Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Вятский государственный университет»

Колледж ВятГУ

**ОТЧЕТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ №5**

**«Составление плана обеспечения непрерывной работы и восстановления»**

**«МДК 06.02** **Инженерно-техническая поддержка сопровождения информационных систем»**

Выполнил: студент учебной группы

ИСПк-302-52-00

Холин П.Э.

Преподаватель:

Самоделкин П.А.

Киров

2024

**Цель работы -** изучение приемов и методов организации непрерывной работы информационных систем, подлежащих защите.

**Задание**:

1. Изучить:

* порядок обеспечения непрерывной работы и восстановления.
* меры обеспечения непрерывной работы и восстановления автоматизированной системы.
* средства обеспечения непрерывной работы и восстановления информации.
* порядок составления Плана защиты и Плана обеспечения непрерывной работы и восстановления информации.
* программные и информационные ресурсы резервного копирования в Системе
* технические средства, подлежащие дублированию (резервированию) в Системе
* обязанности и действия персонала по обеспечению непрерывной работы и восстановления системы.

2. Составить План обеспечения непрерывной работы и восстановления информации на вашем компьютере.

**Результаты выполнения задания**

### ****План обеспечения непрерывной работы и восстановления информации****

#### ****1. Общие положения****

1.1. Цель плана – обеспечить защиту и сохранность данных, минимизировать последствия кризисных ситуаций и оперативно восстановить работоспособность системы.

1.2. Потенциальные кризисные ситуации:

* Угрожающие: физическая потеря оборудования, полное нарушение функционирования операционной системы, уничтожение важной информации.
* Серьезные: потеря данных, снижение производительности компьютера, проникновение вирусного ПО.

**2. Меры обеспечения непрерывной работы**

2.1. Организационные меры:

* Регулярное создание резервных копий важной информации.
* Настройка автоматического копирования (раз в неделю).

2.2. Технические меры:

* Использование внешних дисков и облачного хранилища для копий.
* Установка антивирусного ПО и регулярное его обновление.

#### ****3. Резервное копирование****

3.1. Объекты резервирования:

* Важные документы (рабочие файлы, проекты).
* Системные настройки и ключевые программы.

3.2. Средства:

* Внешний жесткий диск на 1 ТБ.
* Облачный сервис (Google Drive, Яндекс Диск).

3.3. Регламент:

* Полное копирование системы осуществляется один раз в месяц.
* Инкрементное копирование должно фиксировать только новые или измененные данные раз в день.

#### ****4. Действия в случае кризисных ситуаций****

4.1. При угрозе утраты данных:

* При обнаружении подозрительного поведения системы или сбоя в её работе необходимо незамедлительно отключить компьютер от сети
* Использовать аварийный режим ОС для восстановления.

4.2. При потере данных:

* Загрузить резервную копию с внешнего носителя.
* Использовать программное обеспечение для восстановления удаленных данных (Recuva, EaseUS).

4.3. Восстановление системы:

* Перезагрузить компьютер в безопасном режиме.
* Заменить поврежденные файлы резервными копиями.

#### ****5. Пересмотр плана****

5.1. Полный пересмотр плана должен осуществляться не реже одного раза в год.

5.2. Частичный пересмотр может проводиться по мере необходимости (при добавлении нового оборудования или обновлении операционной системы).

#### ****6. Ответственные за реализацию****

Владелец компьютера обязан следить за соблюдением всех положений данного плана. Он несет ответственность за своевременное резервное копирование данных, установку обновлений системы и программного обеспечения, а также контроль за состоянием оборудования.

**Выводы по работе**

В ходе работы был разработан план обеспечения непрерывной работы и восстановления информации для личного компьютера. Были проанализированы основные кризисные ситуации, их классификация и меры по минимизации ущерба. Особое внимание уделено процедурам резервного копирования, восстановлению данных, а также действиям в случае потери работоспособности системы. План включает в себя рекомендации по техническим и организационным мерам, а также расписание их выполнения.