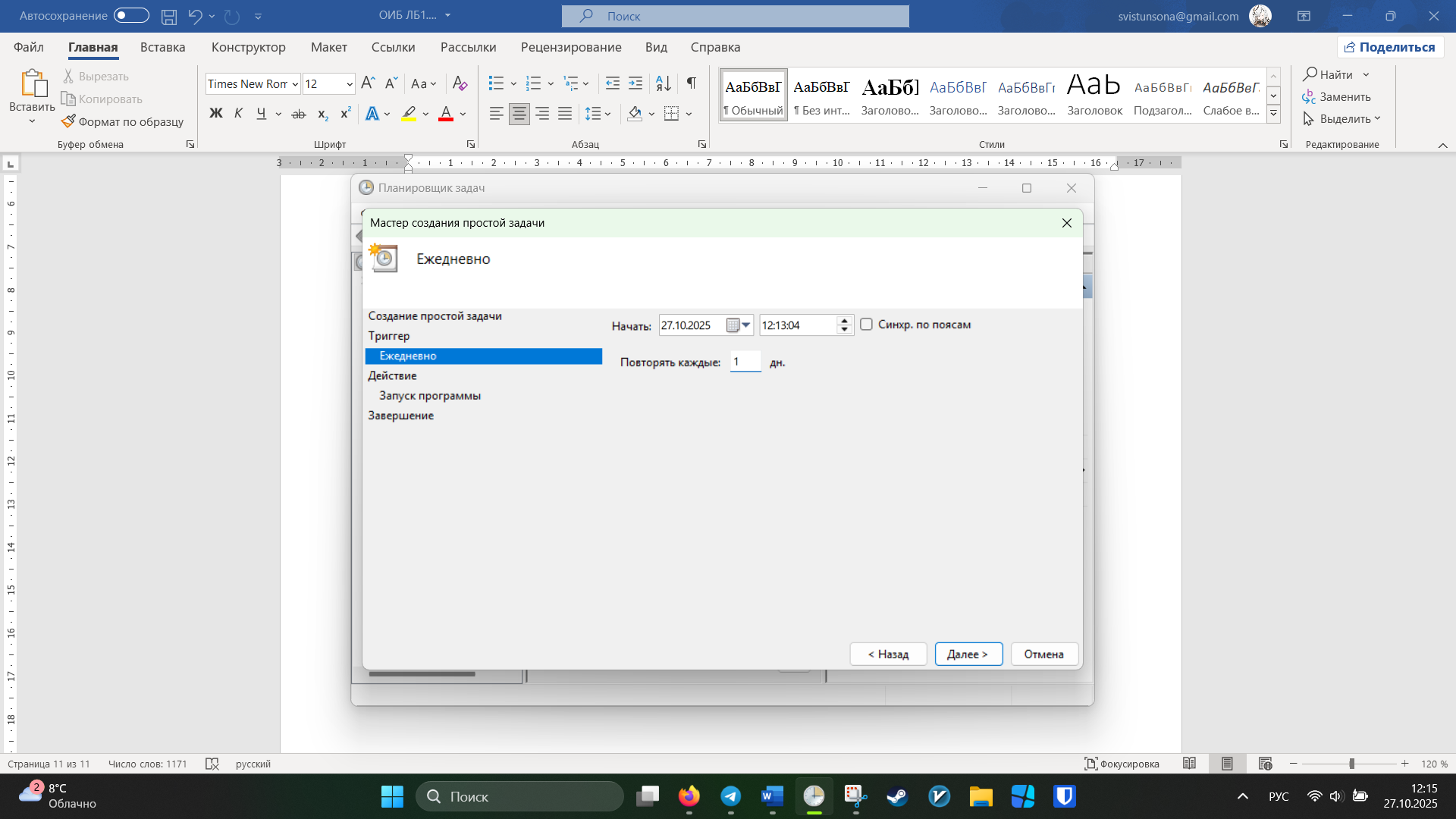
1. Запустите программу «Мастер планирования заданий»



1. Выберите программу «WinRar»
2. Укажите имя создаваемого задания и периодичность его выполнения
3. Укажите имя пользователя (от имени которого будет выполняться задание) и его пароль
4. Установите галочку задания дополнительных параметров и нажмите кнопку «Готово»





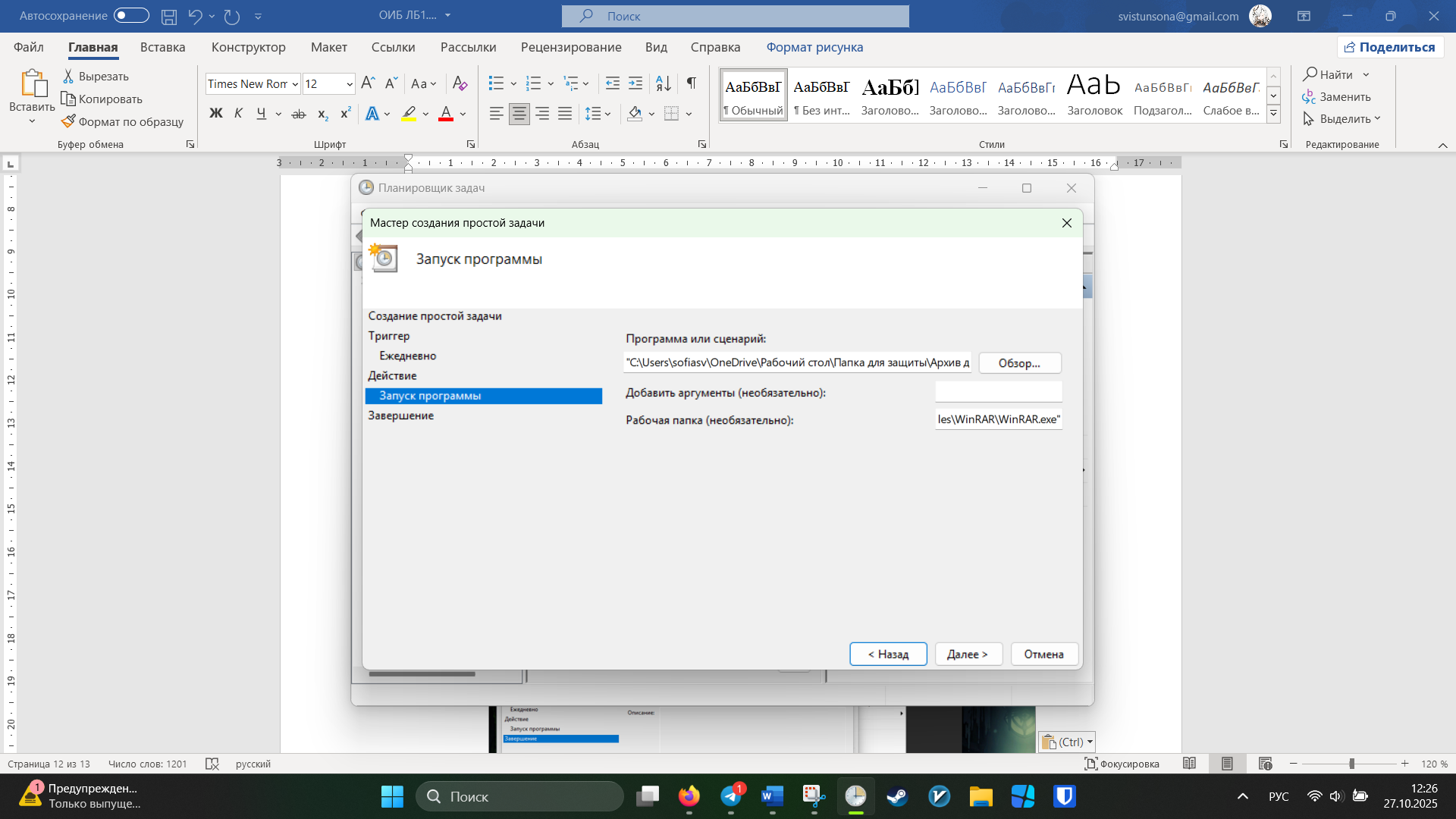


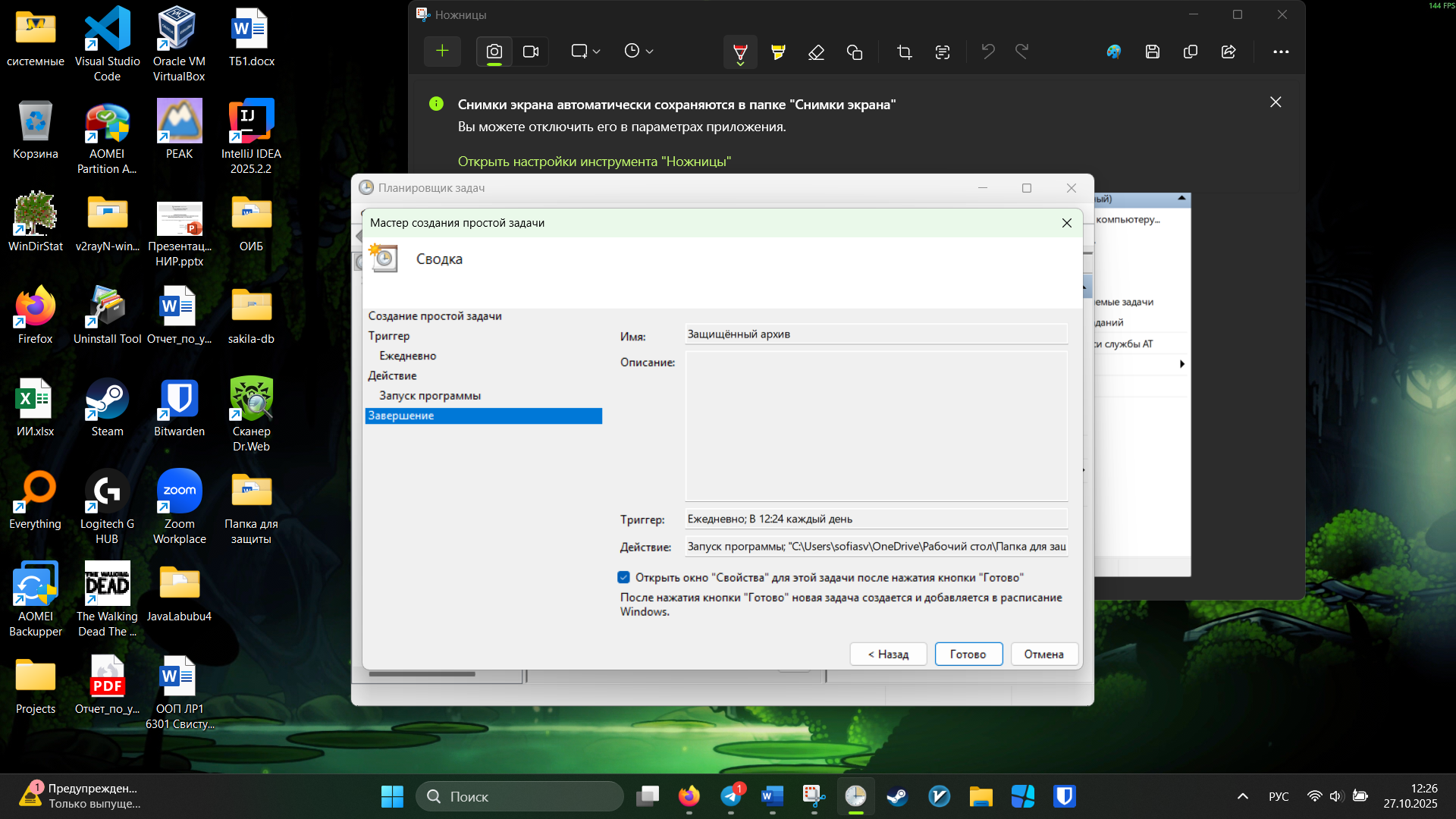


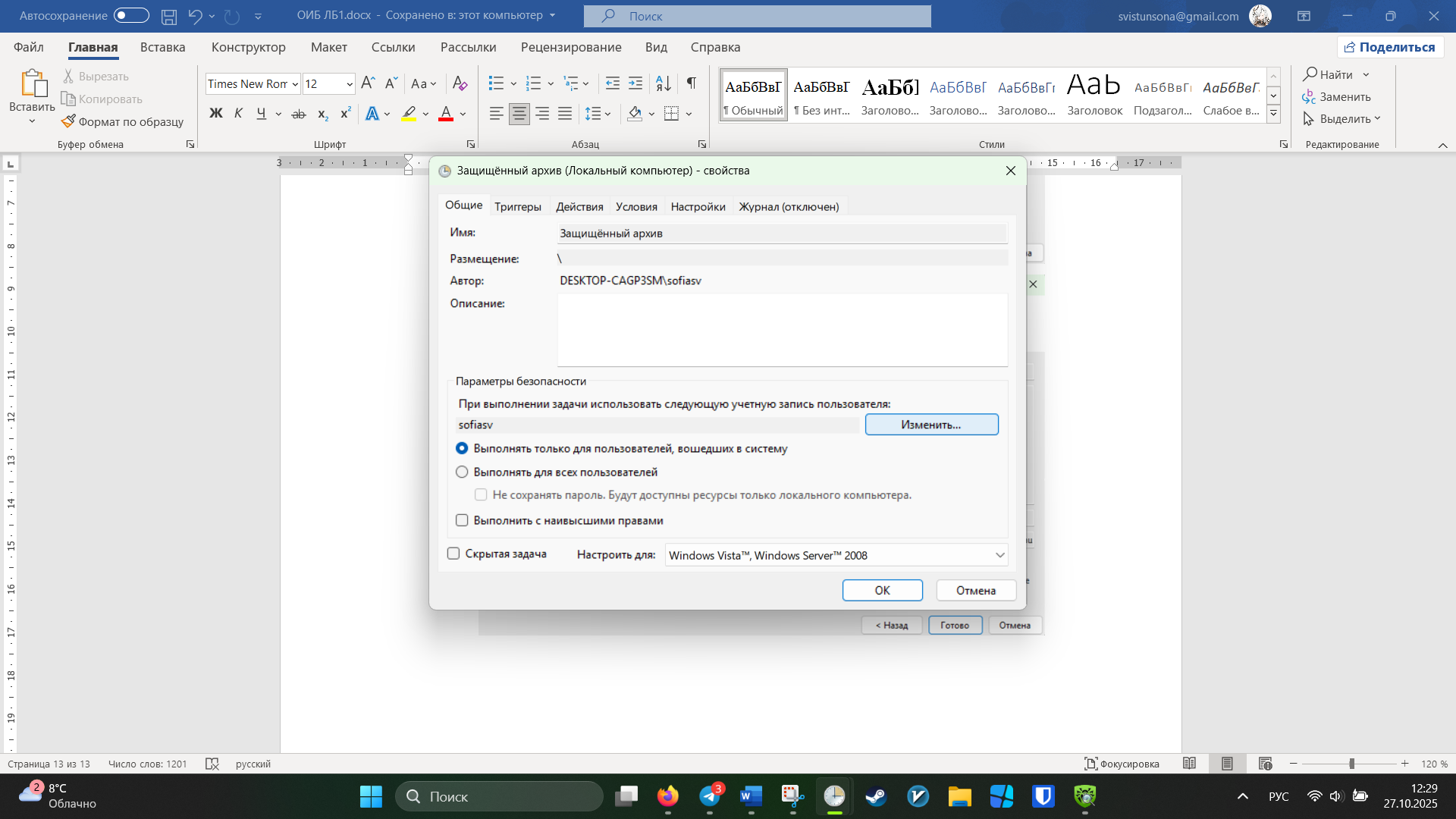
1. В дополнительных параметрах на вкладке «Задания» в поле «Выполнить» укажите

параметры запуска программы WinRar: полное имя программы, команда добавления в

архив, полное имя архива и шаблон архивируемых файлов



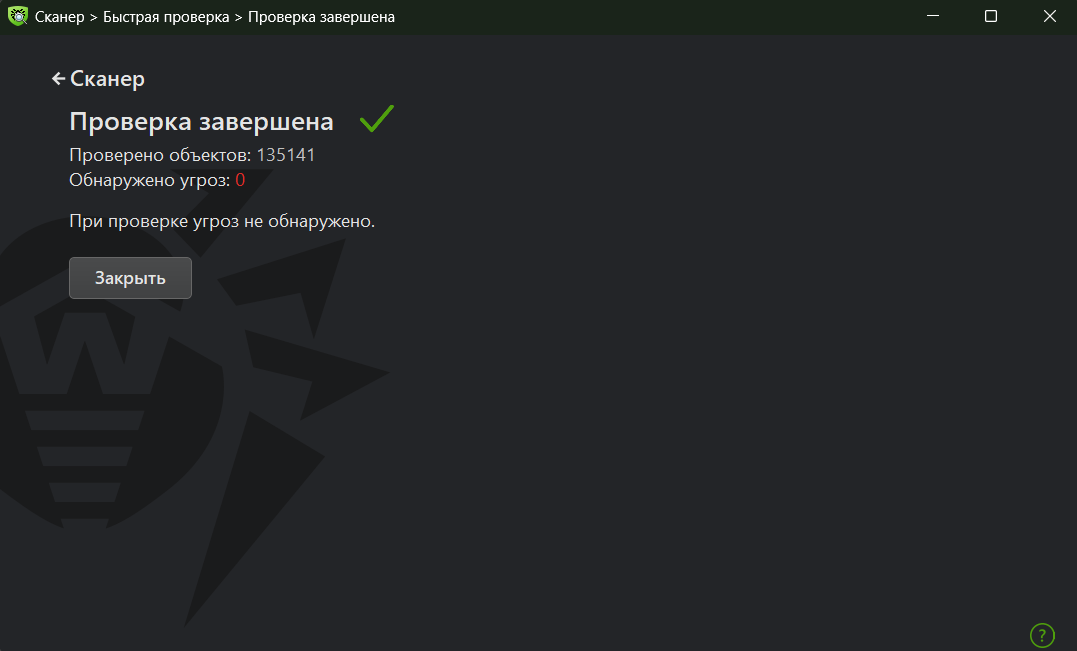




1. Ознакомьтесь с дополнительными параметрами на вкладках «Расписание» и «Параметры» и нажмете кнопку «OK»
2. Перезагрузите компьютер и проверьте наличие созданного архива.



1. Измените дополнительные параметры запуска программы WinRar так, чтобы при по-вторном добавлении файлов в архив старые файлы удалялись
2. Запустите программу антивирус, например Kaspersky AntiVirus, и проверьте компьютер на наличие вирусов. Если в процессе работы программы были обнаружены вирусы, то необходимо «вылечить» или удалить зараженные файлы.



1. Запустите программу «Проверка диска» (кнопка «Пуск» | «Программы» | «Стандартные» | «Служебные» | «Проверка диска») и проверьте жесткие диски компьютера на наличие ошибок.



1. Запустите программу «Дефрагментация диска» (кнопка «Пуск» | «Программы» | «Стандартные» | «Служебные» | «Дефрагментация диска») и оптимизируйте жесткие диски компьютера.

