МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ ТЫВА
Государственное бюджетное профессиональное образовательное учреждение
Республики Тыва
«Тувинский техникум информационных технологий»

ПРИКАЗ

«01» 12 2023 г. № 1639

г. Кызыл

Об утверждении Положения резервного копирования информационных систем в ГБПОУ РТ «Тувинский техникум информационных технологий»

В соответствии с Федеральным законом от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить Положение резервного копирования информационных систем в ГБПОУ РТ «Тувинский техникум информационных технологий» согласно приложению.
2. Контроль над исполнением настоящего приказа возложить на ответственного за обеспечение безопасности персональных данных в ГБПОУ РТ «Тувинский техникум информационных технологий».
3. Приказ вступает в силу со дня его подписания.

Директор Ховалыг С-С.А.

	Министерство образования Республики Тыва
	Государственное бюджетное профессиональное образовательное учреждение Республики Тыва «Тувинский техникум информационных технологий»

УТВЕРЖДЕН
приказом № 1639
от 01.12.2023 г

ПОЛОЖЕНИЕ

резервного копирования информационных систем в Государственном бюджетном профессиональном образовательном учреждении Республики Тыва «Тувинский техникум информационных технологий»

ИНА-48
Версия 1.0

Принято на заседании
Педагогического совета
Протокол № 1
«25» 08 2023 г.

Ответственность	Должность	Фамилия/подпись	Дата
Разработал	Специалист по работе с общественностью	Лен-оол А.Ю.	05.12.2023г
Согласовал	Заместитель директора по инновационно-цифровому образованию	Ооржак М-Н.М.	05.12.2023г
Согласовал	Юрист-консульт	А.А. Дууза	
Согласовал	Председатель ССУ	Ч.Д. Куулар	
Согласовал	Председатель Родкомитета	У.Т. Ховалыг	

Кызыл, 2023 г.

Содержание

1.Общие положения

1.1. Настоящий стандарт определяет единый порядок резервного копирования информационных систем ГБПОУ РТ «Тувинский техникум информационных технологий» (далее – ГБПОУ РТ «ТТИТ»).

1.2. В настоящем положении используются следующие определения:

Резервное копирование – процесс создания копии текущего состояния данных на носителе (жестком диске, компакт-диске и т.д.), предназначенном для восстановления данных в случае их повреждения.

Администратор системы резервного копирования – сотрудник отдела АСУ, имеющий допуск к управление процессом резервного копирования и восстановления информации.

Ресурс сервера (далее Ресурс) – каталог, файл с данными, программное обеспечение или база данных.

Отчуждаемые носители – портативные устройства, выполненные в форме USB брелока, смарт-карты или флеш-драйва, обеспечивающие хранение информации.

Операционная система – комплекс взаимосвязанных программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем.

Съемные носители информации – CD, DVD, Blue-ray диски.

СУБД – система управления базами данных.

2. Основная часть

2.1 Целью резервного копирования является предотвращение потери информации при сбоях оборудования, программного обеспечения, в критических и кризисных ситуациях.

2.2 Наиболее частыми причинами потери информации могут быть:

- аппаратные сбои;
- сбои операционной системы и прикладного программного обеспечения;
- компьютерные вирусы;
- непреднамеренное удаление информации, ошибки пользователей;
- преднамеренное удаление информации.

2.3 Места хранения резервных копий:

- сервера;
- рабочие станции;
- сетевые хранилища данных.
- отчуждаемые носители информации.

2.4 Объекты хранения информации:

- системное программное обеспечение, размещенное на серверах.
- прикладное программное обеспечение, размещенное на серверах.
- базы данных информационных систем, размещенные на серверах.

- документация подразделений ГБПОУ РТ «ТТИТ», хранящаяся на файлообменном сервере.

2.5 Резервному копированию подлежит информация следующих основных категорий:

- персональная информация пользователей (личные рабочие каталоги на файловых серверах);
- групповая информация пользователей (общие каталоги подразделений);
- информация, необходимая для восстановления работоспособности Ресурсов ГБПОУ РТ «ТТИТ».

3. Характеристики резервного копирования и восстановления

3.1 Резервное копирование больших объемов данных необходимо проводить в ночное время суток и выходные дни, исходя из наименьшей загруженности информационных систем ГБПОУ РТ «ТТИТ» в это время.

3.2 Методы резервного копирования:

- клонирование (point-in-time), т.е. создание нескольких физических копий томов (клонов);
- создание мгновенной копии (snapshot), т.е. создание логической копии диска, его образа.
- копирование:

•полное копирование - создание полной копии (одна копия);

•инкрементальное копирование - создание копий измененных данных, которые были изменены после последнего полного, инкрементального или дифференциального копирования (несколько копий, первая запись – это полная копия, вторая запись – копия только тех данных, которые были изменены со времени первой записи, а на третьем этапе копируются данные модифицированные со времени второго этапа и т.д.);

•дифференциальное копирование - создание последней копии измененных данных со времени проведения полного копирования (две копии, первая запись – это полная копия, а на последующих этапах копируются только данные, которые изменились со времени проведения полного копирования).

3.3 В соответствии требования критичности потери информации информационные ресурсы ГБПОУ РТ «ТТИТ» условно разделяются на и две категории:

а) Критичные.

Резервное копирование осуществляется не реже 1 раз в сутки, с глубиной хранения не менее 1 недели. Данные касающиеся финансово-хозяйственной деятельности ГБПОУ РТ «ТТИТ» (базы данных 1С: Зарплата и кадры, 1С: Бухгалтерия), web-ресурсы: корпоративный портал и сайт ГБПОУ РТ «ТТИТ». Документация подразделений ГБПОУ РТ «ТТИТ», хранящаяся на файлообменном сервере, переносимые профиля удаленных рабочих столов пользователей.

б) Не критичные.

Резервное копирование осуществляется не реже 2 раза в месяц, с глубиной хранения не менее 1месяца.

3.4 Общие вопросы процедуры

Кроме плановых случаев, механизмы резервного копирования задействуются при модернизации и установке нового оборудования и прикладного программного обеспечения, обеспечивая перенос и резервирование данных на обновляемом сервере или рабочем месте.

Резервное копирование производится согласно расписанию разработанному администратором резервного копирования и утвержденному заместителем директора по инновационно-цифровому образованию (приложение 1).

4. Схемы резервного копирования

4.1 Создание и хранение резервной копии на оборудовании ГБПОУ РТ «ТТИТ». Чтобы снизить вероятность потери информации, настоятельное рекомендуется хранить файлы оригинальных данных и их резервные копии на разных системах хранения данных.

4.2 Хранение резервных копий на съемных или отчуждаемых носителях.

5. Организация резервного копирования

5.1 Обязанность администратора системы резервного копирования возлагается на системного администратора, в случае его отсутствия на лицо его замещающего.

5.2 Основными задачами Администратора системы резервного копирования являются:

- составление плана резервного копирования и проверки резервных копий;
- установление жизненного цикла и календаря операций;
- ежедневный обзор логов процесса резервного копирования;
- защита базы данных резервного копирования;
- ежедневное определение временного окна резервного копирования;
- развитие системы резервного копирования;
- манипуляции с резервными копиями;
- еженедельная проверка целостности резервных копий.

5.3 Основные обязанности Администратора системы резервного копирования:

- обеспечить функционирование и поддержание работоспособности средств системы резервного копирования и восстановления информации;
- немедленно докладывать заместителю директора по инновационно-цифровому образованию, о выявленных попытках несанкционированного доступа к резервируемой информации, выявленных ошибках и сбоях при резервном копировании, а также принимать необходимые меры по их устранению;

- принимать меры по восстановлению работоспособности средств системы резервного копирования информации.

5.4 Контроль результатов всех процедур резервного копирования осуществляется Администратором системы резервного копирования.

6. Восстановление информации из резервных копий

6.1 В случае необходимости восстановление данных из резервных копий, производится Администратором резервного копирования или лицом его замещающего.

6.2 Восстановление данных из резервных копий происходит в случае удаления данных или нарушения целостности данных, вследствие воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

6.3 При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными инкрементальными резервными копиями.

Лист ознакомления

№ п/п	Должность	Ф.И.О.	Подпись	Дата

№ п/п	Должность	Ф.И.О.	Подпись	Дата