МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Колледж программирования и кибербезопасности

Отчет о выполнении практического задания

по дисциплине «МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении»

Практическое задание № 7

Специальность – 10.05.02 Информационная безопасность телекоммуникационных систем

Выполнил студент:

_____ Маркаров М. О.

Группа: ИБ-32

Руководитель:

_____ Герасин В. Ю.

Работа защищена с оценкой _____

Дата защиты _____

Москва

2024

Практическая работа № 7

Тема: Антивирусная защита.

Цель: получить навыки работы с паролями в различных программах изучить операции антивирусной защиты информации.

Ход работы:

Задание №1 Создать документ Microsoft Word и сохранить определения пароля и парольной системы. Выполнить установку парольной защиты на электронные документы.

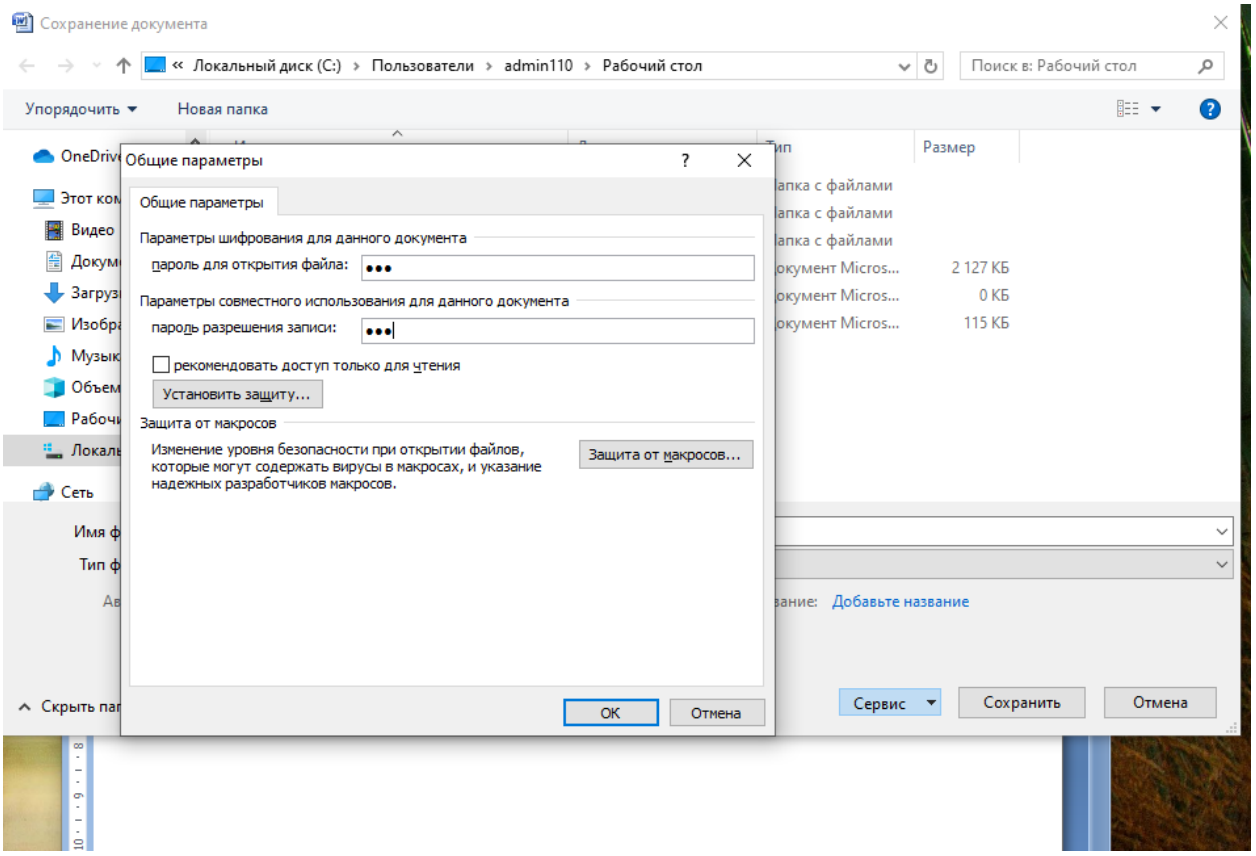

Рис. 1 Добавление пароля на офисный документ MS Word

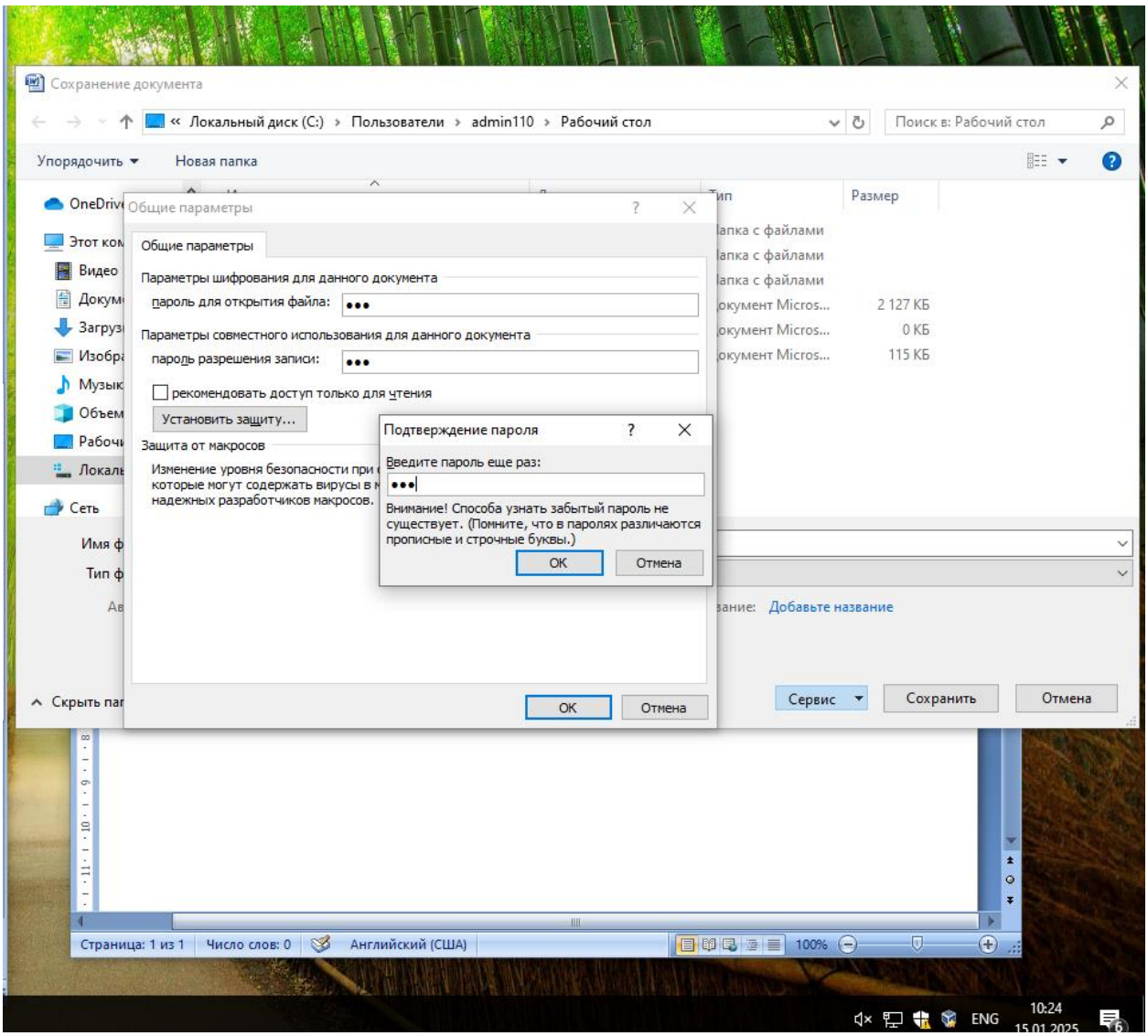

Рис. 2 Процесс ввода пароля который был ведён в прошлый разы

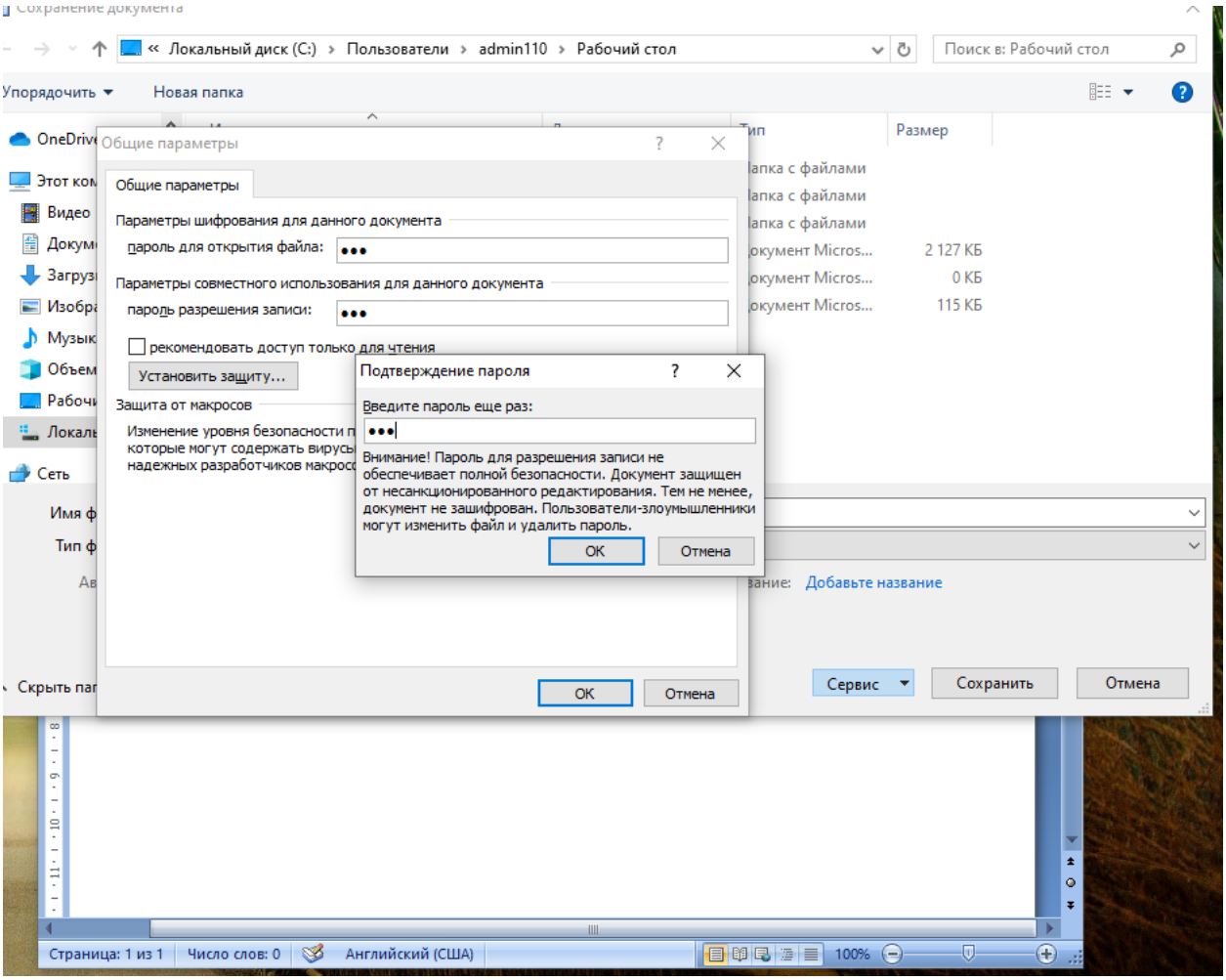

Рис. 3 Процесс ввода пароля (заключительный этап)

Задание №2 Создайте папку «Группа_ФИО». Для резервного копирования данных архивируйте файлы в папке с названием «Группа_ФИО» архиватором RAR с паролем 123.

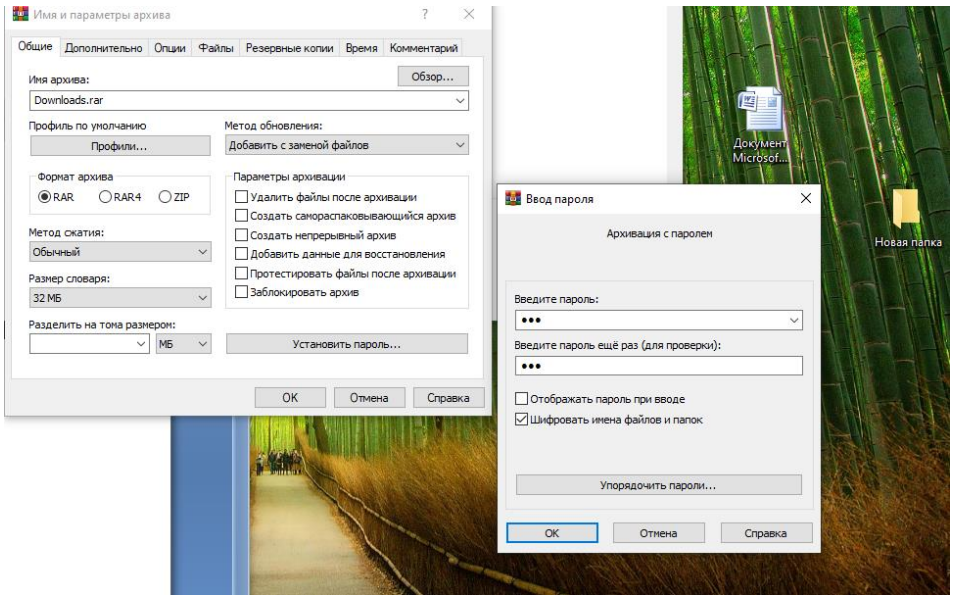

Рис. 4 Создание архива который будет разархивировать после ввода пароля 123

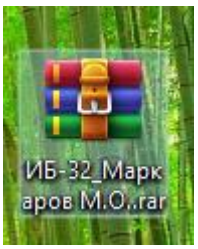

Рис. 5 Результат после ввода пароля (изменено название архива на ИБ-32_Маркаров М.О..rar)

Задание №3 Изучение антивирусной программы и сканирование папок на наличие вирусов.

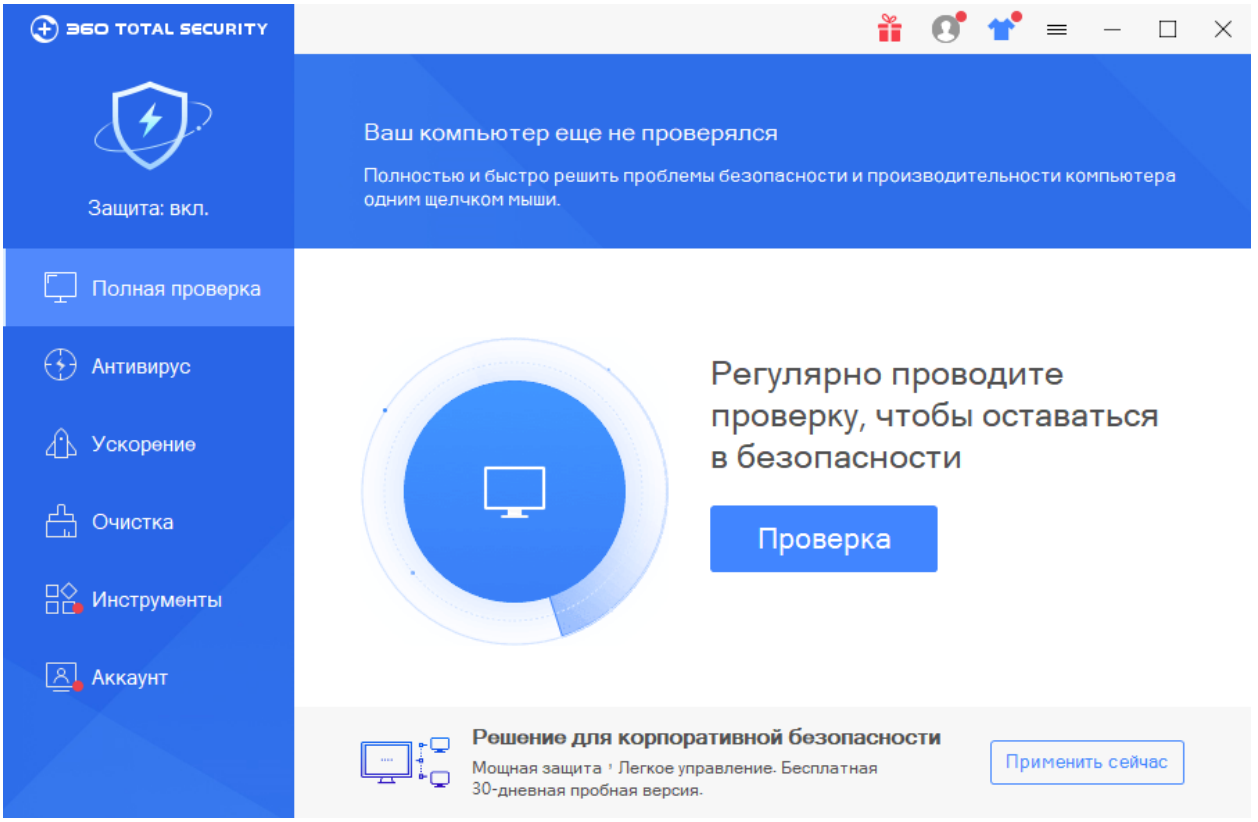

Рис. 6 Интерфейс антивирусного ПО 360 Total Security

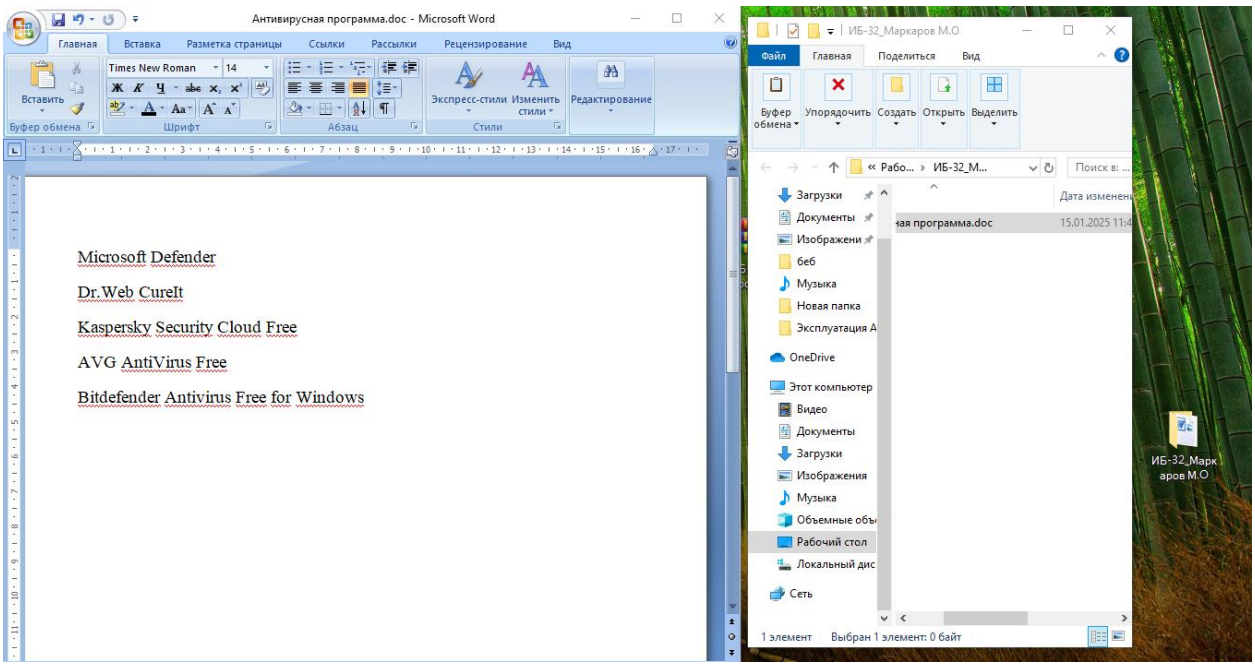

Рис. 7 Пишем в папке документе в формате doc не менее пяти антивирусных программ

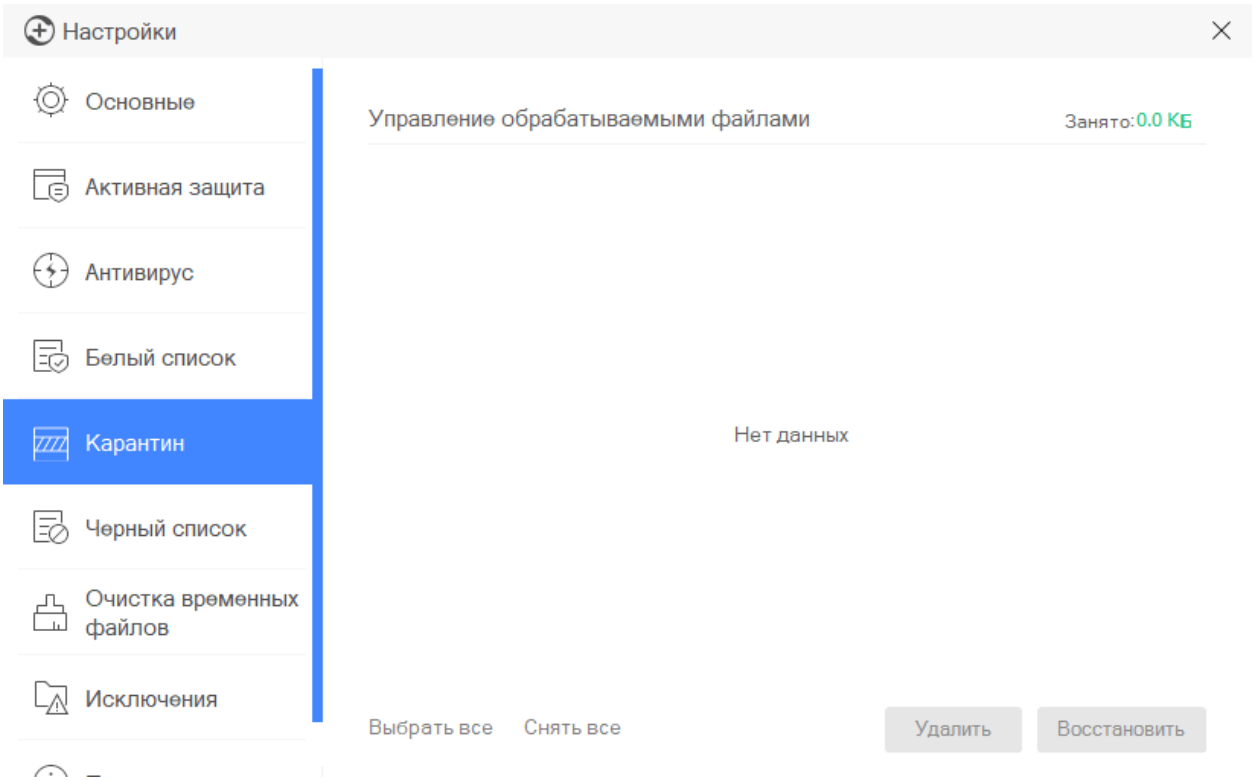

Рис. 8 Карантин пуст

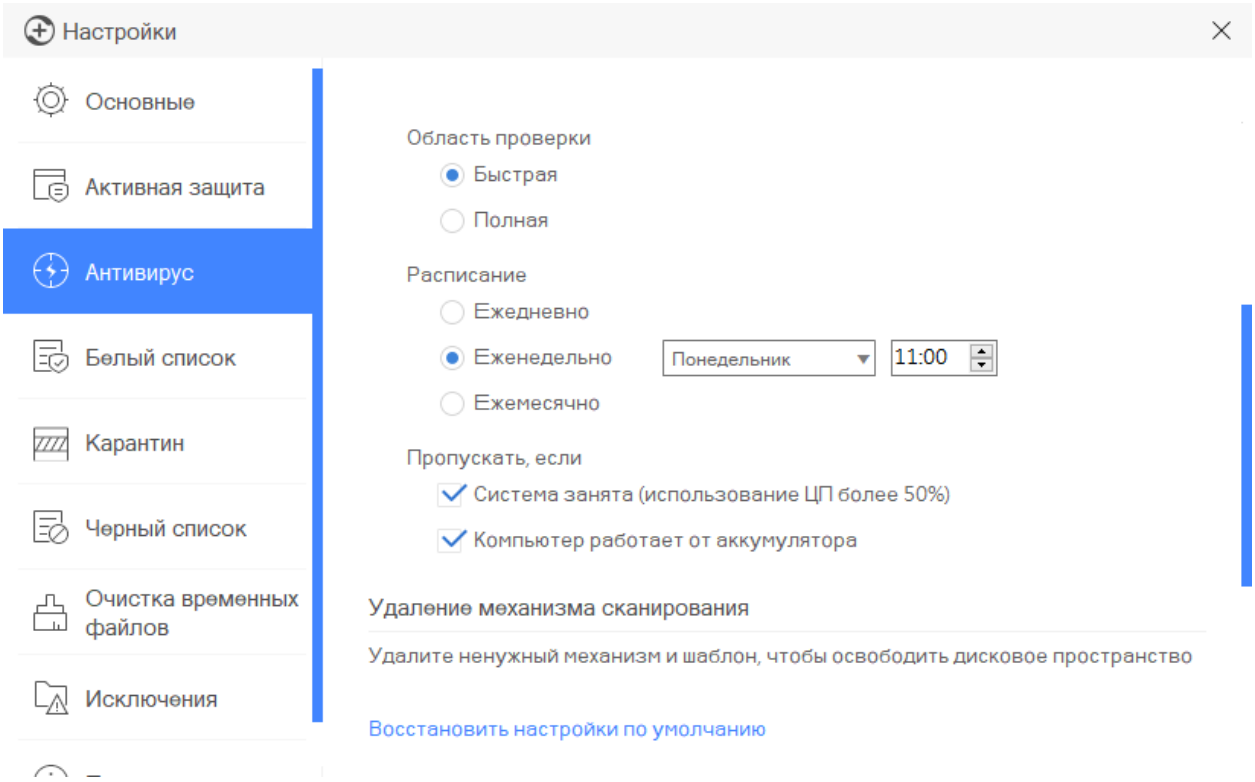

Рис. 9 Во вкладке параметры мы поставили запланированную проверку котора раз в неделю в 11:00 будет сканировать систему

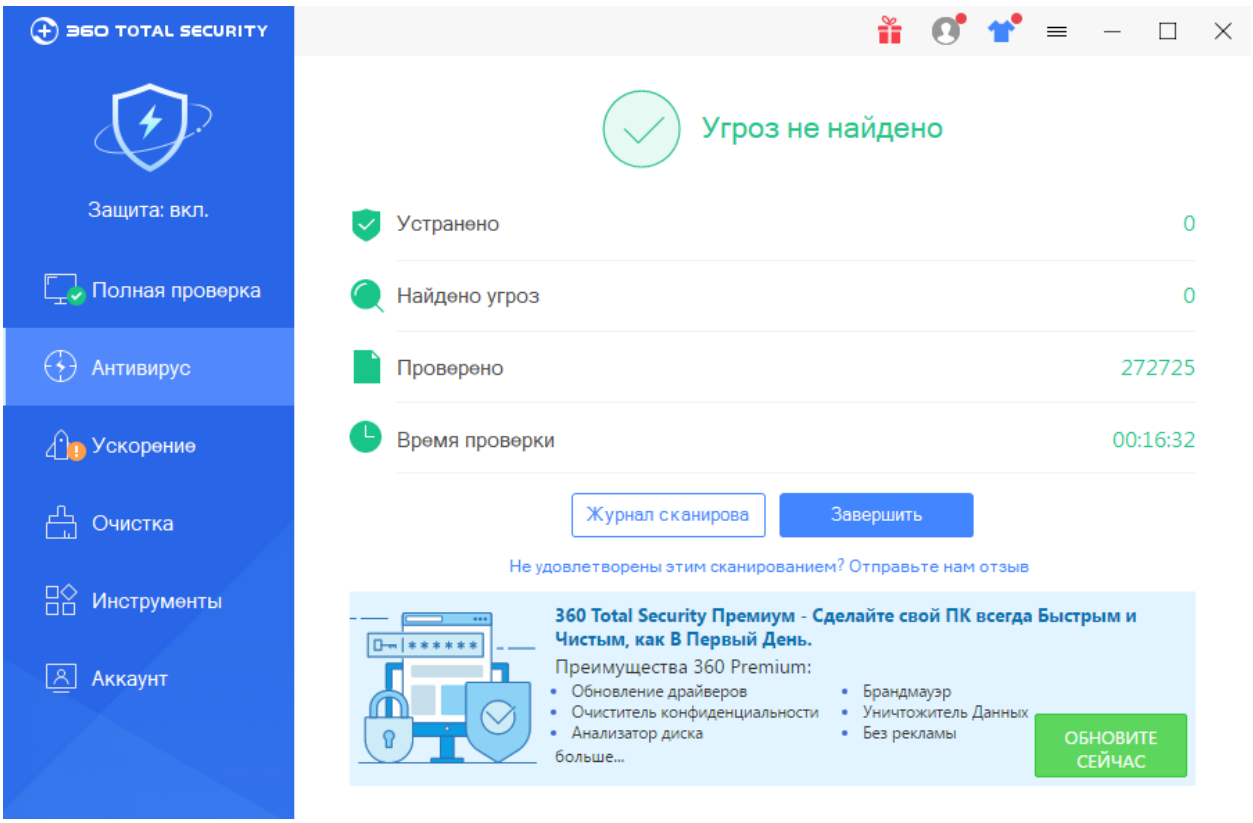

Рис. 10 Полная проверка с включённым носителем.

На (рис. 10) демонстрируется полная проверка с обновлением антивирусных баз.

Контрольные вопросы.

1. Что такое пароль?

Пароль комбинация символов букв, цифр, специальных знаков, используемая для предоставления доступа к защищенным данным, системам или устройствам.

2. Что такое парольная система?

Парольная система механизм аутентификации, который использует пароли для проверки подлинности пользователя и предоставления доступа к ресурсам.

3. Какие бывают пароли?

Простыми (например, "123456") или сложными (например, "P@ssw0rd!2023"), одноразовыми (OTP — одноразовые пароли), графическими (используются изображения или узоры), биометрическими (используют отпечатки пальцев, распознавание лица и т.д.).

4. Что нужно делать для резервного копирования данных?

1) Выбрать данные для копирования.

2) Определить место хранения резервной копии

3) Использовать специализированные программы или встроенные инструменты операционной системы.

4) Регулярно обновлять резервные копии.

5. Что называется компьютерным вирусом?

Компьютерный вирус вредоносная программа, способная к самовоспроизведению и распространению, которая может повреждать данные, нарушать работу системы или красть информацию.

6. По каким признакам классифицируются компьютерные вирусы?

1) Среде обитания (файловые, загрузочные, макровирусы и т.д.).

2) Способу воздействия (безвредные, опасные, очень опасные).

3) Алгоритму работы (резидентные, нерезидентные, полиморфные и т.д.).

7. Как классифицируются вирусы по среде обитания?

1) Файловые (заражают исполняемые файлы).

2)Загрузочные (заражают загрузочные секторы дисков).

3) Макровирусы (заражают документы с макросами, например, Word или Excel).

4) Сетевые (распространяются через сеть).

8. Какие типы компьютерных вирусов выделяются по способу воздействия?

По способу воздействия вирусы делятся на:

1) Безвредные (не наносят вреда, но могут занимать ресурсы).

2) Опасные (вызывают сбои в работе системы).

3) Очень опасные (уничтожают данные или нарушают работу системы).

9. Какие методы защиты от компьютерных вирусов можно использовать?

Методы защиты включают установку антивирусного ПО, регулярное обновление программного обеспечения, осторожность при открытии вложений в электронной почте, использование брандмауэров, резервное копирование данных.

10. На какие виды можно подразделить программы защиты от компьютерных вирусов?

Программы защиты делятся на антивирусы обнаруживают и удаляют вирусы, файерволы контролируют сетевой трафик, антишпионские программы борются с программами-шпионами, программы для резервного копирования защищают данные от потери, сканеры уязвимостей проверяют систему на наличие уязвимостей.

Вывод в результате проделанной работы мы ознакомились с работой антивирусного ПО а также научились пользоваться системными файлами и архивами.