

Молдавский Государственный Университет Молдовы  
Факультет Математики и Информатики  
Департамент Информатики

Лабораторная работа №4  
по предмету “Безопасность Информационных Систем”  
тема: “Резервное копирование и восстановление”

Преподаватель: Dr Conf. Unif. Новак Л.  
Выполнила: Павлышина Александра I2302

Кишинев, 2024

## Цель работы

Цель данной лабораторной работы заключается в том, чтобы узнать принципы работы резервного копирования и восстановления.

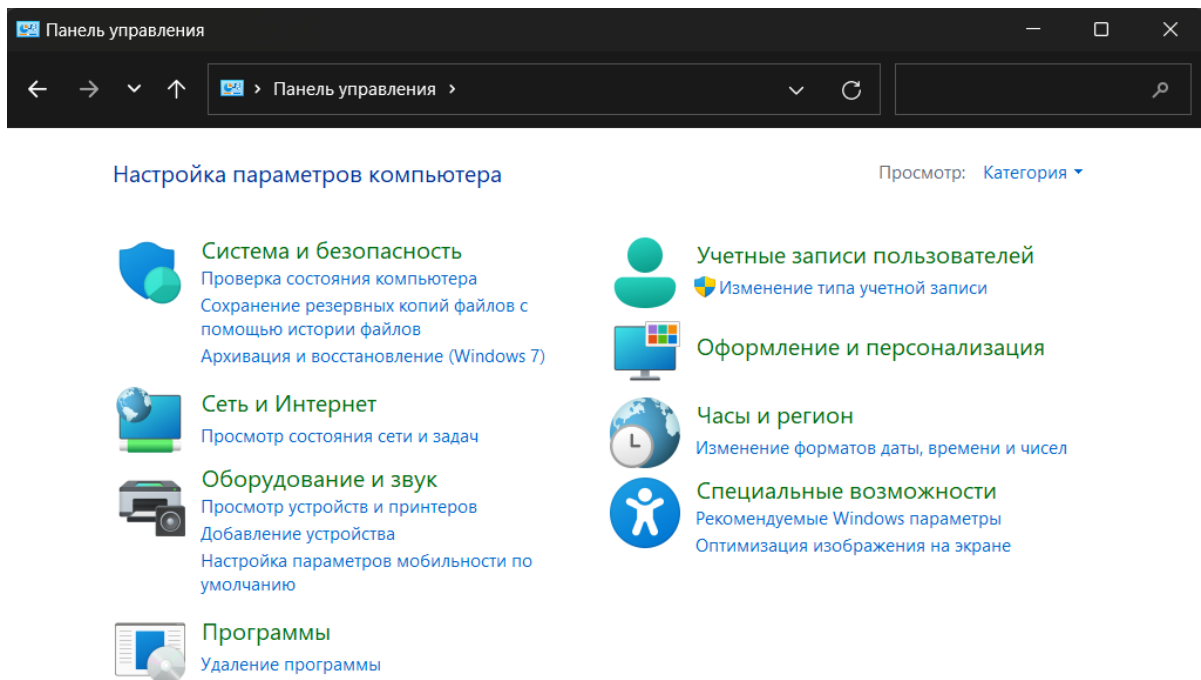
## Ход работы

Резервное копирование — процесс создания копий данных для их защиты от потерь, повреждений или случайного удаления. Восстановление — процесс восстановления данных из резервных копий.

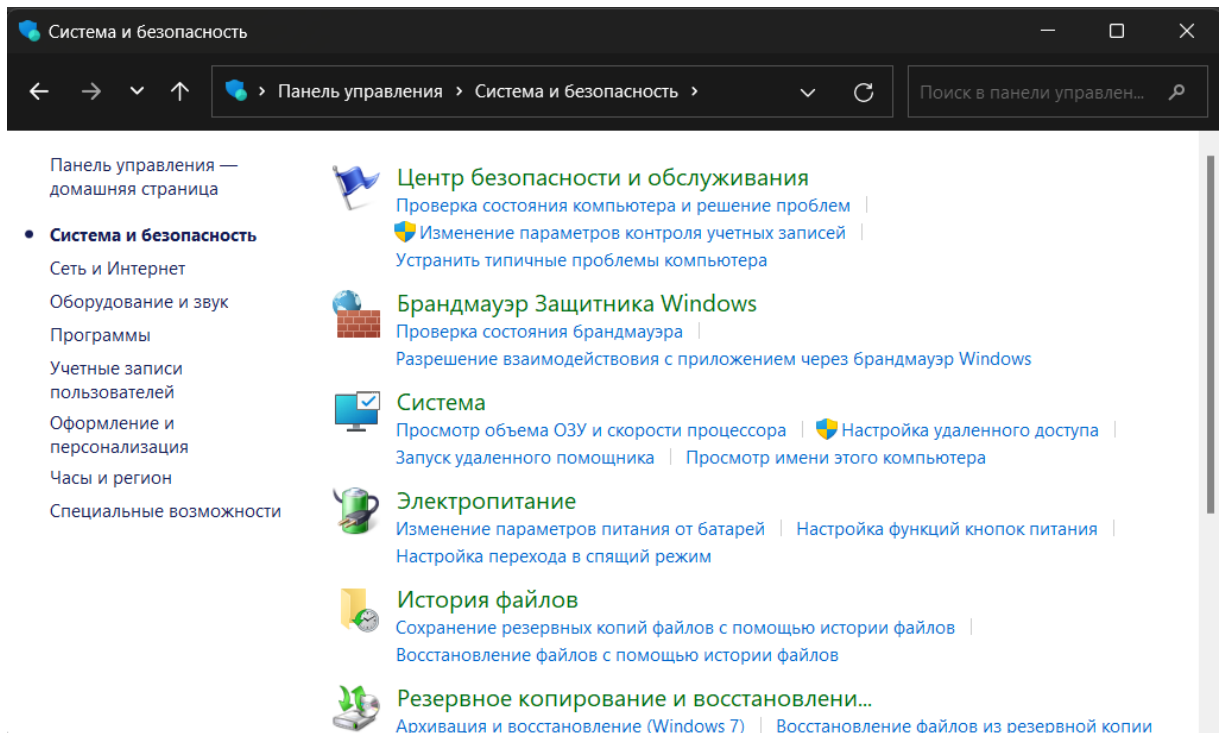
## Windows

Для создания резервной копии нужно выполнить следующие шаги:

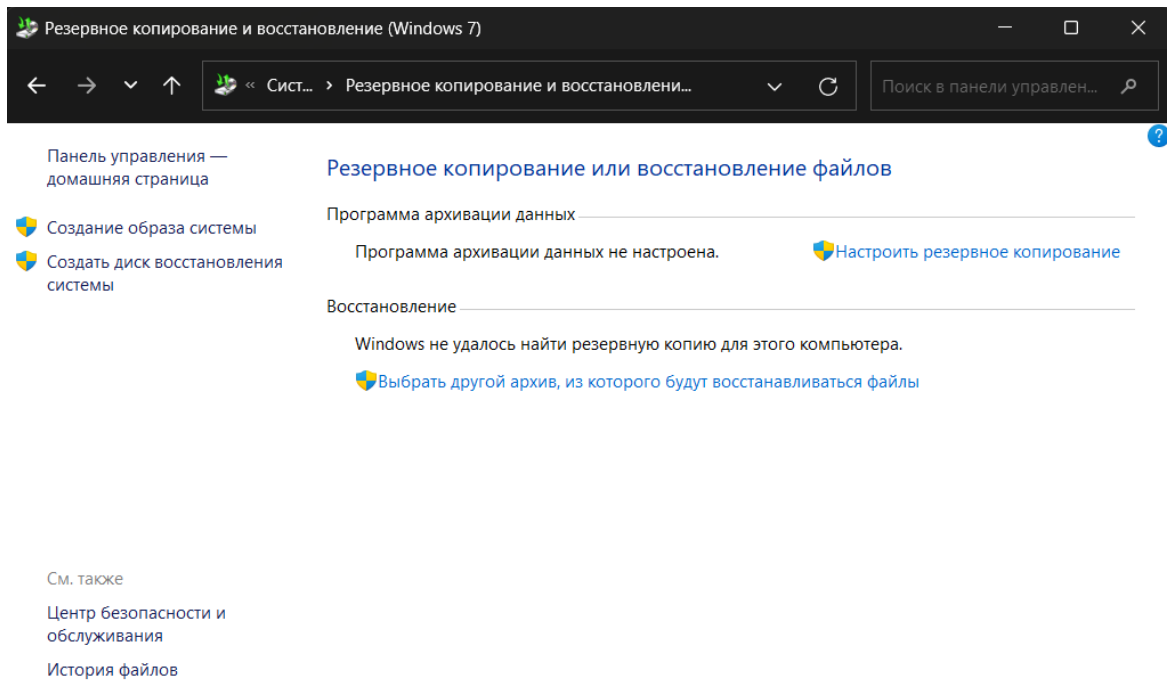
1. Перейти в панель управления



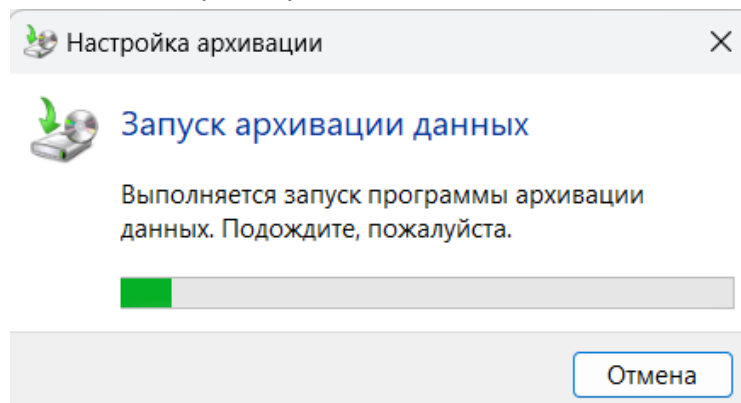
## 2. Далее во вкладку “Система и безопасность”




## 3. В соответствующем разделе “Резервное копирование и восстановление” выбрать “Настроить резервное копирование”



4. Далее ждем запуск архивации данных и выбираем тот диск, которому требуется выполнить резервное копирование, нам предоставится выбор вручную выбрать, что мы конкретно хотим заархивировать или позволить Windows самому решать.




←  Настройка архивации

✕

Выберите, где вы хотите хранить создаваемые архивы

Мы рекомендуем хранить резервную копию на внешнем жестком диске.

Сохранять архив:

Место назначения архивации	Свободно	Полный р...
 SKLAD (D:)	339,40 ГБ	398,81 ГБ

Обновить

Сохранить в сети...

Далее

Отмена

## Что вы хотите архивировать?

☒ Предоставить выбор Windows (рекомендуется)

Windows выполнит архивацию файлов, сохраненных в библиотеках, на рабочем столе и в стандартных папках Windows. Также Windows создаст образ системы, который можно использовать для восстановления компьютера в случае неполадок. Эти объекты будут регулярно архивироваться по расписанию.

☐ Предоставить мне выбор



Вы можете выбрать библиотеки и папки, а также указать, следует ли включать в резервную копию образ системы. Выбранные элементы будут регулярно архивироваться по расписанию.

5. В конечном итоге настраиваем расписание и подтверждаем настройки.


## Проверьте еще раз параметры архивации

Расположение архива: SKLAD (D:)

Сводка архивации:

Элементы	Включены в резервную ко...
 Все пользователи	Папки Windows по умолча...
 Образ системы	Включено

Расписание: Кажд. воскресенье в 19:00 [Изменить расписание](#)

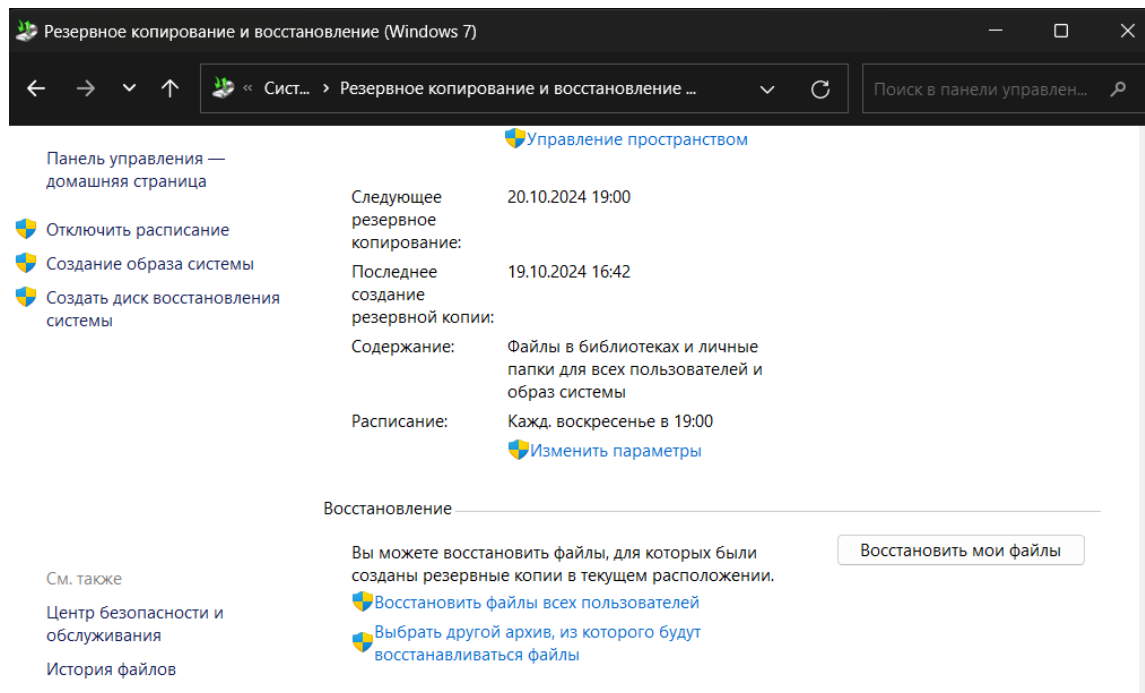
 Для восстановления образа может потребоваться диск восстановления системы.  
[Подробнее](#)

Сохранить параметры и запустить архивацию

Отмена

А для восстановления мы следуем следующим шагам:


1. Также заходим в панель управления, во вкладку “Система и безопасность” и “Резервное копирование и восстановление”.




## 2. Выбираем «Восстановить мои файлы».

### Восстановление

Вы можете восстановить файлы, для которых были созданы резервные копии в текущем расположении.

 [Восстановить файлы всех пользователей](#)

 [Выбрать другой архив, из которого будут восстанавливаться файлы](#)

Восстановить мои файлы

## 3. Следуем инструкциям по выбору копий для восстановления.

←

Восстановление файлов

×

Выберите в архиве файлы и папки для восстановления

Для всех файлов будет восстановлена самая последняя версия.  
[Выбрать другую дату](#)

Имя	Папка	Дата изменения
Нажмите кнопку "Обзор файлов", "Обзор папок" или "Поиск" для добавления файлов к этому списку.		

Поиск...

Обзор файлов

Обзор папок

Удалить

Удалить все

Далее

Отмена

## Linux/Ubuntu

Изучив предложенную информацию в интернете, можно выделить следующие шаги для резервного копирования и восстановления для данных ОС.

Шаги для резервного копирования:

1. Использование `rsync` (Этот метод позволяет синхронизировать файлы из исходного каталога в резервный)

```
rsync -avh --delete /source_directory /backup_directory|
```

2. Использование `tar` для архивирования (Создает сжатый архив для хранения)



```
tar -cvpzf backup.tar.gz /source_directory|
```

Шаги для восстановления:

1. Для восстановления с использованием tar (Извлекает архив в указанное место)

```
tar -xvpzf backup.tar.gz -C /restore_directory|
```

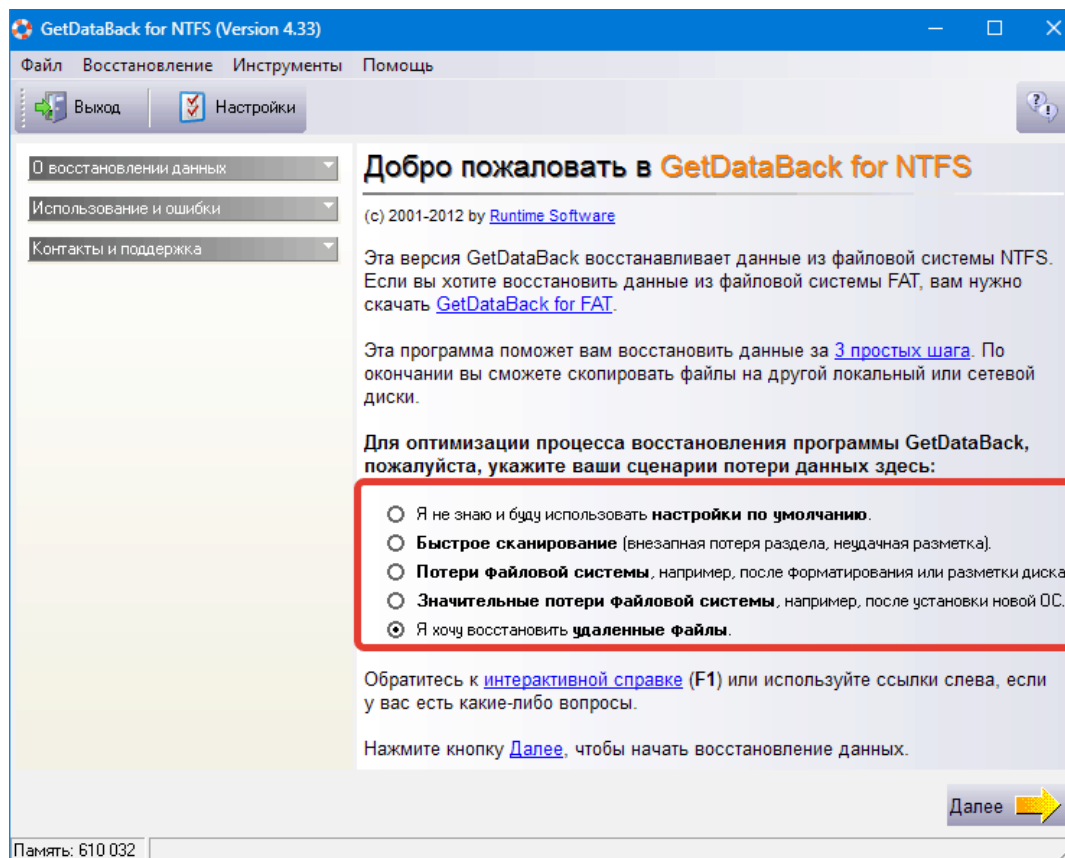
## Системы резервного копирования и восстановления

- Функции: Создание резервных копий, шифрование, автоматическое расписание, выборочная восстановление.
- Конфигурация: Настройка источников данных, места хранения и частоты создания копий.
- Выполнение и восстановление:
  - Бесплатные системы: Duplicati, Bacula.
  - Лицензированные системы: Acronis True Image, Veeam.
  - Онлайн-системы: Backblaze, Google Drive.

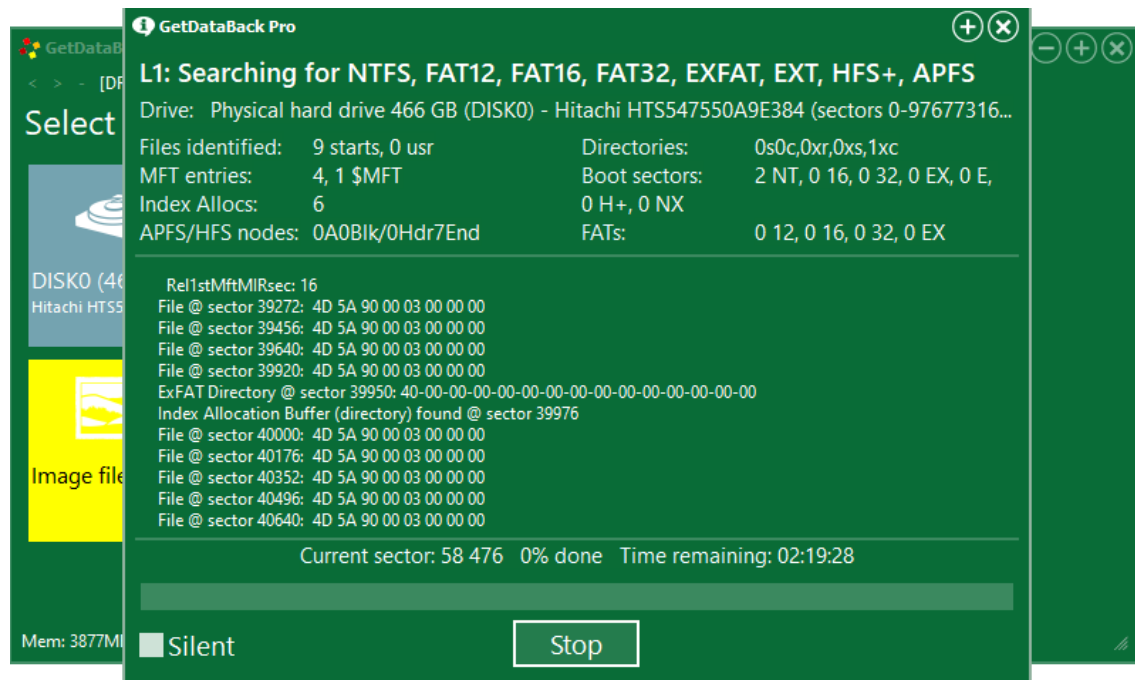
### ***GetDataBack***

Данное программное средство предназначено для восстановления информации с исправных носителей, утерянной в результате форматирования, удаления, установки ОС, сбоев в файловой системе и/или в структуре разделов на диске, флешке или рэйд-массиве. Существует две разновидности утилиты: для файловой системы *FAT* и для *NTFS*. *FAT* использует таблицу размещения файлов для отслеживания расположения файлов на диске. *NTFS* предлагает расширенные функции, такие как права доступа к файлам, шифрование, сжатие и ведение журнала.

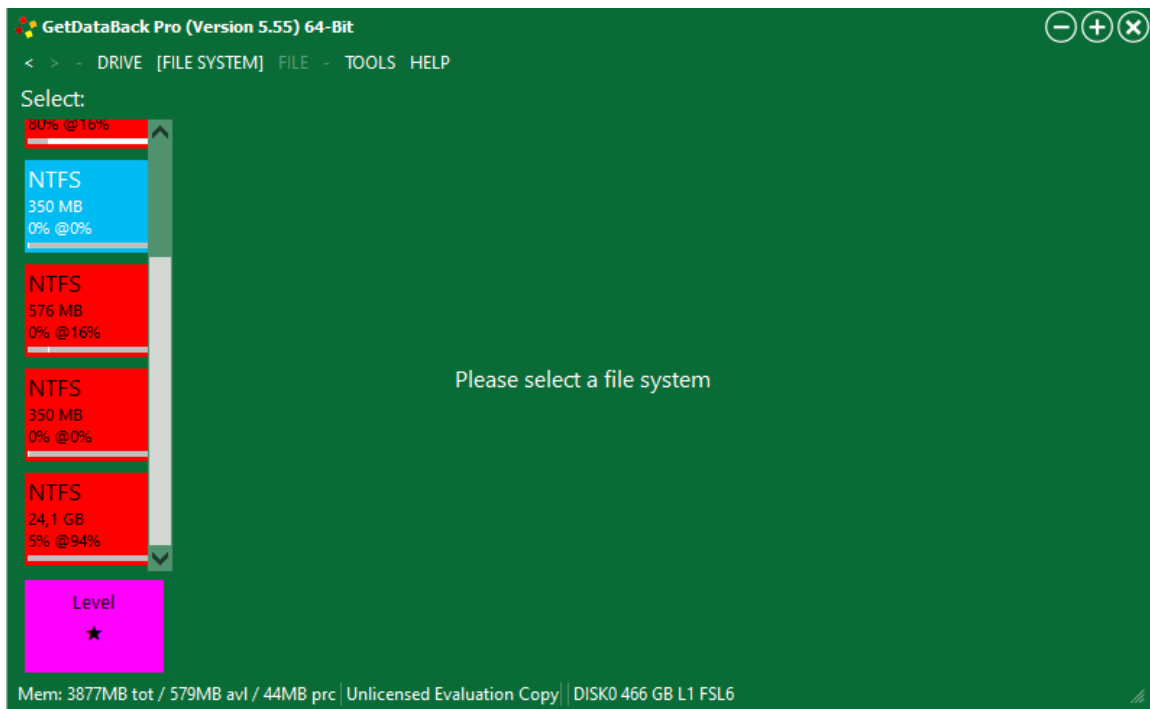
Я покажу работу данного приложения на основе *NTFS*. Скачав приложение, при запуске нам предлагается выбор сценария, по которому данные были утеряны, и согласно полученным сведениям утилита сформирует масштабы диагностики устройства.



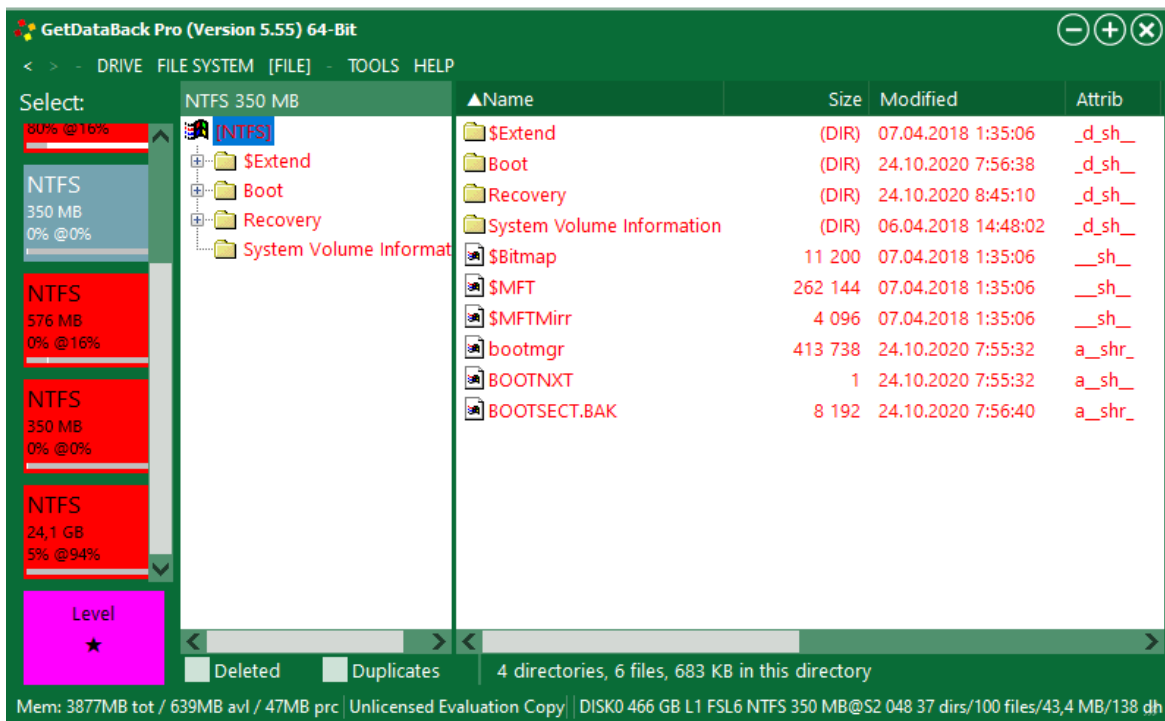
После выбора сценария потери данных жмём кнопку «Далее» и выбираем диск (или раздел), откуда будем восстанавливать информацию.



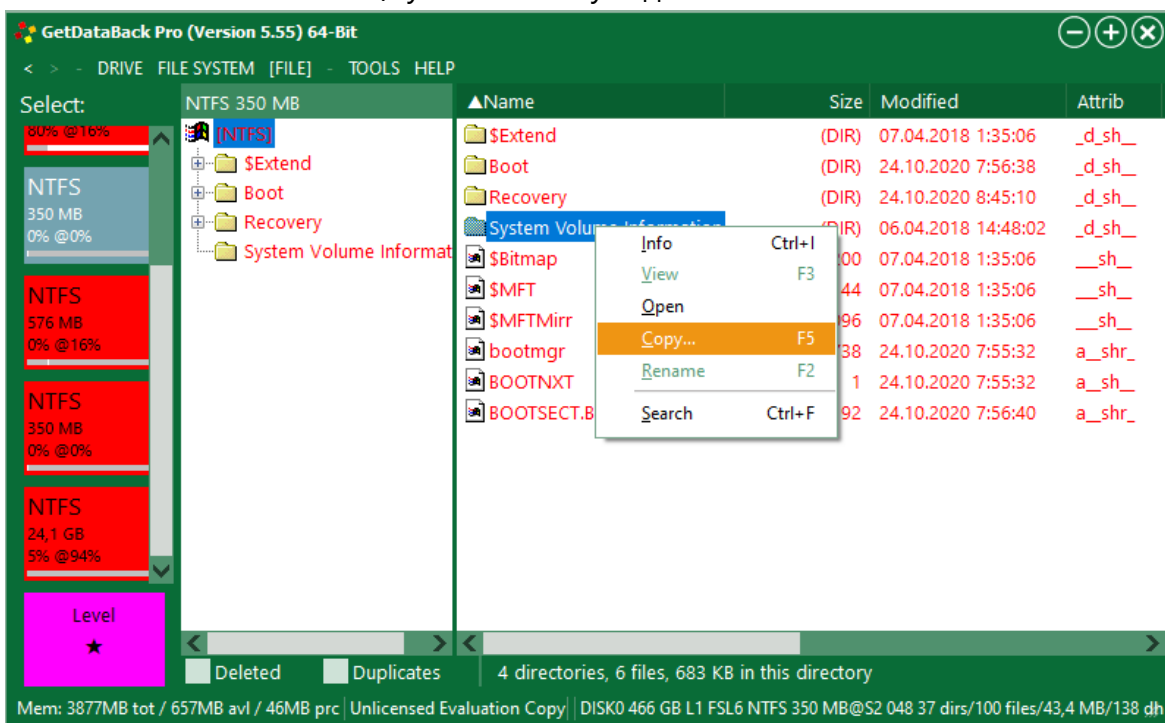
На следующем шаге программа определит файловую систему, нажимаем «Далее».



Просканировав систему, программа открывает структуру диска. Внизу интерфейса есть обозначения, сориентировавшись по ним, можно сразу увидеть нужные файлы.



Выбираем объект, который нужно восстанавливать (опция «копировать» из контекстного меню объекта), указываем путь для восстанавливаемого элемента.



## ***Vault Technology (CyberArk)***

Vault Technology (CyberArk) — это специализированное решение, разработанное для защиты критически важных данных и учетных данных от киберугроз. Эта технология часто используется в корпоративной среде для защиты от взломов, атак программ-вымогателей, утечек данных и других угроз.

Принципы работы: Использует механизм изоляции и многоуровневую аутентификацию для защиты данных. Доступ к данным возможен только через строго контролируемые каналы, что исключает возможность прямого доступа к хранилищу.

### Преимущества:

- Высокий уровень безопасности
- Многоуровневая аутентификация
- Мониторинг и аудит (ведется журнал всех действий пользователей в системе)
- Восстановление после атак

### Недостатки:

- Стоимость
- Сложность внедрения (требует тщательной настройки и интеграции с существующими системами компании)
- Требования к инфраструктуре (для обеспечения изоляции и защиты данных может потребоваться выделенная инфраструктура, что увеличивает затраты на оборудование и поддержку)

### Применение:

- В крупных компаниях и корпорациях. Защита от атак вымогателей, кражи данных и обеспечения безопасности для критически важных сервисов.
- В финансовом секторе. Защита информации о банковских транзакциях и клиентских данных.
- В государственных структурах. Обеспечение безопасности данных в критически важных инфраструктурах, таких как энергетика и транспорт.
- В IT-компаниях и облачных сервисах. Защита учетных данных и ключей доступа для облачных платформ и разработчиков.

В заключение можно сделать вывод, что CyberArk Vault Technology — это мощное решение для защиты привилегированных учетных данных и чувствительной информации. Оно обеспечивает высокий уровень безопасности, но требует значительных затрат на внедрение и поддержку. Для организаций, которые ценят безопасность своих данных, это решение может стать ключевым элементом в их стратегии защиты от киберугроз.

### **Процесс восстановления с CD/DVD**

1. Запустить программу для восстановления и выбрать устройство.
2. Сканировать диск и выбрать файлы для восстановления.

### **Восстановление с карт памяти**

1. Подключить карту памяти к компьютеру.
2. Запустить программу для восстановления, выбрать карту памяти и выполнить сканирование.

## **Вывод**

В ходе лабораторной работы мы научились основам резервного копирования и восстановления данных в операционных системах Windows и Linux, освоили инструменты и команды для автоматизации этих процессов. Узнали о системах защиты данных, таких как CyberArk, и их роли в обеспечении безопасности привилегированных учетных данных. Также приобрели навыки использования программ для восстановления утраченной информации с различных носителей, что важно для предотвращения потерь данных в случае сбоев или атак.

## Библиография

1. [GetDataBack FAT/NTFS инструкция как пользоваться Программы для восстановления данных \(mhdd.ru\)](#)
2. [Что такое резервное копирование данных? — Подробнее о резервном копировании данных — AWS \(amazon.com\)](#)
3. [Восстановление утерянных или удаленных файлов - Служба поддержки Майкрософт \(microsoft.com\)](#)
4. [CyberArk Software \(softprom.com\)](#)