МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА АВТОМОБИЛЬНОГО ТРАНСПОРТА, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ТЕХНИЧЕСКИМ ДИСЦИПЛИНАМ

Организация системы резервного копирования при обеспечении защиты информации в образовательной организации

Магистерская диссертация
по направлению: 44.04.04 Профессиональное обучение (по отраслям)
Направленность (профиль): Управление информационной безопасностью в профессиональном образовании
Форма обучения заочная

Проверка на объем заимствований:
80,47 % авторского текста

Работа рекомендована к защите
«17» января 2022 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил(а):
Студент(ка) группы ЗФ-309-210-2-1
Белов Алексей Иванович

Научный руководитель:
Дмитриев Михаил Сергеевич, д.тех.н., профессор

Челябинск
2022

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность исследования. Усиление роли информационных технологий в процессах управления образовательных организаций обусловливает повышение требований к целостности и доступности данных в течение их жизненного цикла. В последние годы возросло внимание к системам резервного копирования — наиболее распространенному средству обеспечения сохранности данных. Проводится большое количество исследований, нацеленных на их совершенствование. Одно из основных направлений исследований связано с улучшением процессов управления хранением данных, разработкой новых алгоритмов резервного копирования, совершенствованием процесса восстановления данных.

Резервное копирование - это процесс создания когерентной (непротиворечивой) копии данных. Резервное копирование становится все более важным на фоне значительного увеличения объема данных в компьютерной индустрии. Подсистема резервного копирования - очень важная часть любой информационной системы.

При правильной ее организации она способна решить сразу же две задачи. Во-первых, надежно защитить весь спектр важных данных от утери. Во-вторых, организовать быструю миграцию с одного ПК на другой в случае необходимости, то есть, фактически обеспечить бесперебойную работу сотрудников. Только в этом случае можно говорить об эффективной работе резервного копирования. Овладение тактикой резервного копирования - неотъемлемый атрибут профессионализма пользователя и системного администратора.

Создание системы резервного копирования является немаловажной задачей при построении ИТ-инфраструктуры и реализации политики информационной безопасности организации профессионального образования. Но почему-то важность резервирования данных многие осознают только после потери критически важной информации.

Сложность проблемы эффективного хранения усугубляется наблюдаемым экспоненциальным ростом количества данных, который, согласно исследованиям, ведущего международного аналитического агентства IDC, составляет 50-100 % ежегодно. Планирование ожидаемых объемов данных является необходимой составляющей процесса управления их хранением. Инструментарий оценки роста объема хранилищ для резервирования данных практически не представлен в современных системах. Требуется разработка способа прогнозирования объема хранимых резервных копий.

В общем случае в хранилище может существовать несколько наборов элементарных резервных копий, пригодных для восстановления. Это обусловливает проблему нахождения оптимального набора копий для восстановления независимо от использованного алгоритма с учетом утраченных и дополнительно созданных копий.

Для выполнения процедуры резервного копирования обычно создаются специальные программно-аппаратные подсистемы, называемые подсистемами резервного копирования. Они как раз и предназначены как для проведения регулярного автоматического копирования системных и пользовательских данных, так и для оперативного восстановления данных. Хранение информации отдельно от системных файлов уже является обязательным правилом. В случае обычного пользователя это означает, как минимум, разделение HDD на три логических диска: для системы, для приложений, для данных. В случае образовательной организации с большим объемом конфиденциальной информации - размещение информации на других, не системных физических дисках. Эта мера облегчает и саму операцию архивирования данных. Принцип раздельного хранения информации относится и к файловым архивам и к образам дисков. Их необходимо также хранить как минимум на несистемных разделах одного HDD. Принцип раздельного хранения информации должен реализовываться еще жестче: как минимум одна из копий должна храниться в отдельном

месте, чтобы не потерять информацию в случае непредвиденных обстоятельств.

Это определяет актуальность создания системы защиты информации на объекте, ориентированной на угрозы безопасности, представленные в документах ФСТЭК и ФСБ России.

Анализ состояния проблемы информационной безопасности в организациях профессионального образования позволил выявить *противоречие* между целесообразностью использования комплексных мер при реализации политики ИБ образовательного учреждения и недостаточной защищенностью от потери или искажения данных.

Это определило проблему исследования, заключающуюся в необходимости внедрения системы резервного копирования для реализации политики безопасности в организации профессионального образования.

Таким образом, можно сделать вывод, что тема исследования «Организация системы резервного копирования при обеспечении защиты информации в образовательной организации» является актуальной, а полученные результаты имеют важное практическое значение.

Цель исследования: теоретико-методическое обоснование и разработка рекомендаций по организации системы резервного копирования при обеспечении защиты информации в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего».

Объект исследования: процесс обеспечения информационной безопасности в организации профессионального образования.

Предмет исследования: организация системы резервного копирования.

Гипотеза исследования: разработка рекомендаций по организации системы резервного копирования и их внедрение позволит повысить уровень информационной безопасности в организации профессионального образования.

Задачи исследования:

– проанализировать понятие, назначение, функции и особенности систем резервного копирования;

– изучить технологии резервного копирования и хранения резервных копий и данных, проанализировать программно-технические средства резервного копирования, наиболее подходящие для реализации систем резервного копирования в организации профессионального образования;

– проанализировать информационные системы в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего»;

– разработать рекомендации по организации системы резервного копирования при обеспечении защиты информации в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего»;

– произвести оценку эффективности разработанных рекомендаций и экономических затрат на их реализацию.

Для решения поставленных задач были использованы следующие *методы исследования:* изучение и анализ теоретико-методической литературы по теме исследования; документоведческий метод (анализ документации образовательной организации); анализ и сопоставление имеющихся средств для защиты данных; анализ и классификация собранных данных с последующим моделированием и проектированием системы защиты персональных данных; метод апробации результатов; метод экспертной оценки качества разработанных мер защиты.

Теоретической и методологической базой исследования явились нормативно-правовые акты законодательства Российской Федерации, а также труды следующих авторов: Авдеев М.Ю., Алексеев С.С., Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С., Бадьина А., Бархатова Е.Ю., Беспалов Ю.Ф., Сенаторова Н.В., Терещенко Л.К. Хужокова И.М., Якушев В.С.

Состояние изученности проблемы.

Общетеоретические аспекты исследования информационной безопасности представлены в публикациях Е. Б. Белова, Е. А. Ерофеева, В.Н. Лопатина, А. А. Стрельцова, В. А. Тихонова, В. В. Райх, Ю. С. Уфимцева.

Крупный вклад в развитие теории и практики информационной безопасности внесли И.И. Быстров, В.А. Герасименко, О.Ю. Гаценко, А.А. Грушо, В.С. Заборовский, П.Д. Зегжда, Д.П. Зегжда, В.А. Конявский, А.А. Малюк, А.А. Молдовян и др.

Ряд работ посвящен системно-управленческому аспекту информационной безопасности: А. А. Кононова, А. В. Манойло, С. А. Мелина, Ю. А. Родичева, Д. И. Правикова, А. С. Устинова, Д. Б. Фролова.

Практическая значимость работы заключается в анализе имеющихся на рынке систем резервного копирования и выборе наиболее подходящей для внедрения в систему информационной безопасности ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего»; возможности применения разработанных рекомендаций в других учебных заведениях СПО.

База исследования: ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего».

Ход исследования и его результаты докладывались и обсуждались на международных конференциях: Международная научно-практическая конференция «Синтез науки и образования в решении глобальных проблем современности», г. Стерлитамак, февраль 2022 года; Международная научно-практическая конференция «Научно-технический прогресс и инновационные технологии», г. Ижевск, декабрь 2021 г.

Структура магистерской диссертации: работа состоит из введения, трех глав, заключения, списка использованных источников, состоящего из 51 наименования.

ГЛАВА 1 ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ РАЗРАБОТКИ И ПРИМЕНЕНИЯ СИСТЕМ РЕЗЕРВНОГО КОПИРОВАНИЯ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ

1.1 Понятие, назначение, функции и особенности систем резервного копирования

Термины и определения.

Резервное копирование (англ. backup copy) — процесс создания копии данных на носителе (жестком диске, дискете и т. д.), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

Система резервного копирования – это программный или программно-аппаратный комплекс для создания копий данных с определенной периодичностью для их последующего восстановления.

Стратегия резервного копирования - одна или несколько операций резервного копирования данных.

Резервное копирование или бэкап - процесс создания копии данных на носителе (оптический диск, жесткий диск и другие) с целью восстановления данных в первоначальном месте их расположения в случае их повреждения или разрушения. Резервное копирование предназначено для быстрого и недорогого восстановления информации (документов, приложений, настроек) в случае утери рабочей копии по какой-либо причине.

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

Наиболее частыми причинами потери информации могут быть:

- аппаратные сбои;
- сбои операционной системы и прикладного программного обеспечения;
- вирусы, черви и троянские кони;

– непреднамеренное уничтожение информации, ошибки пользователей;

– преднамеренное уничтожение информации.

Реализация основной задачи резервного копирования способствует также упорядочению информации и процедур ее использования. В частности, становится ясно, какая информация хранится на том или ином рабочем месте, как она используется пользователями и программным обеспечением, появляется возможность оценить ее количественные характеристики, например, объемы и частоту использования.

Жизненный цикл информации включает:

– создание;

– копирование;

– использование;

– хранение: текущее (требуется резервное копирование); долговременное (требуется архивирование).

Резервное копирование снимает зависимость информации от конкретного рабочего места, она становится перемещаемой и не привязанной к одному компьютеру или помещению. При возникновении критических ситуаций, которые могут привести к потере работоспособности оборудования или программного обеспечения, можно в краткие сроки перенести данные и ПО в другое место, на другой компьютер или в другое помещение.

Основные функции системы резервного копирования:

– создания резервных копий файлов, баз данных, приложений, системной информации и других необходимых данных;

– восстановление данных в случае утери информации;

– регулярное автоматизированное создание резервных копий на основании политик бэкапа;

– возможность восстановления нескольких версий файлов;

– надежное хранение резервных копий в течение установленного периода времени;

– обеспечение требуемого времени восстановления информации из резервных копий.

Места хранения электронной информации:

- сервера;
- рабочие станции.

Объекты хранения информации:

- ОС и утилиты;
- прикладное (специализированное) ПО;
- данные.

Методы резервного копирования:

1) клонирование (point-in-time), т.е. создание нескольких физических копий томов (клонов);

2) создание мгновенной копии (snapshot), т.е. создание логической копии диска, его образа;

3) 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).

К системам резервного хранения информации применяют три критерия и требования:

– предельная простота и быстрота внедрения данных технологий в любых масштабах предприятия - от небольшой фирмы до больших корпораций;

– надежность хранения информации – об этом критерии мы говорили выше;

– предельная простота и автоматизация эксплуатации внедренных систем.

Резервному копированию подлежит информация следующих основных категорий:

- персональная информация пользователей (личные каталоги на файловых серверах);
- групповая информация пользователей (общие каталоги отделов);
- информация, необходимая для восстановления серверов и систем управления базами данных (далее – СУБД);
- персональные профили пользователей сети;
- информация автоматизированных систем, в т.ч. баз данных;
- данные справочно-информационных систем общего использования («Гарант», «Консультант+» и т.п.);
- рабочие копии установочных компонент программного обеспечения рабочих станций;
- регистрационная информация системы информационной безопасности автоматизированных систем.

Машинным носителям информации, содержащим резервную копию, присваивается гриф конфиденциальности по наивысшему грифу содержащихся на них сведений в соответствии с «Перечнем сведений составляющих коммерческую тайну».

Существует два основных способа резервного копирования данных.

1. Создание бэкапа. В этом случае пользователь сам выбирает для копирования определенные файлы и / или папки. Так, к примеру, можно сделать резервную копию папки «Мои документы». При этом существует возможность выбора для копирования файлов определенных форматов, к примеру всех MP3-файлов или всех изображений в формате JPEG, которые хранятся в одной папке.

2. Создание образа - точной копии всего жесткого диска или одного из его разделов (включая операционную систему Windows, все установленные в системном разделе программы и данные). Основное преимущество данного способа: при полном выходе компьютера из строя операционную систему можно восстановить из образа. Кроме того, хорошая программа резервного копирования позволяет выполнять поиск внутри образа и последующее восстановление отдельных папок и файлов, ошибочно удаленных с компьютера.

В начале необходимо выбрать место для сохранения резервной копии, к примеру внешний жесткий диск, на котором достаточно свободного места. При полном резервном копировании программа создает из выбранных файлов один большой файл, содержащий резервные копии всех данных. Впоследствии при выполнении дифференциального или инкрементного копирования туда же записываются дополнительные данные.

Выбор накопителя. Встроенный жесткий диск - худший вариант: при возникновении механических дефектов винчестера резервная копия данных будет безвозвратно утеряна. Оптимальный вариант - приобретение внешнего жесткого диска, который будет использоваться исключительно для хранения копий.

График резервного копирования. При его составлении выполняйте следующие правила.

1. При покупке нового компьютера рекомендуется, не откладывая, выполнить полное резервное копирование. Так в случае возникновения

проблем вы всегда сможете восстановить первоначальное состояние системы.

2. Повторное полное резервное копирование необходимо произвести тогда, когда вы установите все программы, с которыми обычно работаете, и драйверы для всех компонентов компьютера, а также настроите доступ в Интернет.

3. Перед проведением на компьютере важных изменений, независимо от того, касаются они аппаратного или программного обеспечения, также необходимо выполнять резервное копирование данных.

4. Выполняйте резервное копирование регулярно, через небольшие промежутки времени.

Способ резервного копирования. Вы можете регулярно выполнять полное резервное копирование данных. Однако не все файлы постоянно изменяются. Кроме того, на это уходит много времени и места на диске, так как сохраняется содержимое всех дорожек диска. Существует два различных способа регулярного обновления резервных копий файлов. Поэтому при слежении за актуальностью данных вы можете выбирать между дифференциальным и инкрементным копированием.

Под дифференциальным копированием понимается копирование изменившейся информации за определенный отрезок времени. Причем каждое последующее копирование включает в себя как изменившиеся файлы, так и те, которые остались неизмененными со времени полного бэкапа. То есть дифференциальное копирование - это копирование всей разницы между первым и последним копированием.

Инкрементный бэкап копирует только новые и изменившиеся файлы со времен предыдущего копирования, а не первого. Поэтому, как правило, дифференциальный бэкап занимает больше места на носителе, чем инкрементальный. Но инкрементальный бэкап сложнее восстанавливать, так как приходится учитывать не только первый и последний бэкап-файлы, но и все промежуточные инкременты.

Хорошие программы резервного копирования сжимают данные для экономии места на диске и предоставляют следующие функции резервного копирования, такие как планировщик, возможность шифрования данных и дополнительную защиту бэкапа паролем.

Потеря информации возможна вследствие непреодолимых обстоятельств – разгул стихии, землетрясение. Так что и нужно предусмотреть возможность восстановления информации вследствие всего этого. Лучше всего хранить информацию, которая была зарезервирована, в другом помещении.

Если же информация повредилась в результате вирусной атаки или действия вредоносного программного обеспечения, нужно установить хорошую антивирусную защиту на все компьютеры, входящие в локальную сеть, и периодически обновлять антивирусные базы сигнатур. При этом нужно еще и хранить копии важной информации в таком месте, до которого вредоносное программное обеспечение даже теоретически добраться не сможет.

При сбое или уничтожении информации по вине человеческого фактора нужно тщательнейшим образом распределить все права доступа к ресурсам в сети, организовать регулярное резервное копирование информации, и регулярно обновлять используемое на компьютерах программное обеспечение.

1.2 Технологии резервного копирования и хранения резервных копий и данных

В зависимости от важности хранимой на компьютере информации и от частоты её использования, выполняют несколько видов резервного копирования данных:

1. Полное резервное копирование (Full backup).
2. Дифференциальное резервное копирование (Differential backup).
3. Инкрементное резервное копирование (Incremental backup).

1. Полное резервное копирование.

Является главным и основополагающим методом создания резервных копий, при котором выбранный массив данных копируется целиком. Это наиболее полный и надежный вид резервного копирования, хотя и самый затратный. В случае необходимости сохранить несколько копий данных общий хранимый объем будет увеличиваться пропорционально их количеству. Для предотвращения большого объёма использованных ресурсов используют алгоритмы сжатия, а также сочетание этого метода с другими видами резервного копирования: инкрементным или дифференциальным. И, конечно, полное резервное копирование незаменимо в случае, когда нужно подготовить резервную копию для быстрого восстановления системы с нуля.

Достоинства метода:

– легкий поиск файлов - Поскольку выполняется резервное копирование всех данных, содержащихся на устройстве, для поиска нужного файла не требуется просматривать несколько носителей;

– текущая резервная копия всей системы всегда расположена на одном носителе или наборе носителей - Если потребуется восстановить всю систему, то всю необходимую информацию можно найти в последней полной резервной копии.

Недостатки метода:

– избыточная защита данных - поскольку большинство файлов системы изменяются достаточно редко, то каждая последующая полная резервная копия представляет собой копию данных, сохраненных в ходе первого полного резервного копирования. Для полного резервного копирования требуется большой объём носителя.

– полное резервное копирование занимает больше времени - Для создания полных резервных копий может потребоваться длительное время, в особенности, если для хранения выбраны устройства в сети.

2. Дифференциальное резервное копирование.

Отличается от инкрементного тем, что копируются данные с

последнего момента выполнения Full backup. Данные при этом помещаются в архив «нарастающим итогом». В системах семейства Windows этот эффект достигается тем, что архивный бит при дифференциальном копировании не сбрасывается, поэтому измененные данные попадают в архивную копию, пока полное копирование не обнулит архивные биты.В силу того, что каждая новая копия, созданная таким образом, содержит данные из предыдущей, это более удобно для полного восстановления данных на момент аварии. Для этого нужны только две копии: полная и последняя из дифференциальных, поэтому вернуть к жизни данные можно гораздо быстрее, чем поэтапно накатывать все инкременты. К тому же этот вид копирования избавлен от вышеперечисленных особенностей инкрементного, когда при полном восстановлении старые файлы, возрождаются из пепла. Возникает меньше путаницы. Но дифференциальное копирование значительно проигрывает инкрементному в экономии требуемого пространства. Так как в каждой новой копии хранятся данные из предыдущих, суммарный объем зарезервированных данных может быть сопоставим с полным копированием. И, конечно, при планировании расписания (и расчетах, поместится ли процесс бэкапа во временное «окно») нужно учитывать время на создание последней, самой большой, дифференциальной копии.

Достоинства метода:

– легкий поиск файлов - Для восстановления системы, защищенной с помощью стратегии дифференциального резервного копирования требуются две резервные копии - последняя полная резервная копия и последняя дифференциальная резервная копия. Время восстановления значительно меньше по сравнению со стратегиями резервного копирования, для которых требуются последняя полная резервная копия и все инкрементальные резервные копии, созданные с момента последнего полного резервного копирования;

– меньшее время резервного копирования и восстановления - Дифференциальное резервное копирование занимает меньше времени, чем

полное резервное копирование. Восстановление после аварии выполняется быстрее, поскольку для полного восстановления устройства необходимы только последняя полная резервная копия и дифференциальная резервная копия.

Недостаток метода: избыточная защита данных (сохраняются все файлы, измененные с момента последнего инкрементального резервного копирования. Таким образом, создаются избыточные резервные копии).

3. Инкрементное резервное копирование.

В отличие от полного резервного копирования в этом случае копируются не все данные (файлы, сектора и т.д.), а только те, что были изменены с момента последнего копирования. Для выяснения времени копирования могут применяться различные методы, например, в системах под управлением операционных систем семейства Windows используется соответствующий атрибут файла (архивный бит), который устанавливается, когда файл был изменен, и сбрасывается программой резервного копирования. В других системах может использоваться дата изменения файла. Понятно, что схема с применением данного вида резервного копирования будет неполноценной, если время от времени не проводить полное резервное копирование. При полном восстановлении системы нужно провести восстановление из последней копии, созданной Full backup, а потом поочередно восстановить данные из инкрементных копий в порядке их создания. Данный вид используется для того, чтобы в случае создания архивных копий сократить расходуемые объемы на устройствах хранения информации (например, сократить число используемых ленточных носителей). Также это позволит минимизировать время выполнения заданий резервного копирования, что может быть крайне важно в условиях, когда машина работает постоянно, или прокачивать большие объемы информации. У инкрементного копирования есть один нюанс: поэтапное восстановление возвращает и нужные удаленные файлы за период восстановления. Например: допустим, по выходным дням выполняется полное копирование, а

по будням инкрементное. Пользователь в понедельник создал файл, во вторник его изменил, в среду переименовал, в четверг удалил. Так вот при последовательном поэтапном восстановлении данных за недельный период мы получим два файла: со старым именем за вторник до переименования, и с новым именем, созданным в среду. Это произошло потому, что в разных инкрементных копиях хранились разные версии одного и того же файла, и в итоге будут восстановлены все варианты. Поэтому при последовательном восстановлении данных из архива «как есть» имеет смысл резервировать больше дискового пространства, чтобы смогли поместиться в том числе и удаленные файлы.

Достоинства метода:

– эффективное использование носителей - поскольку сохраняются только файлы, измененные с момента последнего полного или инкрементального резервного копирования, резервные копии занимают меньше места;

– меньшее время резервного копирования и восстановления - инкрементальное резервное копирование занимает меньше времени, чем полное и дифференциальное резервное копирование.

Недостаток метода: данные резервного копирования сохраняются на нескольких носителях.

Поскольку резервные копии расположены на нескольких носителях, восстановление устройства после аварии может занять больше времени. Кроме того, для эффективного восстановления работоспособности системы носители должны обрабатываться в правильном порядке.

В процессе выполнения резервного копирования данных появляется проблема выбора технологии хранения резервных копий и данных. В настоящее время особой популярностью пользуются следующие виды носителей:

1. Накопители на магнитных лентах.

2. Дисковые накопители.

3. Сетевые технологии.

1. Накопители на магнитных лентах.

Не только в крупных корпорациях, но и на предприятиях малого бизнеса хорошо понимают необходимость резервного копирования и восстановления информации. В системах масштаба предприятия и сетях крупных департаментов, в небольших компаниях и у индивидуальных пользователей одинаковым успехом пользуются потоковые накопители, или стримеры. В основе их конструкции лежит лентопротяжный механизм, работающий в инерционном режиме. Для обоснованного выбора системы резервного копирования надо ясно представлять себе достоинства и недостатки разных устройств, которые во многом определяются емкостью системы, ее быстродействием, надежностью и ценой. Основные стимулы к повышению производительности ленточных устройств среднего и старшего класса - это широкое использование Интернета и распространение корпоративных интрасетей, увеличение числа серверов (нужных, чтобы обеспечить рост этих сетей), а также ужесточение требований к хранению информации и ее восстановлению в случае аварий. Спрос на системы резервного копирования и хранения данных особенно подстегивается все более активным использованием таких приложений, как мультимедиа, видео по запросу, звуковое информационное наполнение, обработка изображений и т.п.

Применяются два метода записи на магнитную ленту: наклонный и линейный серпантинный. В системах наклонной записи несколько считывающих/записывающих головок размещают на вращающемся барабане, установленном под углом к вертикальной оси (аналогичная схема применяется в бытовой видеоаппаратуре). Движение ленты при записи/чтении возможно только в одном направлении. В системах линейной серпантинной записи считывающая/записывающая головка при движении ленты неподвижна. Данные на ленте записываются в виде множества параллельных дорожек (серпантина). Головка размещается на специальной

подставке; по достижении конца ленты она сдвигается на другую дорожку. Движение ленты при записи/чтении идет в обоих направлениях. На самом деле таких головок обычно устанавливается несколько, чтобы они обслуживали сразу несколько дорожек (они образуют несколько каналов записи/чтения).

Плюсы хранения данных на ленточном носителе:

– низкая стоимость;

– низкое энергопотребление накопителя;

– большие объемы данных;

– простой способ увеличения объема хранимых данных без значительных инвестиций.

Минусы хранения данных на ленточном носителе:

– низкая скорость доступа к данным;

– сложный процесс обработки параллельных запросов к данным.

2. Дисковые накопители.

Существует два наиболее часто встречающихся вида дисковых накопителей: накопители на жёстких магнитных дисках и накопители на оптических дисках.

Накопители на жестких магнитных дисках (Hard Disk Drive, HDD) являются основными устройствами оперативного хранения информации. Для современных одиночных накопителей характерны объемы от сотен мегабайт до нескольких гигабайт при времени доступа 5-15 мс и скорости передачи данных 1-10 Мбайт/с. Относительно корпуса сервера различают внутренние и внешние накопители. Внутренние накопители существенно дешевле, но их максимальное количество ограничивается числом свободных отсеков корпуса, мощностью и количеством соответствующих разъемов блока питания сервера. Установка и замена обычных внутренних накопителей требует выключения сервера, что в некоторых случаях недопустимо. Внутренние накопители с возможностью "горячей" замены (Hot Swap) представляют собой обычные винчестеры, установленные в специальные

кассеты с разъемами. Кассеты обычно вставляются в специальные отсеки со стороны лицевой панели корпуса, конструкция позволяет вынимать и вставлять дисководы при включенном питании сервера. Для стандартных корпусов существуют недорогие приспособления (Mobile Rack), обеспечивающие оперативную съемность стандартных винчестеров. Внешние накопители имеют собственные корпуса и блоки питания, их максимальное количество определяется возможностями интерфейса. Обслуживание внешних накопителей может производиться и при работающем сервере, хотя может требовать прекращения доступа к части дисков сервера.

Для больших объемов хранимых данных применяются блоки внешних накопителей - дисковые массивы и стойки, представляющие собой сложные устройства с собственными интеллектуальными контроллерами, обеспечивающими, кроме обычных режимов работы, диагностику и тестирование своих накопителей. Более сложными и надежными устройствами хранения являются RAID-массивы (Redundant Array of Inexpensive Disks - избыточный массив недорогих дисков). Для пользователя RAID представляет собой один (обычно SCSI) диск, в котором производится одновременная распределенная избыточная запись (считывание) данных на несколько физических накопителей (типично 4-5) по правилам, определяемым уровнем реализации (0-10). Например, RAID Level 5 позволяет при считывании исправлять ошибки и осуществлять замену любого диска без остановки обращения к данным.

Устройства считывания компакт-дисков CD-ROM расширяют возможности системы хранения данных NetWare. Существующие накопители обеспечивают скорость считывания от 150 кбайт/с до 300/600/900/1500 Кбайт/с для 2-,4-,6- и 10-скоростных моделей при времени доступа 200-500 мс. NetWare позволяет монтировать компакт-диск как сетевой том, доступный пользователям для чтения. Объем тома может достигать 682 Мбайт (780 Мбайт для Mode 2). Устройства CD-ROM

выпускаются с различными интерфейсами, как специфическими (Sony, Panasonic, Mitsumi), так и общего применения: IDE и SCSI. Сервер NetWare обслуживает только CD-ROM с интерфейсами SCSI, новые драйверы существуют и для IDE; устройства со специфическими интерфейсами могут использоваться только в DOS для инсталляции системы. С точки зрения повышения производительности предпочтительнее использование CD-ROM SCSI, однако они существенно дороже аналогичных IDE-устройств. В сервере с дисками SCSI применение CD-ROM с интерфейсом IDE может оказаться невозможным из-за конфликтов адаптеров.

Достоинствами таких накопителей является:

– быстрый доступ к данным;

– возможность параллельного доступа к данным без значительной потери скорости.

Недостатки дисковых накопителей:

– более высокая стоимость чем ленты;

– более высокое энергопотребление;

– более дорогое расширение системы хранения данных;

– невозможность обеспечения высокой безопасности копий.

3. Сетевые технологии.

Сетевое хранение данных построено на трех фундаментальных компонентах: коммутации, хранении и файлах. Все продукты хранения можно представить в виде комбинации функций данных компонентов. Поначалу это может вызвать замешательство: поскольку продукты хранения разрабатывались по совершенно разным направлениям, функции часто перекрывают друг друга.

В сети работает множество приложений типа «клиент-сервер» и различных видов распределенных приложений, но в то же время хранение является уникальным и специализированным типом приложения, которое может функционировать в нескольких сетевых средах. Поскольку процессы хранения тесно интегрированы с сетями, будет уместно напомнить, что

сетевые хранилища представляют собой системные приложения. Сервисами, которые предоставляются сетевыми приложениями хранения, могут пользоваться сложные корпоративные программы и пользовательские приложения. Как и в случае со многими технологиями, некоторые типы систем лучше отвечают требованиям сложных приложений высокого уровня.

Термин «коммутация» применяется ко всему программному и аппаратному обеспечению и к службам, которые обеспечивают транспортировку хранения и управление ею в сетевом хранилище. Сюда входят такие различные элементы, как разводка кабелей, сетевые контроллеры ввода-вывода, коммутаторы, концентраторы, аппаратура выборки адресов, контроль связи данных, транспортные протоколы, безопасность и резервы ресурсов. В сетевых хранилищах все еще широко используются технологии шин данных SCSI и ATA, и, скорее всего, они будут использоваться еще долго. Фактически продукты SCSI и ATA сегодня применяются гораздо чаще в технологии NAS. Существуют два важных различия между сетями хранения SAN и обычными локальными сетями LAN. Сети хранения SAN автоматически синхронизируют данные между отдельными системами и хранилищами. В сетевых хранилищах необходимы компоненты высокой степени точности для обеспечения надежной и предсказуемой среды. Несмотря на ограничения по расстоянию, параллельная SCSI -- чрезвычайно надежная и предсказуемая технология. Если новые технологии коммутации, такие как Fibre Channel, Ethernet и InfiniBand, сменят SCSI, они должны будут продемонстрировать аналогичный или лучший уровень надежности и предсказуемости. Имеется и такая точка зрения, которая рассматривает коммутацию как канал хранилища. Сам термин «канал», берущий свое начало в среде больших вычислительных машин, предполагает высокую надежность и работоспособность.

Хранение в основном затрагивает блочные операции адресного пространства, включая создание виртуальной среды, когда адреса

логического блока хранения отображаются из одного адресного пространства в другое. Вообще говоря, в сетевых хранилищах функция хранения почти не изменилась, если не считать двух заметных отличий. Первое -- это возможность нахождения технологий виртуализации устройства, например управление устройством внутри оборудования сетевого хранения. Этот вид функции иногда называют контроллером домена хранения или виртуализацией LUN. Второе главное отличие хранения заключается в масштабируемости. Продукты хранения, такие как подсистемы хранения, имеют значительно больше контроллеров/интерфейсов, чем предыдущие поколения шинной технологии, а также намного больший объем хранения.

Функция организации файлов представляет абстрактный объект конечному пользователю и приложениям, а также организует разметку данных на реальных или виртуальных устройствах хранения. Основную часть функциональности файлов в сетевых хранилищах обеспечивают файловые системы и базы данных; их дополняют приложения управления хранением, например операции резервного копирования, также являющиеся файловыми приложениями. Сетевое хранение к настоящему времени почти не изменило файловые функции, за исключением разработки файловых систем NAS, в частности файловой системы WAFL компании Network Appliance. Кроме упомянутых технологий хранения данных NAS и SAN, ориентированных на крупные и глобальные сети, в небольших локальных сетях доминирующее положение занимает технология DAS, в соответствии с которой хранилище находится внутри сервера, обеспечивающего объем хранилища и необходимую вычислительную мощность.

Простейшим примером DAS может служить накопитель на жестком диске внутри персонального компьютера или ленточный накопитель, подключенный к единственному серверу. Запросы ввода-вывода (называемые также командами или протоколами передачи данных) непосредственно обращаются к этим устройствам. Однако такие системы плохо масштабируются, и компании с целью расширения объема хранилища

вынуждены приобретать дополнительные серверы. Эта архитектура очень дорогая и может использоваться только для создания небольших по объему хранилищ данных.

Технология RAID.

RAID (избыточный массив недорогих / независимых дисков) - это технология, используемая для защиты данных в случае отказа диска. Эта технология имеет несколько уровней, из которых каждый защищает данные по-разному.

RAID может быть реализован с помощью аппаратного или программного обеспечения, либо их комбинации. Аппаратный RAID обычно проще в использовании, потому что он предоставляет его сразу после запуска аппаратного устройства.

Программный RAID использует программное обеспечение, что означает нагрузку на процессор.

RAID 0.

RAID 0 - это просто комбинация нескольких дисков в один блок (рис. 1). Фактически эта технология служит только для увеличения производительности дисководов, при этом вероятность выхода из строя увеличивается, потому что есть больше юнитов, которые могут выйти из строя и сделать недоступными определенную часть данных. Для реализации RAID 0 требуется минимум два диска. Лучшая производительность достигается, когда у каждого устройства есть собственный контроллер, даже если в этом нет необходимости.

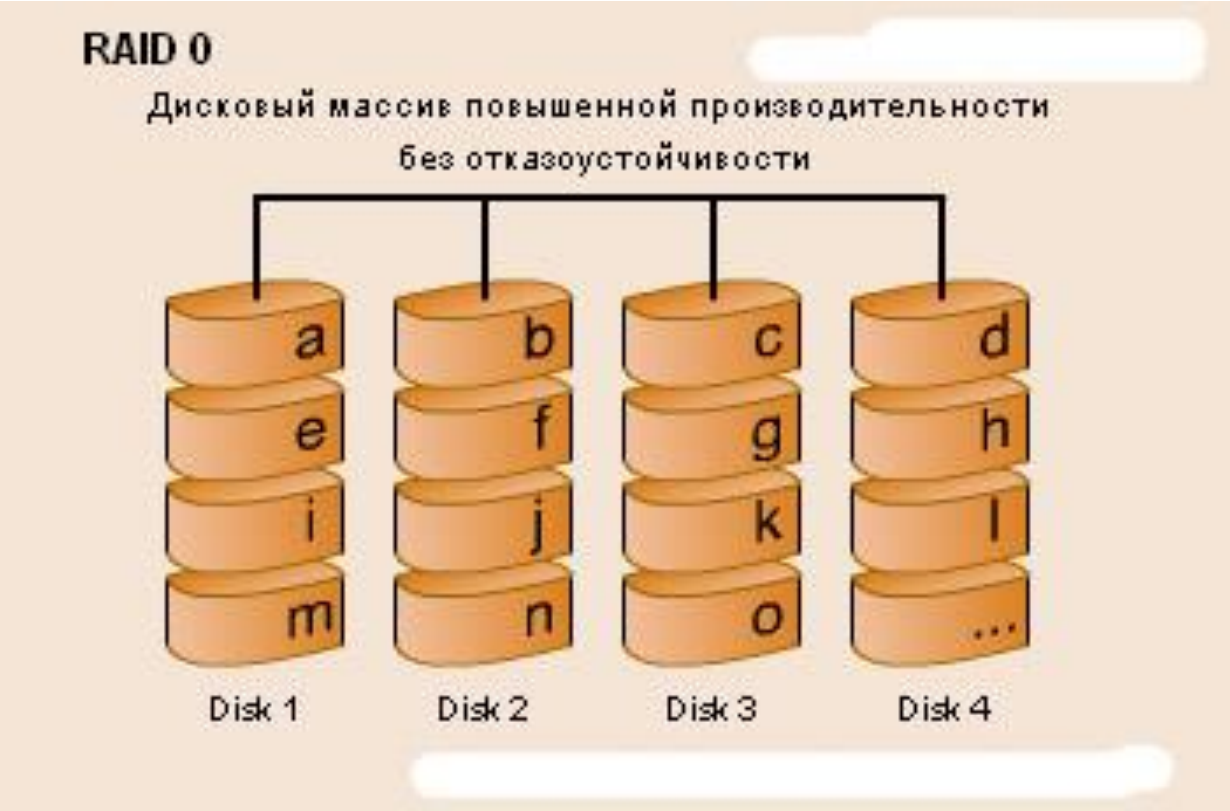

Рисунок 1 – RAID 0

RAID 1.

RAID 1, часто также называемый зеркалированием, повторяет запись с одного диска на другой диск. Это увеличивает отказоустойчивость, так как под рукой есть текущая резервная копия. Выход из строя одного из дисков, что является одним из наиболее частых отказов оборудования RAID 1, не является критичной проблемой, так как достаточно заменить поврежденный диск и диски снова синхронизируются. Скорость записи здесь слабее, потому что данные записываются в большее количество секторов одновременно. Для реализации RAID 1 требуется минимум два диска (рис. 2).

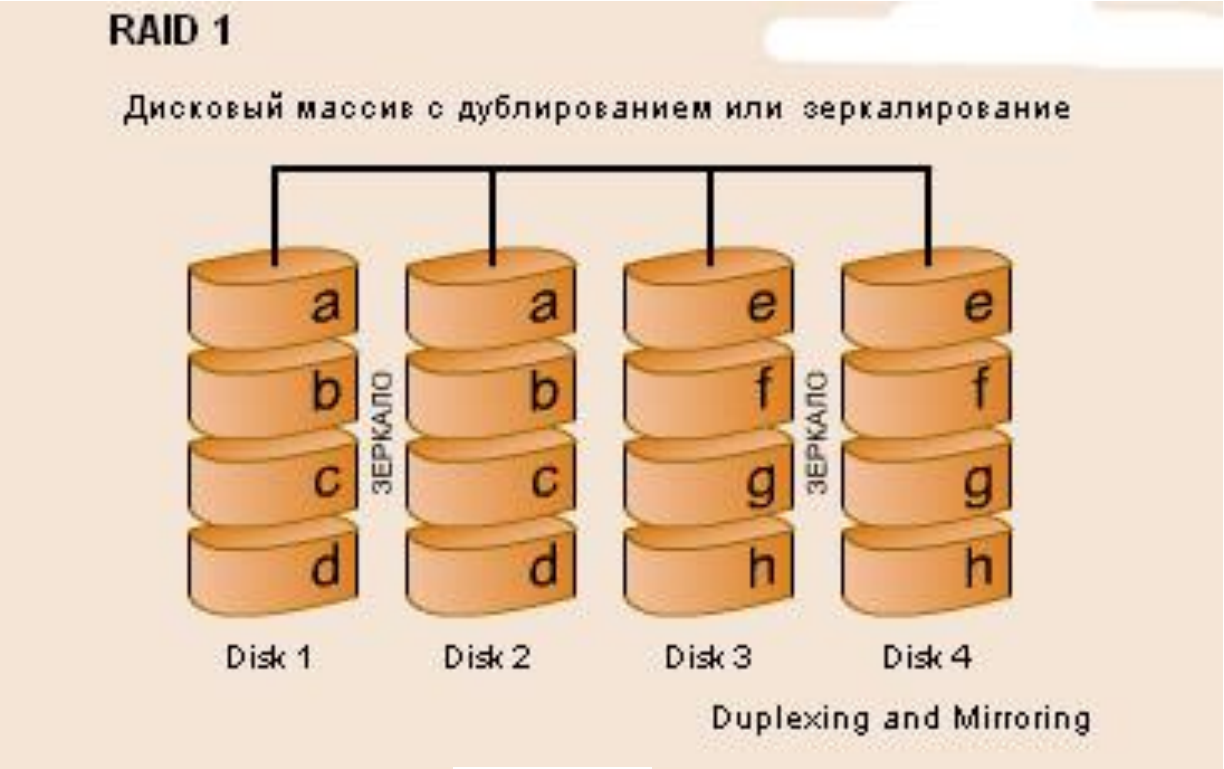

Рисунок 2 – RAID 1

RAID 2.

RAID 2 - отказоустойчивый дисковый массив с использованием кода Хемминга Hamming Code ECC (рис. 3).

RAID 2 - использует коды исправления ошибок Хемминга (Hamming Code ECC). Коды позволяют исправлять одиночные и обнаруживать двойные неисправности.

Преимущества:

– быстрая коррекция ошибок («на лету»);

– очень высокая скорость передачи данных больших объемов;

– при увеличении количества дисков, накладные расходы уменьшаются;

– достаточно простая реализация.

Недостатки:

– высокая стоимость при малом количестве дисков;

– низкая скорость обработки запросов (не подходит для систем ориентированных на обработку транзакций).

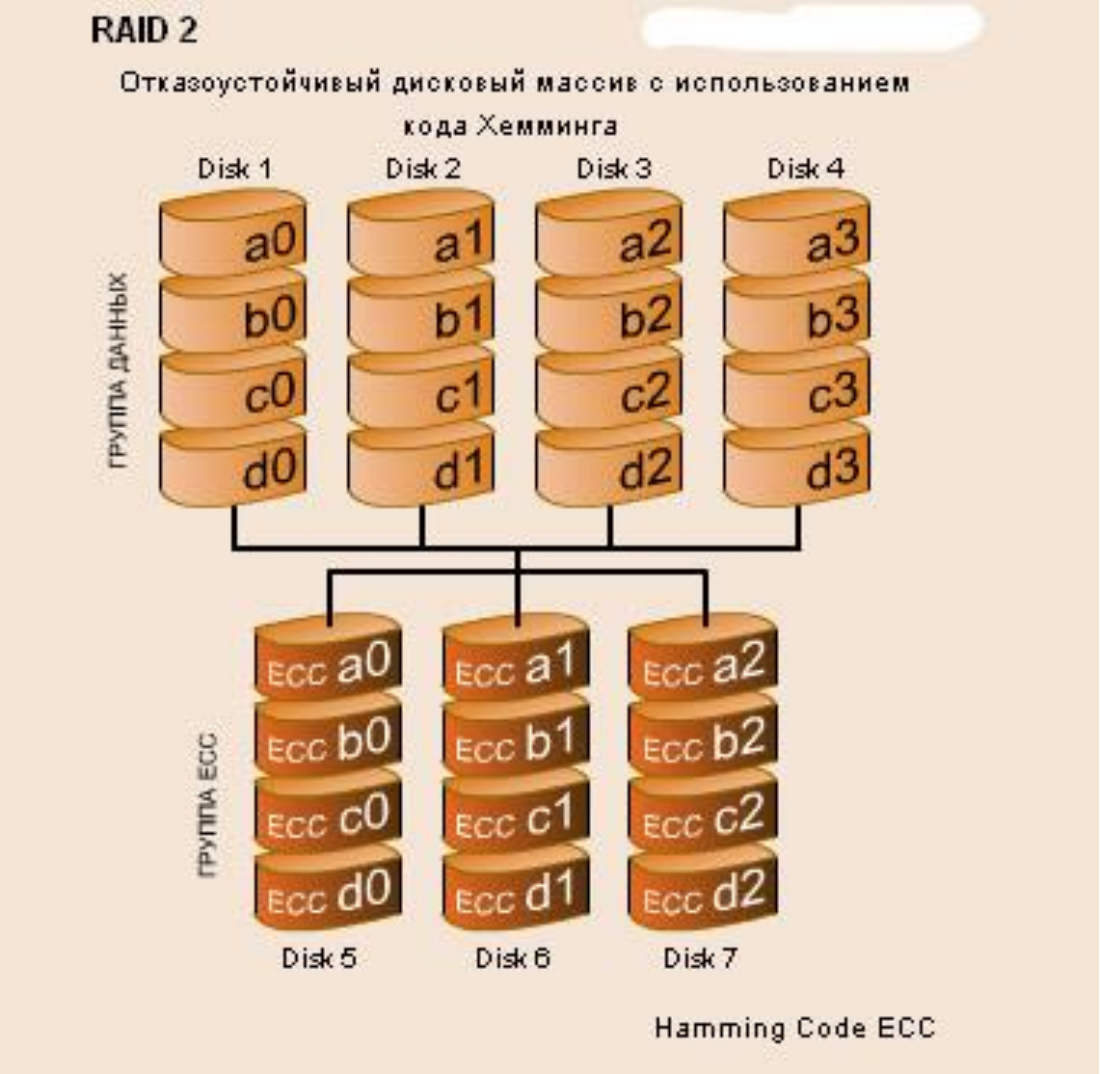

Рисунок 3 – RAID 2

RAID 3.

Отказоустойчивый массив с параллельной передачей данных и четностью Parallel Transfer Disks with Parity.

RAID 3 - данные хранятся по принципу striping на уровне байтов с контрольной суммой на одном из дисков (рис. 4). Массив не имеет проблему некоторой избыточности как в RAID 2-го уровня. Диски с контрольной суммой используемые в RAID 2, необходимы для определения ошибочного заряда. Однако большинство современных контроллеров способны определить, когда диск отказал при помощи спец сигналов или дополнительного кодирования информации, записанной на диск и используемой для исправления случайных сбоев.

Преимущества:

– очень высокая скорость передачи данных;

– отказ диска мало влияет на скорость работы массива;

– малые накладные расходы для реализации избыточности.

Недостатки:

– непростаяреализация;

– низкая производительность при большой интенсивности запросов данных небольшого объема.

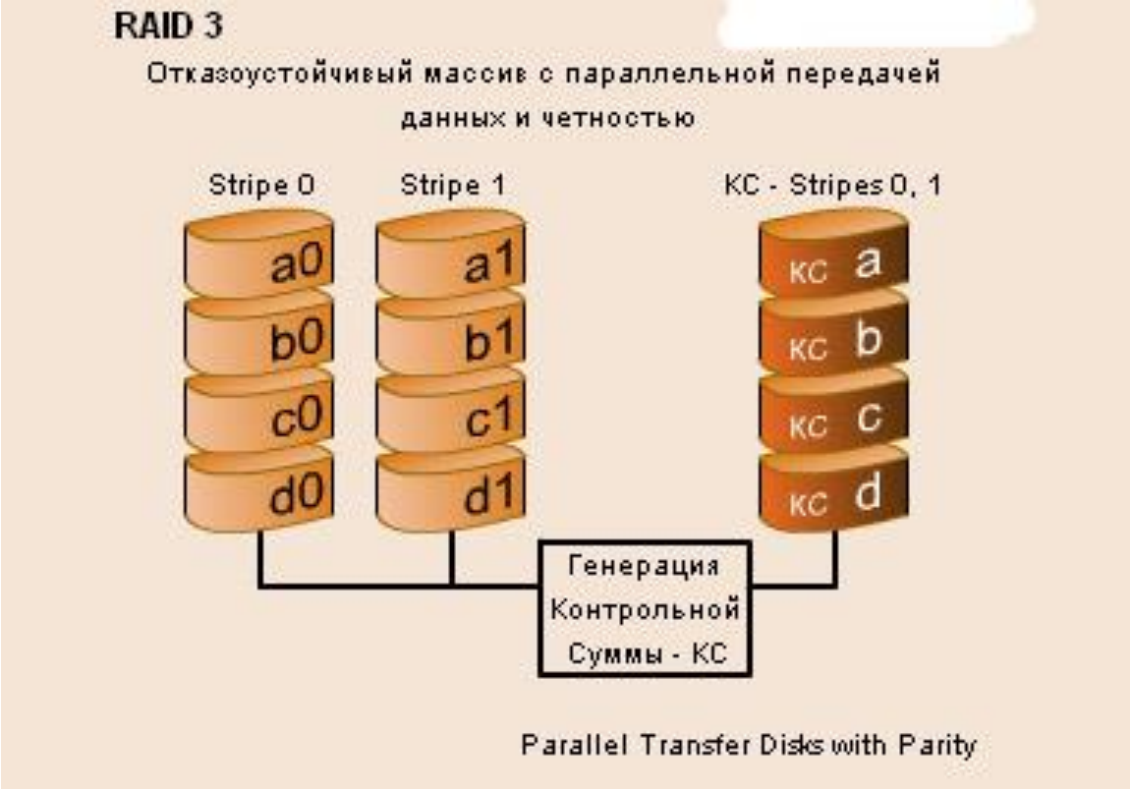

Рисунок 4 – RAID 3

RAID 4.

RAID 4 - это решение, очень похожее на RAID 3. Он отличается от RAID 3 тем, что читает на уровне блока вместо байтов. Показания менее одного блока обычно очень быстрые и обычно эта скорость увеличивается с каждой добавленной единицей. Для реализации RAID 4, как и в случае с RAID 3, требуется минимум три диска.

RAID 5.

RAID 5 похож на RAID 4. Он также позволяет разбивать на разделы и записывать данные для исправления ошибок, которые приводят к

повышению производительности и отказоустойчивости. Данные о четности хранятся на каждом блоке. Скорость записи выше, чем у RAID 4, а скорость чтения наоборот медленнее, потому что информация о четности занимает место на каждом блоке, и эти данные необходимо пропускать при чтении.

RAID 5 очень подходит для серверов баз данных. Для реализации RAID 5 требуется минимум три диска

RAID 10.

RAID 10 представляет собой комбинацию RAID 1 и RAID 0. Он предлагает все преимущества в производительности разделения и также повысить отказоустойчивость за счет зеркалирования. Минус здесь - более высокая цена, поскольку реализация этого варианта требует использования как минимум четырех дисков. RAID 10 подходит для серверов баз данных, поскольку обеспечивает высокую производительность и отказоустойчивость.

RAID 0 + 1.

Вариант RAID 0 + 1 часто путают с вариантом RAID 10. RAID 10 - это многораздельный массив. диски с зеркальными сегментами, где RAID 0 + 1 - зеркальный массив сегментированные единицы. Этот вариант подходит в ситуациях, когда больше делается упор на производительность, чем на надежность. Как и RAID 10, это решение относительно дорогое и для реализации требуется минимум четыре диска.

1.3 Программно-технические средства резервного копирования

Существующие в настоящее время программы резервного копирования избавляют пользователей и системных администраторов от необходимости «вручную» отслеживать периодичность создания и обновления резервных копий, замены носителей и т. п. Правда, перечень предоставляемых такими программами сервисных возможностей существенно зависит от категории программы.

Все программы резервного копирования можно условно разделить на три категории:

1. Системы начального уровня, включаемые в состав операционных систем. К ним можно также отнести большинство бесплатных и условно-бесплатных программ резервного копирования. Эти программы предназначены для индивидуальных пользователей и небольших организаций.

2. Системы среднего уровня; при относительно невысокой цене они обладают широкими возможностями по резервному копированию и архивации данных. Подобных систем довольно много (в частности, ARCserveIT компании Computer Associates, Backup Exec от Seagate Software и Net Worker компании Legato Systems).

3. Системы верхнего уровня предназначены для резервного копирования и архивирования в сложных гетерогенных средах. Они поддерживают разнообразные аппаратные платформы, операционные системы, базы данных и приложения корпоративного уровня, имеют средства интеграции с системами управления сетью и обеспечивают возможность резервного копирования/архивирования с использованием разнообразных типов накопителей. К подобным системам можно отнести ADSM компании ЮМ и OpenView OmniBack II от Hewlett Packard. Однако для многих организаций (не говоря уже об индивидуальных пользователях) они весьма дороги.

Одной из важных характеристик программ резервного копирования является перечень поддерживаемых типов сменных носителей. Вместе с тем, при создании резервной копии в «ручном» режиме, можно использовать любое из существующих на сегодняшний день устройств хранения данных. Перечень с краткой характеристикой приведен в таблице 1.

Таблица 1 – Устройства хранения данных, применяемые при резервном копировании

Тип устройства	Достоинства	Недостатки
Жесткий диск (HDD)	емкость, быстродействие, высокая надежность, долговечность, многократная перезапись, низкая стоимость, возможность загрузки резервной копии	Ненадежность при транспортировке, воздействие ЭМ излучений, (подключение ..)
CD-R, CD-RW	Приемлемое быстродействие и скорость, н. стоимость, надежность, долговечность	Емкость, не все виды ПК оснащены
DVD	Большая емкость, тоже что CD	Специализация, не все виды ПК оснащены
Карты памяти SD, MS, (CF), MMC	Емкость, скорость, надежность, приемлемое быстродействие и скорость, возможность использования для переноса между разнотипными устройствами	
Модули флеш памяти	То же	
Внешний жесткий Диск Mobile Rack, Стример, флоппи, ZIP, ZIV, магнитооптические	USB	

Программы для резервного копирования позволяют сохранять любую информацию на вашем персональном компьютере или сервере, а так позволяют поднять на новый уровень безопасность корпоративной сети. Вот краткий перечень документов, программ и настроек, которые можно резервировать и восстанавливать с помощью бэкап приложений:

1. Операционная система и все системные настройки, включая настройки и содержимое рабочего стола, документы, записи регистра. С помощью программы можно создавать образ жесткого диска и восстанавливать систему полностью.

2. Электронная почта, то есть учетные записи, письма, структура папок, адресные книги и любые другие элементы. Так же можно резервировать серверные системы управления корпоративной электронной почтой.

3. Базы данных и системы управления базами данных. Многие базы данных можно резервировать без остановки сервера.

4. Приложения для обмена мгновенными сообщениями и IP-телефонии.

5. Популярные приложения и их настройки. Например, графические пакеты Adobe Photoshop и Corel Draw.

Программы резервного копирования позволяют легко управлять данными, всегда поддерживая копии в актуальном состоянии. Они смогут выручить вас даже при полном отказе жесткого диска, а также при разрушительном действии вирусов или ошибочном удалении файлов. С их помощью также упрощается процесс переноса данных с одного жесткого диска на другой.

Хорошие программы резервного копирования сжимают данные для экономии места на диске и предоставляют следующие функции резервного копирования, такие как планировщик, возможность шифрования данных и дополнительную защиту бэкапа паролем.

True Image Home, разработчик Acronis, давно является лидером среди программ резервного копирования. При создании образа или резервных копий отдельных файлов этот продукт работает очень скрупулезно.

Достоинства: имеет расширенные возможности планировщика и возможны все способы резервного копирования.

Недостатки: нет поддержки записи на DVD-RW и Blue-ray-диски, а также необходима обязательная регистрация обновлений программы.

BackltUp & Burn, разработчик Nero, позволяет создавать полные резервные копии жестких дисков и разделов.

Достоинства: расширенные возможности планировщика и встроенная программа для записи дисков.

Недостатки: отсутствует возможность обновления образа путем дифференциального или инкрементного копирования.

Backup & Recoveri 10 Suite, разработчик Paragon - Software, копирование всего жесткого диска и отдельных файлов и папок делает одинаково хорошо, но имеет запутанный интерфейс.

Достоинства: расширенные возможности планировщика.

Недостатки: нет функции шифрования резервной копии и не поддерживает инкрементное резервное копирование.

Perfekt Image 12, разработчик Awanquest, создает только полный или дифференциальный образ жесткого диска.

Достоинства: расширенные возможности планировщика.

Недостатки: нет возможности просмотра файлов в созданном образе и необходимость обязательной регистрации.

R - Drive Image 4.6, разработчик Drive Image, может восстанавливать отдельные файлы, извлекая их из образа.

Достоинства: высокая степень сжатия резервных копий и расширенные возможности планировщика.

Недостатки: нет функции создания резервных копий отдельных файлов и необходимость обязательной регистрации.

NovaBACKUP 11, разработчик Novastor, имеет сложный интерфейс.

Достоинства: эффективное резервное копирование дисков и разделов.

Недостатки: нет возможности создания дифференциального и инкрементного образов, обязательная регистрация и высокая цена.

DiskImage 4.1, разработчик Oo - software, хорошо копирует образы и восстанавливает файлы из них и имеет низкую стоимость.

Достоинства: расширенные возможности планировщика.

Недостатки: нет функции создания резервных копий отдельных файлов и папок и низкая скорость работы при высокой степени сжатия.

ShadowProtekt Desktop Edition 3.5, разработчик Storagecraft, может найти отдельные файлы и восстановить их из образа.

Достоинства: высокая скорость работы.

Недостатки: необходимость обязательной регистрации, высокая стоимость и нет функции создания резервных копий отдельных файлов и папок.

Таким образом, существует множество программ резервного копирования. Кроме того, было рассмотрено 8 таких программ. Все они

имеют свои достоинства и недостатки по сравнению друг с другом. Такие программы находят широкое применение как в домашних условиях, так и в образовательных организациях. В основном эти программы распространяются за деньги, правда, некоторые компании, производящие данный продукт распространяют бесплатные версии своих программ в качестве рекламы. В этом случае такие рекламные версии имеют ограниченный срок действия и очень ограниченный функционал. Но существую программы распространяемые абсолютно бесплатно.

Среди программ для резервного копирования без труда можно выбрать ту, которая подойдет конкретному пользователю, в зависимости от решаемых им задач. Но каким именно продутом все-таки воспользоваться, должен решить сам пользователь.

При выборе продукта резервного копирования необходимо выполнить анализ информационной системы заказчика с целью определения факта необходимости использования, в силу действующего законодательства, сертифицированного продукта резервного копирования. Использование сертифицированных продуктов позволяет снизить расходы заказчика на оценку соответствия своей информационной системы в целом, так как в отношении сертифицированного продукта не требуется проводить оценочные испытания в составе информационной системы.

Выводы по главе 1

По итогам первой главы магистерской диссертации можно сделать следующие выводы.

Дано определение понятия «система резервного копирования» и выделены её основные функции. Система резервного копирования – это программный или программно-аппаратный комплекс для создания копий данных с определенной периодичностью для их последующего восстановления и выполняющий следующие функции: защиту от потери

критически важной информации; быстрое восстановление, как отдельных данных, так и всей системы полностью.

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

Описаны технологии резервного копирования и хранения резервных копий и данных.

Проанализированы программно-технические средства резервного копирования.

Все программы резервного копирования можно условно разделить на три категории:

1. Системы начального уровня, включаемые в состав операционных систем. К ним можно также отнести большинство бесплатных и условно-бесплатных программ резервного копирования. Эти программы предназначены для индивидуальных пользователей и небольших организаций.

2. Системы среднего уровня; при относительно невысокой цене они обладают широкими возможностями по резервному копированию и архивации данных.

3. Системы верхнего уровня предназначены для резервного копирования и архивирования в сложных гетерогенных средах. Они поддерживают разнообразные аппаратные платформы, операционные системы, базы данных и приложения корпоративного уровня, имеют средства интеграции с системами управления сетью и обеспечивают возможность резервного копирования/архивирования с использованием разнообразных типов накопителей.

При выборе продукта резервного копирования необходимо выполнить анализ информационной системы заказчика с целью определения факта необходимости использования, в силу действующего законодательства, сертифицированного продукта резервного копирования. Использование

сертифицированных продуктов позволяет снизить расходы заказчика на оценку соответствия своей информационной системы в целом, так как в отношении сертифицированного продукта не требуется проводить оценочные испытания в составе информационной системы.

ГЛАВА 2 АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГБПОУ «ЧЕЛЯБИНСКИЙ ТЕХНИКУМ ПРОМЫШЛЕННОСТИ И ГОРОДСКОГО ХОЗЯЙСТВА ИМЕНИ Я.П. ОСАДЧЕГО»

2.1 Общие сведения о ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего»

Базой исследования является Государственное бюджетное профессиональное образовательное учреждение «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего», располагающегося по адресу: 454129, Российская Федерация, Уральский федеральный округ, город Челябинск, ул. Масленникова, 21.

Структура управления техникума относится к линейно-функциональной, то есть к такой структуре, где связи и отношения субъектов характеризуются одновременно и субординацией, и координацией. Непосредственное управление учреждением осуществляет директор.

Директор — Худолей Елена Сергеевна.

Структура управления ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего» представлена на рисунке 5.

Рисунок 5 – Структура управления ГБПОУ «ЧТПиГХ имени Я.П. Осадчего»

ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего» представляет собой комплекс из нескольких зданий различного назначения: два учебных корпуса, учебно-производственные мастерские, общежитие для студентов.

В ЧТПиГХ имеются следующие лаборатории и мастерские**:** лаборатория технического обслуживания и ремонта автомобилей и двигателей внутреннего сгорания, электрооборудования автомобилей; лаборатория – учебный кулинарный цех, учебный кондитерский цех, технологического оборудования кулинарного и кондитерского производства; лаборатория по профессии «Мастер по обработке цифровой информации»; лаборатория Электротехники с основами электроники; лаборатория технических измерений, и инженерной графики; лаборатория товароведения продовольственных товаров; слесарная мастерская; сварочная № 1, № 2; электромонтажная мастерская.

Учебные корпуса техникума (ул. Масленникова, 21 и Энергетиков, 2) оснащены столовыми. Обе столовые рассчитаны на 120 мест. На сегодняшний день техникум располагает тремя общежитиями, рассчитанными на 536 человек.

Профессии и специальности ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего».

В настоящее время в техникуме работает 118 человек, в том числе 56 педагогических работников. Контингент обучающихся составляет 882 человека, обучающихся по десяти программам, в т.ч. две из числа наиболее востребованных и перспективных на современном рынке труда ТОП-50.

Номенклатура программ базового образования согласно лицензии представлена в таблице 2.

Таблица 2 – Программы подготовки квалифицированных рабочих кадров и специалистов среднего звена

КОД специальности	Наименование специальности, профессии
46.01.03	Делопроизводитель
19.01.17	Повар. Кондитер
15.01.05	Сварщик (ручной и частично механизированной сварки (наплавки)
19.01.03	Мастер по обработке цифровой информации
19.01.03	Монтажник сантехнических, вентиляционных систем и оборудования
18.02.07	Монтаж и эксплуатация внутренних сантехнических устройств, кондиционирования воздуха и вентиляции
23.02.03	Техническое обслуживание и ремонт автомобильного транспорта
19.02.10	Технология продукции общественного питания
08.02.08	Монтаж и эксплуатация оборудования и систем газоснабжения

На базе техникума действует ресурсный центр по подготовке рабочим профессиям. Перечень программ дополнительного образования, по которым идет обучение в ресурсном центре, представлен в таблице 3.

Таблица 3 – Программы дополнительного образования

№ п/п	Код	Наименование	Уровень	Срок обучения	Квалификация
1	**2**	**3**	**4**	**5**	**6**
1	16199	Оператор ЭВМ	Профессиональная подготовка	5 месяцев	2 разряд
			Переподготовка	2,5 месяцев	2 разряд
			Повышение квалификации	80 часов	3,4 разряды
2	18560	Слесарь-сантехник	Профессиональная подготовка	4 месяцев	2 разряд
			Переподготовка	2 месяцев	2 разряд
			Повышение квалификации	80 часов	3-6 разряды
3	19149	Токарь	Профессиональная подготовка	5 месяцев	2 разряд
			Переподготовка	2,5 месяцев	2 разряд
			Повышение квалификации	80 часов	3-6 разряды

Продолжение таблицы 3

4	16675	Повар	Профессиональная подготовка	5 месяцев	2 разряд
			Переподготовка	2,5 месяцев	2 разряд
			Повышение квалификации	80 часов	3-6 разряды
5	12901	Кондитер	Профессиональная подготовка	5 месяцев	2 разряд
			Переподготовка	2,5 месяцев	2 разряд
			Повышение квалификации	80 часов	3-6 разряды
6	18554	Слесарь по эксплуатации и ремонту газового оборудования	Профессиональная подготовка	4 месяцев	2 разряд
			Переподготовка	2 месяцев	2 разряд
			Повышение квалификации	80 часов	3-5 разряды
7	19756	Электрогазосварщик	Профессиональная подготовка	6 месяцев	2 разряд
			Переподготовка	3 месяцев	2 разряд
			Повышение квалификации	80 часов	3-6 разряды
8	18511	Электромонтёр по ремонту и обслуживанию электрооборудования	Профессиональная подготовка	5 месяцев	2,3 разряды
			Переподготовка	2,5 месяцев	2,3 разряды
			Повышение квалификации	80 часов	3-6 разряды
9	18559	Слесарь-ремонтник	Профессиональная подготовка	5 месяцев	2 разряд
			Переподготовка	2,5 месяцев	2 разряд
			Повышение квалификации	80 часов	3-7 разряды
10	11176	Бармен	Переподготовка	160 часов	4 разряд
			Повышение квалификации	80 часов	5 разряд
11	16399	Официант	Профессиональная подготовка	4 месяцев	3 разряд
			Переподготовка	2 месяцев	3 разряд
			Повышение квалификации	80 часов	4,5 разряды

Продолжение таблицы 3

12	18466	Слесарь механосборочных работ	Профессиональная подготовка	5 месяцев	2 разряд
13	18809	Станочник широкого профиля	Профессиональная подготовка	5 месяцев	2,3 разряды
			Переподготовка	2,5 месяцев	2,3 разряды
			Повышение квалификации	80 часов	разряд
			Переподготовка	2 месяцев	2 разряд
14	19479	Фрезеровщик	Профессиональная подготовка	5 месяцев	2 разряд
			Переподготовка	2 месяцев	2 разряд

В настоящее время подготовка специалистов осуществляется по очной форме обучения:

Подготовка квалифицированных рабочих кадров:

– 46.01.03 Делопроизводитель;

– 19.01.17 Повар. Кондитер;

– 15.01.05 Сварщик (ручной и частично механизированной сварки (наплавки); - 19.01.03 Мастер по обработке цифровой информации;

– 19.01.03 Монтажник сантехнических, вентиляционных систем и оборудования.

Подготовка специалистов среднего звена:

– 18.02.07 Монтаж и эксплуатация внутренних сантехнических устройств, кондиционирования воздуха и вентиляции;

– 23.02.03 Техническое обслуживание и ремонт автомобильного транспорта;

– 19.02.10 Технология продукции общественного питания;

– 18.02.08 Монтаж и эксплуатация оборудования и систем газоснабжения.

В образовательном процессе ЧТПиГХ им. Я.П. Осадчего используются такие средства обучения и воспитания, как:

1. Печатные (учебники и учебные пособия, книги для чтения, хрестоматии, рабочие тетради, атласы, раздаточный материал, энциклопедии, словари и др.).

2. Электронные образовательные ресурсы (образовательные мультимедийные учебники, сетевые образовательные ресурсы, мультимедийные универсальные энциклопедии и т.п.).

3. Аудиовизуальные (презентации, слайд – фильмы, видеофильмы образовательные, учебные кинофильмы, учебные фильмы на цифровых носителях и др.).

4. Наглядные плоскостные (плакаты, карты настенные, иллюстрации настенные, магнитные доски и др.).

5. Демонстрационные (муляжи, макеты, стенды, модели в разрезе, модели демонстрационные и др.)

В техникуме имеются следующие средства обучения и воспитания, достаточные для организации образовательного процесса в соответствии с обязательными требованиями.

В техникуме проводится систематическая работа по расширению и обновлению компьютерного парка, разработке и внедрению программно-информационного обеспечения учебного процесса.

В техникуме оборудовано 4 компьютерных аудитории. Программное обеспечение, используемое в учебном процессе, основано как на требованиях ГОС СПО, так и требованиях высокотехнологичных производств и компьютеризации управленческой деятельности базового предприятия и организаций города, на которых проходят производственную практику обучающиеся и включает:

- операционную систему Windows;
- операционную систему MS DOS;
- операционную оболочку NC;
- операционную оболочку FAR;
- антивирусные программы Dr.Web, Sp|DerGuard;

– архиваторы MS RAR, WIN RAR;

– программное обеспечение Microsoft Word;

– электронные таблицы Excel;

– процессор презентаций Power Point.

В техникуме имеются мультимедийные проекторы, телевизоры. В учебном процессе используется интерактивные доски, переносные мультимедийные проекторы, обеспечение бесплатным выходом в Интернет.

Оснащенность учебных помещений вычислительной техникой - 82%.

Локальная вычислительная сеть (ЛВС): имеется.

Характеристики:

1. Физическая среда: кабель UTP5, Ethernet.
2. Транспортный уровень передачи информации - протокол TCP/IP.
3. Логическая организация ЛВС - рабочие группы MS Windows.
4. Средство обмена файлами и сетевой печати - протокол SMB.
5. Подключение к интернет – есть.
6. Эффективность использования сети - 55-60%.

Количество аудиторий, обеспеченных АРМ (компьютер, проектор, выход в интернет) – 25 шт.

Количество разработанных электронных образовательных ресурсов – 28 шт.

Техникум располагает также фондом информационных ресурсов в количестве 180 экз. и подписан на виртуальный абонемент ЧОУНБ (2 доступа), всероссийский методический интернет-портал «Росметод», ЭБС IPRbooks.

Таким образом, информационно-методические материалы по реализуемым образовательным программам среднего профессионального образования соответствуют требованиям федеральных государственных образовательных стандартов среднего профессионального образования по профессиям и специальностям.

2.2 Анализ информационных систем в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего»: структура, функционирование, средства защиты

В ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» действует политика обработки и защиты персональных данных.

При обработке персональных данных в Техникуме соблюдаются конституционные права и свободы человека и гражданина на неприкосновенность частной жизни, личную и семейную тайну.

Персональные данные субъектов в Техникуме обрабатываются как на бумажных носителях, так и в электронном виде - в компьютерных программах и электронных базах данных (в ИСПДн) с передачей по локальной компьютерной сети и по сети Internet.

Безопасность персональных данных достигается путем обеспечения их конфиденциальности, целостности и доступности.

В Техникуме функционирует комплексная система защиты персональных данных, которая включает:

1. Организационные мероприятия

- действующие организационно-распорядительные документы по защите ПДн, регламентирующие порядок обработки ПДн и ответственность должностных лиц;
- осуществление внутреннего периодического контроля;
- учет машинных носителей персональных данных;
- физическая охрана зданий и помещений;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- обучение сотрудников вопросам защиты ПДн.

2. Технические меры защиты

- модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- техническое задание для ИСПДн, содержащее требования к системе защиты;
- подсистема резервного копирования информации;
- подсистема парольной защиты;
- подсистема антивирусной защиты;
- подсистема криптографической защиты;
- средства защиты информации от несанкционированного доступа;
- средства межсетевого экранирования;
- сейфы и запирающиеся шкафы для хранения носителей персональных данных;
- пожарная и охранная сигнализация.

Допуск к персональным данным субъекта имеют только те сотрудники Техникума, которым персональные данные необходимы в связи с исполнением ими своих служебных (трудовых) обязанностей.

Каждый сотрудник имеет доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения служебных (трудовых) обязанностей.

В состав информационных систем персональных данных ГБПОУ «Челябинский техникум промышленности и городского хозяйства им. Я.П. Осадчего» входит: 1С:Колледж, 1С:Зарплата и кадры 8.2, 1С Предприятие 8.3, Контур-Экстерн, официальный сайт учреждения http://chtpgh.ru/.

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно- вычислительные комплекты и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации, применяемые в информационных системах.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение,

блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Средства защиты информации, применяемые в информационных системах, в обязательном порядке проходят процедуру оценки соответствия в установленном законодательством РФ порядке.

Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер, а также применения технических и (или) программных средств.

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Безопасность персональных данных при их обработке в информационной системе персональных данных обеспечивает специалист, ответственный за организацию обработки информационных систем персональных данных.

При обработке персональных данных в информационной системе должно быть обеспечено:

– проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

– своевременное обнаружение фактов несанкционированного доступа к персональным данным;

– недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

– возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– постоянный контроль над обеспечением уровня защищенности персональных данных.

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают:

– определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

– проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

– установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

– обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

– учет лиц, допущенных к работе с персональными данными в информационной системе;

– контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документации;

– разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

– описание системы защиты персональных данных.

Иные требования по обеспечению безопасности информации и средств защиты информации в ГБПОУ «Челябинский техникум промышленности и городского хозяйства им. Я.П. Осадчего» выполняются в соответствии с требованиями федеральных органов исполнительной власти и органов исполнительной власти Челябинской области.

В ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» эксплуатируются следующие информационные системы персональных данных (далее - ИСПДн) с использованием средств криптографической защиты информации (далее - СКЗИ, криптосредства):

1. ИСПДн «Бухгалтерия и кадры» в составе следующих подсистем:

- «Система дистанционного банковского обслуживания «Клиент-Банк», АО «Уральский банк реконструкции и развития» (далее - СДБО «Клиент-Банк УБРиР»);

- «Информационная система электронного документооборота «Интернет отчетность - Контур-Экстерн» (далее - ИС ЭДО «Контур-Экстерн»).

Для ИСПДн «Бухгалтерия и кадры» разработана ООО «СИБ Альпикс» и утверждена директором ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» «Модель угроз безопасности персональных данных ...» № СИБА.МУ.59 от 09.06.2016.

2. ИСПДн «ФИС ГИА и Приема».

Для ИСПДн «ФИС ГИА и Приема» разработана ООО «СИБ Альпикс» и утверждена директором ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» «Модель угроз безопасности персональных данных ...» № СИБА.МУ.61 от 09.06.2016.

Документы обучающихся вносятся в 1С:Колледж, Контур-Экстерн.

Согласно актам определения уровня защищенности ИСПДн «Бухгалтерия и кадры» и «ФИС ГИА и Приема», №№ б/н от 28.06.2016, комиссия установила:

- ИСПДн являются информационными системами, обрабатывающими иные категории персональных данных (менее чем 100 000 субъектов персональных данных);

- для ИСПДн актуальны угрозы 3-го типа;

- 4-ый уровень защищенности персональных данных при их обработке в ИСПДн.

Для защиты информации в ИСПДн ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» используются следующие СКЗИ:

- ПАК «ViPNet Terminal 3.0», сертификат соответствия ФСБ России имеется;

- ПАК «КриптоПро CSP» версии 3.6, сертификат соответствия ФСБ России имеется.

Схема информационных потоков в ИСПДн представлена в таблице 4.

Таблица 4 – Схема информационных потоков в ИСПДн

Субъекты ПДн	Цели обработки	Категории ПДн	Правовые основания обработки
Сотрудники Техникума	Реализация трудовых отношений, начисление заработной платы, передача информации в налоговые органы. Пенсионный Фонд	– фото; – фамилия, имя, отчество; – паспортные данные; – дата и место рождения; – сведения о месте регистрации, проживания; – контактная информация (телефон домашний, телефон мобильный, e-mail); – сведения об образовании; – семейное положение (состав семьи, копия св-ва о браке, копия св-в о рождении детей);	Гражданский кодекс РФ от 30.11.1994 № 51-ФЗ; Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ; Налоговый Кодекс РФ часть первая от 31 июля 1998 г. № 146-ФЗ и часть вторая от 5 августа 2000 г. № 117-ФЗ; Согласие на обработку персональных данных

Продолжение таблицы 4

Кандидаты на вакантную должность	Принятие решения о трудоустройстве, формирование кадрового резерва	– фамилия, имя, отчество; – дата; – контактная информация (телефон мобильный, e-mail); – сведения об образовании; – опыт работы.	Согласие на обработку персональных данных
Практиканты	Прохождение практики (учебной, производственной)	– фамилия, имя. отчество; – контактная информация (телефон мобильный); – сведения об месте учебы.	Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ; Согласие на обработку персональных данных

В случаях, когда на виртуальных машинах обрабатывается информация ограниченного доступа, не относящаяся к государственной тайне, в обязательном порядке должны выполняться требования законодательства РФ к используемому программному обеспечению, выполняющему резервное копирование такой информации: такое программное обеспечение должно пройти процедуру оценки соответствия, как правило, в форме сертификации по требованиям ФСТЭК.

Для обеспечения физической целостности данных, во избежание умышленного или неумышленного уничтожения, или искажения защищаемой информации и конфигураций информационных систем организуется резервное копирование баз данных, конфигураций, файлов настроек, конфигурационных файлов. Порядок резервного копирования, дублирования, хранения архивов и восстановления информации определен Порядком резервирования и восстановления информации. Для обеспечения гарантированного восстановления особо важной информации, которая может быть утеряна вследствие аппаратных сбоев, воздействия вирусов-шифровальщиков производится ежедневное резервное копирование содержимого дисков. Данный процесс запускается по служебной записке сотрудника на имя директора ГБПОУ «ЧТПиГХ им. Я.П. Осадчего».

Ответственными за организацию резервного копирования, хранения копий и восстановления информации являются администраторы ИС, ответственные сотрудники ГБПОУ «ЧТПиГХ им. Я.П. Осадчего».

Выводы по главе 2

Во второй главе магистерской диссертации проведен анализ информационных систем ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего».

В ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» действует политика обработки и защиты персональных данных.

В ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» эксплуатируются следующие информационные системы персональных данных (далее - ИСПДн) с использованием средств криптографической защиты информации (далее - СКЗИ, криптосредства):

1. ИСПДн «Бухгалтерия и кадры» в составе следующих подсистем:

- «Система дистанционного банковского обслуживания «Клиент-Банк», АО «Уральский банк реконструкции и развития» (далее - СДБО «Клиент-Банк УБРиР»);

- «Информационная система электронного документооборота «Интернет отчетность - Контур-Экстерн» (далее - ИС ЭДО «Контур-Экстерн»).

Для ИСПДн «Бухгалтерия и кадры» разработана ООО «СИБ Альпикс» и утверждена директором ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» «Модель угроз безопасности персональных данных ...» № СИБА.МУ.59 от 09.06.2016.

3. ИСПДн «ФИС ГИА и Приема».

Для ИСПДн «ФИС ГИА и Приема» разработана ООО «СИБ Альпикс» и утверждена директором ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» «Модель угроз безопасности персональных данных ...» № СИБА.МУ.61 от 09.06.2016.

Документы обучающихся вносятся в 1С:Колледж, Контур-Экстерн.

Таким образом, система защиты персональных данных при их обработке в информационных системах персональных данных в техникуме создана, но необходимо усовершенствовать систему резервного копирования при обеспечении защиты информации.

ГЛАВА 3 РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ОРГАНИЗАЦИИ СИСТЕМЫ РЕЗЕРВНОГО КОПИРОВАНИЯ В ГБПОУ «ЧЕЛЯБИНСКИЙ ТЕХНИКУМ ПРОМЫШЛЕННОСТИ И ГОРОДСКОГО ХОЗЯЙСТВА ИМЕНИ Я.П. ОСАДЧЕГО»

3.1 Рекомендации по организации системы резервного копирования при обеспечении защиты информации в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего»

Одной из важных задач при эксплуатации информационных систем является обеспечение целостности и сохранности данных, ведь даже в самой надежной из них существует риск потери информации, жизненно важной для предприятия. Поэтому необходимо иметь механизм для быстрого восстановления потерянных данных. Это может быть обеспечено путем построения развитой системы резервного копирования, периодически создающей копии информации с целью ее последующего восстановления в случае частичного или полного разрушения. Кроме того, такая система может собирать и обслуживать архив корпоративных данных.

В большинстве случаев требуется, чтобы система резервного копирования функционировала в вычислительной сети, причем умела манипулировать данными и устройствами независимо от их расположения в этой сети. Такая полноценная сетевая система должна обеспечивать восстановление данных, распределенных по всем узлам вычислительной сети.

Требования к резервному копированию информации, обрабатываемой в государственных информационных системах, информационных системах персональных данных содержатся в перечне законов РФ, подзаконных актов, постановлений правительства, нормативных актов федеральных органов исполнительной власти представлены в таблице 5.

Таблица 5 – Законодательные требования к информационной безопасности процесса резервного копирования информации

Законы	
Закон «Об информации, информационных технологиях и о защите информации»	Статья 16. Защита информации Обладатель информации, оператор информационной системы в случаях, установленных законодательством, обязаны обеспечить: … 5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие НСД
	Статья 13.12. Нарушение правил защиты информации 6. Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами РФ (с 14.12.2013)
Закон 152-ФЗ «О персональных данных»	Статья 19. Меры по обеспечению безопасности персональных данных при их обработке 1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от … неправомерных действий в отношении персональных данных
	Статья 19. Меры по обеспечению безопасности персональных данных при их обработке 2. Обеспечение безопасности персональных данных достигается, в частности: … 7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Продолжение таблицы 5

Приказы ФСТЭК и ФСБ	
Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн»	– организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от класса (уровня) защищенности, угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать: доступность информации… – меры по защите среды виртуализации должны исключать НСД к обрабатываемым данным и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к … системе хранения данных, сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям. – меры ЗСВ.8, ОДТ.4 и ОДТ.5.
Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»	
Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды	
Приказ ФСБ № 416, ФСТЭК № 489 от 31.08.2010	11. В информационных системах общего пользования должны быть обеспечены: …; возможность оперативного восстановления информации, модифицированной или уничтоженной вследствие неправомерных действий… 15. ... Подсистема информационной безопасности должна обеспечивать восстановление информации в ИСОП, модифицированной или уничтоженной вследствие неправомерных действий в отношении такой информации. Время восстановления процесса предоставления информации пользователям не должно превышать 8 часов

Согласно законодательным актам были разработаны рекомендации по организации системы резервного копирования при обеспечении защиты информации.

Рекомендации состоят из 3 этапов.

Этап 1. Разработка регламента копирования персональных данных субъектов ГБПОУ «ЧТПиГХ им. Я.П. Осадчего».

Регламент о порядке резервного копирования персональных данных субъектов Государственное бюджетное профессиональное образовательное учреждение «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего» (далее – Регламент) разработан в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом Российской Федерации от 27.06.2006 г. N 152-ФЗ «О персональных данных», Доктриной информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации от 09.09.2000 г. № Пр-1895.

Настоящий Регламент определяет порядок резервирования данных для последующего восстановления работоспособности автоматизированных систем ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего» при полной или частичной потере информации, вызванной сбоями или отказами аппаратного, или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.); восстановления информации в случае возникновения такой необходимости; упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации, обрабатываемой в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего» (далее – Техникум»).

В настоящем документе регламентируются действия при выполнении следующих мероприятий:

– резервное копирование;

– контроль резервного копирования;

– хранение резервных копий;

– полное или частичное восстановление данных и приложений.

Резервному копированию подлежит информация следующих основных категорий:

– персональная информация пользователей (личные каталоги на файловых серверах);

– групповая информация пользователей (общие каталоги отделов);

– информация, необходимая для восстановления серверов и систем управления базами данных (далее – СУБД);

– персональные профили пользователей сети;

– информация автоматизированных систем, в т.ч. баз данных;

– справочно-информационная информация систем общего использования;

– рабочие копии установочных компонент программного обеспечения рабочих станций;

– регистрационная информация системы информационной безопасности автоматизированных систем.

Порядок резервного копирования.

Ответственным за организацию резервного копирования персональных данных является администратор информационной безопасности.

Резервное копирование автоматизированных систем производится на основании следующих данных:

– состав и объем копируемых данных, периодичность проведения резервного копирования;

– максимальный срок хранения резервных копий - 1 месяц;

– хранение 3-х следующих архивов;

– архив на 1-е число текущего месяца;

– архив среда-четверг, либо пятница-суббота текущей недели;

– архив сделанный в текущую ночь.

Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации.

О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается директору Техникума в течение рабочего дня после обнаружения указанного события.

Контроль результатов резервного копирования.

Контроль результатов всех процедур резервного копирования осуществляется администратором информационной безопасности в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур.

В случае обнаружения ошибки в резервном копировании, администратор информационно безопасности устраняет ошибку и повторяет процедуру.

На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для ее хранения.

Ротация носителей резервной копии.

Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации автоматизированных систем в случае отказа любого из устройств резервного копирования.

В случае необходимости замены испорченных носителей информации новыми, администратор информационной безопасности заблаговременно за

10 рабочих дней согласовывает с поставщиком спецификации новых носителей информации.

Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются администратором информационной безопасности по графику или по запросу других сотрудников.

В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

Конфиденциальная информация с носителей, которые перестают использоваться в системе резервного копирования, должна стираться с использованием программного обеспечения PGP.

Восстановление информации из резервных копий.

В случае необходимости восстановление данных из резервных копий производится на основании Заявки сотрудника Техникума, согласованной с Ответственным за организацию обработки персональных данных.

Процедура восстановления информации из резервной копии осуществляется в соответствии с методикой восстановления информации.

После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

Этап 2. Выбор технологий.

Устройство NAS.

В качестве устройства NAS было выбрано для техникума: сетевое хранилище QNAP D2 (рис. 6).

Код: 470545; отсеков для дисков: 2; интерфейс: SATA III; форм-фактор: 2.5"/3.5"; LAN: 2 x 10/100/1000 Мбит/с; портов USB3.0: 3; RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, горячая замена дисков; совместимо с IP-камерами.

Это внешний бокс для 2 жестких дисков 3,5 дюйма SATA II/III, поддерживающих RAID 0 и RAID 1. Коробка поставляется без установленного жесткого диска и в настоящее время доступен через интернет-магазин https://www.dns-shop.ru/ по цене 17199 руб.

Рисунок 6 – Сетевое хранилище QNAP D2

Преимущество Накопителя NAS заключается в том, что можно будет использовать диски с сервера, который компания планирует отключать после развертывание архивной копии через FTP.

FTP сервер.

FTP-сервер с емкостью будет предоставлен https://lancloud.ru, поэтому покупать не нужно. В этом случае нет оборудования. Организация будет платить только ежемесячную плату за работу FTP-сервера. Эти ежемесячные платежи должны составлять около 1000 рублей в месяц. в зависимости объёма резервных копий.

Программа для выполнения дифференциального резервного копирования по FTP.

Для выполнения резервного копирования по FTP была выбрана утилита Duplicity. Эта утилита находится в свободном доступе.

В результате необходимо будет только приобрести NAS-бокс и заплатить ежемесячную плату за работу FTP-сервера.

Этап 3. Усовершенствование программно-технических средств резервного копирования.

На рынке программных продуктов для организации резервного копирования уже появились признанные лидеры. Наиболее функционально полным и развитым продуктом является, по нашему мнению, система Защита Данных (Cyber Backup**)** и Acronis Защита Данных Облачная (Cyber Backup Cloud) компании Acronis.

*Acronis Защита Данных (Cyber Backup)***.** Единое решение для защиты данных любых поддерживаемых систем: физических серверов, виртуальных машин, приложений, рабочих станций.

*Acronis Защита Данных Облачная (Cyber Backup Cloud)***.** Для защиты виртуальных, физических и облачных сред, позволяет быстро получить дополнительный доход без первоначальных инвестиций и предлагает бизнес-модель с оплатой по мере использования.

Компоненты Acronis Backup:

1. Компоненты для управляемой машины (агенты). Приложения, которые выполняют резервное копирование данных, их восстановление и другие операции на машинах под управлением Acronis Backup. Агентам необходима лицензия для выполнения операций на каждой управляемой машине.

2. Компоненты для централизованного управления. Эти компоненты в составе Acronis Backup Advanced обеспечивают возможности централизованного управления. Использование этих компонентов не лицензируется.

3. Консоль. Консоль обеспечивает графический интерфейс пользователя для работы с другими компонентами Acronis Backup. Использование консоли не лицензируется.

4. Мастер создания загрузочных носителей. Мастер создания загрузочных носителей создает загрузочные носители, которые позволяют использовать агенты и другие утилиты в среде аварийного восстановления. Лицензия для мастера создания загрузочных носителей не требуется при установке мастера вместе с агентом. Для использования мастера создания загрузочных носителей на машине без агента необходим лицензионный ключ или хотя бы одна лицензия на сервере лицензий. Лицензия может быть свободной или назначенной.

Технические характеристики, функционал.

В таблице 6 представлена информация о поддержке в Acronis Backup различных платформ виртуализации.

Таблица 6 – Поддержка в Acronis Backup различных платформ виртуализации (источник: acronis.com)

Платформа	Резервное копирование на уровне гипервизора	Резервное копирование изнутри гостевой ОС
VMware		
Версии VMware vSphere: 4.0, 4.1, 5.0, 5.1, 5.5 и 6.0 **Выпуски VMware vSphere:** VMware vSphere Essentials VMware vSphere Essentials Plus VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	+	+
VMware vSphere Hypervisor (бесплатная низкоуровневая оболочка ESXi)**		+
VMware Server (VMware Virtual Server) VMware Workstation VMware ACE VMware Player		+

Продолжение таблицы 6

Microsoft		
Windows Server 2008 (x64) с Hyper-V Windows Server 2008 R2 с Hyper-V Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 с Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1 (x64) с Hyper-V Windows 10 с Hyper-V Windows Server 2016 с Hyper-V Microsoft Hyper-V Server 2016	+	+
Microsoft Virtual PC 2004 и 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Citrix		
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2 и 6.5		Только полностью виртуализированные (известные также как HVM) гостевые системы
Red Hat и Linux		
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5 и 3.6		+
Виртуальные машины на основе ядра (KVM)		+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0 и 3.3		+
Oracle VM VirtualBox 4.x		+

* Стандартный выпуск не поддерживает «горячее» подключение, поэтому резервное копирование может выполняться медленнее.

** Резервное копирование на уровне гипервизора не поддерживается для vSphere Hypervisor, так как в этом продукте доступ к удаленному интерфейсу командной строки (RCLI) возможен исключительно в режиме «только для чтения». Агент работает в течение пробного периода vSphere Hypervisor до введения серийного ключа. После введения серийного ключа агент перестает работать.

Сценарии применения.

Локальное развертывание. Установка всех компонентов решения в локальной сети, доступно по бессрочной лицензии (рис. 7).

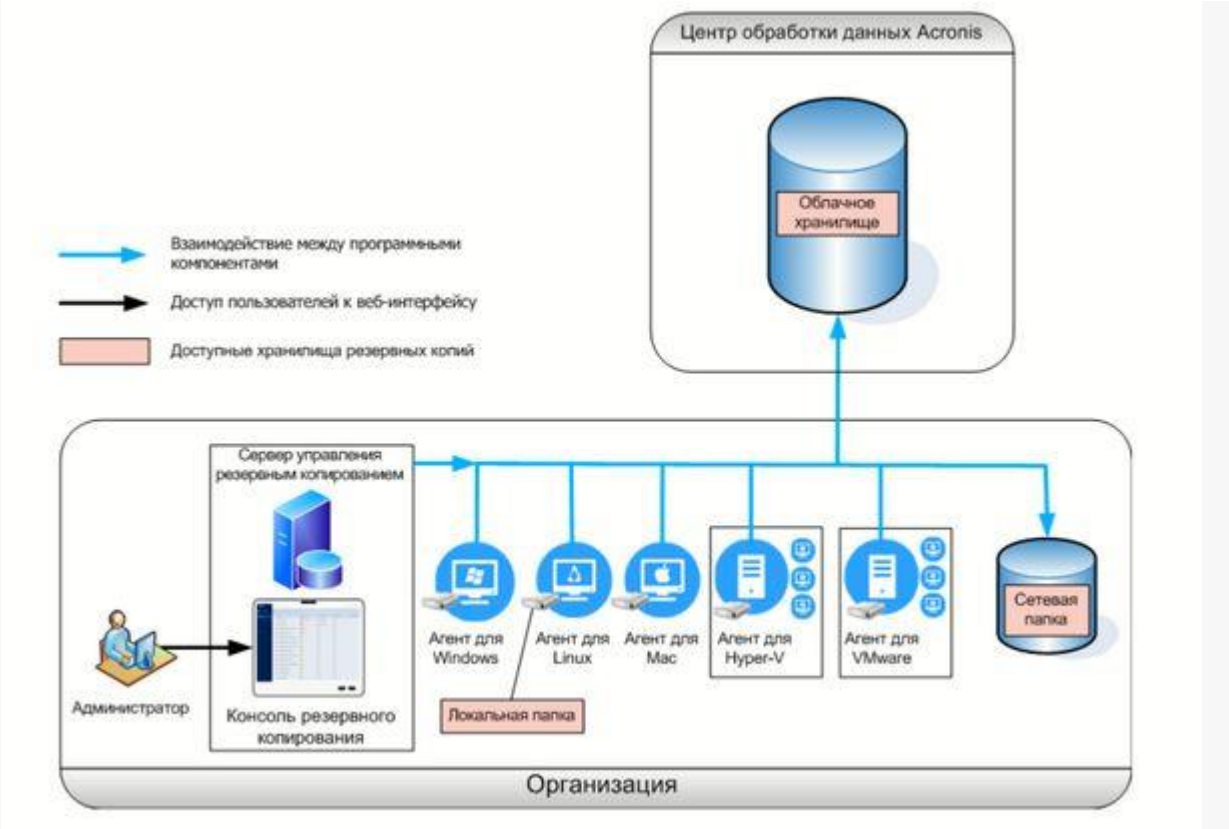

Рисунок 7 – Локальное развертывание Acronis Backup (источник: acronis.com)

Облачное развертывание**.** Сервер управления находится в одном из центров обработки данных Acronis. Преимущество этого подхода состоит в том, что не нужно обслуживать сервер управления в локальной сети. Acronis Backup можно представить, как сервис резервного копирования, предоставляемый Acronis (рис. 8).

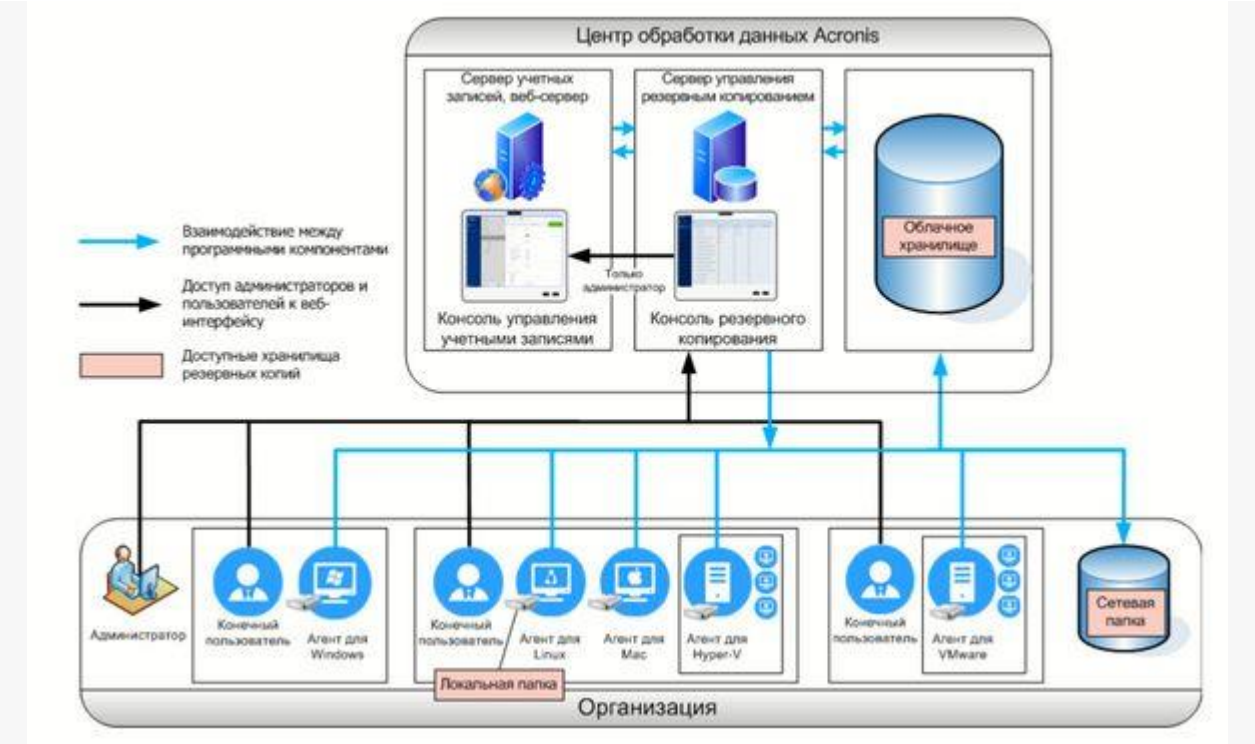

Рисунок 8 – Облачное развертывание Acronis Backup (источник: acronis.com)

Особенности. Детальное сравнение технологий бэкапа VMware vs Veeam vs Symantec vs Acronis представлены в таблице 7.

Таблица 7 – Сравнение технологий бэкапа VMware vs Veeam vs Symantec vs Acronis

Функции и возможности	**Data Recovery + vCenter**	**Veeam**	**Symantec**	**Acronis**
Бэкап данных	+	+	+	+
Создание снимков	+	+	+	+
Бэкап по времени	+	+	+	+
Отправка логов по e-mail	-	+	+	+
Откат машин к предыдущему состоянию	+	+	+	+
Централизованный интерфейс управления	+	+	+	+
Полная совместимость с решениями Vmware	+	+	+	+

Продолжение таблицы 7

Режим дедупликации[1]	+	+	-[2]	-[3]
Инкрементное резервное копирование[4]	+	+	+	+
Настраиваемые параметры для нескольких vCenter в режиме LinkedMode	+	+	+	+
Восстановление отдельных данных	+	+	+	+
Служба теневого копирования томов (VSS)	+	+	+	+
Управление политиками	+	-[5]	+	+
Совмещение со службами vMotion, HA, DRS	+	+	+	+
Поддержка типов хранения данных (Локальное, NFS, Share, iSCSI, Fibre Channel, NAS SAN, USB, DAS, облачные сервисы)	Локальное, NFS, Share, iSCSI, Fibre Channel, NAS	Локальное, NFS, Share, iSCSI, Fibre Channel, NAS, SAN	Локальное, NFS, Share, iSCSI, Fibre Channel, NAS, SAN, USB, DAS	Локальное, NFS, Share, iSCSI, Fibre Channel, NAS, SAN, DAS, облачные сервисы
Требование наличия vCenter	+	-	-	-
Возможность восстановления на другой аппаратной платформе[6]	-	-	+	+
Работа с базами SQL	-	+	-[7]	-
Работа с сервером Exchange	-	+	-[8]	-
Работа с Active Directory	-	+	-[9]	-
Возможность преобразования виртуальных сред в физические (V2P)	-	-	+	+

Продолжение таблицы 7

Возможность преобразования физических сред в виртуальные (P2V)	+	-	+	+
Рекомендация наличия vCenter	+	+	+	+
Моментальное восстановление после сбоя	-	+	+	+
Функция восстановления на «голое железо»[10]	-	-	+	+
Защита файлов шаблонов	-	+	+	-
Репликация данных	-	+	-	-
Проверка восстановления[11]	-	+	-	-
Работа с несколькими версиями ESX	Раздел идет по первой цифре версии	+	+	+
Поддержка ОС	Копирует всю машину, независимо от того какая ОС стоит	Копирует всю машину, независимо от того какая ОС стоит	Windows, Linux	Поддержка большинства ОС
Поддержка платформ	Только VMware	Только VMware	VMware, Microsoft Hyper-V, Citrix Xen, физические	VMware, Microsoft Hyper-V, Citrix Xen, Parallels, физические

Режим дедупликации позволяет сохранять бэкап не всей машины, а лишь данные, которые были изменены с момента последнего бэкапа. Это дает два существенных преимущества:

– существенная экономия места под резервное хранение данных;

– экономия трафика при расположении серверов на дальних друг от друга дистанциях (географическая составляющая).

Функция доступна с дополнительной опцией Deduplication Option.

Функция доступна с дополнительной опцией Deduplication.

Инкрементное резервное копирование позволяет сначала выполнить резервное копирование всего исходного каталога и потом «добавлять» к нему те файлы, которые изменились со времени последнего резервного копирования. Данная функция позволяет делать бэкап машины без перевода ее в режим обслуживания.

Функция, доступная с дополнительной программой Veeam Monitor.

Технология Symantec Restore Anyware позволяет пользователям перенести систему на другой компьютер, не выполняя установки заново.

Для базы данных SQL рекомендуется наличие Symantec Backup Exec Agent for Microsoft SQL Server, добавляющего функцию восстановление структуры базы данных.

Для сервера Exchange рекомендуется наличие Agent for Exchange Server, добавляющего функцию восстановление отдельных сообщений, папок и почтовых ящиков Exchange (устраняет необходимость резервного копирования почтовых ящиков).

Для сервера Active Directory рекомендуется наличие Agent for Active Directory, добавляющего функцию восстановление пользователей Active Directory, а также их свойств и атрибутов.

При утере файлов машины позволяет создать новую ВМ с такими же характеристиками и восстановить на нее старую.

После создания бэкапа данная технология проверяет, сможет ли поднять машину сразу после ее сбоя.

3.2 Оценка эффективности рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации и экономические затраты на их реализацию

Оценка эффективности является важным элементом разработки проектных и плановых решений, позволяющим определить уровень прогрессивности действующей структуры, разрабатываемых проектов или плановых мероприятий и проводится с целью выбора наиболее

рационального варианта структуры или способа ее совершенствования. Эффективность защитных мероприятий (ЗМ) должна оцениваться на стадии проектирования, для получения наилучших показателей работоспособности системы в целом.

При разработке проекта важны экономические показатели, которые наряду с техническими результатами будут определять эффективность системы. В состав затрат на разработку и исследование включаются затраты на проведение всех этапов работ.

Затраты на обеспечение информационной безопасности следует считать эффективными, если они обеспечивают выполнение требований нормативных документов и стандартов, принятых государством, а также концепции информационной безопасности организации.

Оценка эффективности рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего» проводится с использованием технических и программных средств контроля на предмет соответствия установленным действующим законодательством Российской Федерации требованиям.

После разработки рекомендаций по организации системы резервного копирования при обеспечении защиты информации в ИСПДн необходимо оценить эффективность их защиты. Сначала составляются общие критерии гипотетической оценки с указанием средств, которые обеспечат беспристрастный и полноценный анализ.

Программа и методика оценивания.

В программе обязательно должны быть:

- оцениваемый объект;
- запротоколированная очередность мероприятий, включая список и содержание проводимых процедур;
- итоговые оценочные критерии.

Критерии проверки:

1. Емкость хранения.

2. Пропускная способность.

3. Вычислительная мощность.

4. Временные рамки резервирования.

5. Время и точка восстановления.

По итогам вышеописанных манипуляций составляется протокол оценки эффективности рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации в техникуме. Он служит основой составления итогового заключения о состоянии защиты данных.

Расчет показателей эффективности может производиться с помощью различных методов: методы моделирования процессов защиты информации; экспертные оценки; статистический анализ; метод минимизации рисков и т.д.

В рамках исследовательской работы мы выбрали метод экспертной оценки.

Экспертная оценка – основана на компетентном мнении экспертов, знающих данную область и имеющих научно-практический потенциал для принятия решения.

Экспертная оценка эффективности рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации проводилась на базе в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего».

В процессе проведения экспертизы, рекомендации оценивались по следующим критериям:

1. Нормативно-правовая составляющая: соответствие разработанных рекомендаций требованиям действующих в России законодательных и нормативных документов по по орагниазции системы резервного копирования при обеспечении защиты информации.

2. Методическая составляющая рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации: содержательная и функциональная валидность предложенных мер, полнота

разработанных предложений и рекомендаций для совершенствования системы защиты.

3. Технологическая составляющая комплекса: характер предложенных программно-технических средств резервного копирования и рекомендаций по внедрению предложений.

Данные критерии были преобразованы в информационно-оценочную карту, которая представлена в таблице 8.

Перед проведением экспертизы была согласована система баллов, которые выставлялись экспертом при заполнении информационно-оценочной карты. Это было сделано для того, чтобы получаемая оценка обладала свойством надежности. То есть, чтобы разные эксперты, получив одни и те же данные, используя единую систему баллов и методы для их анализа, приходили к близким или одинаковым выводам.

Таблица 8 – Показатели оценки эффективности рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации в техникуме

Показатели оценки эффективности	**Эксперты**		
	Эксперт 1	Эксперт 2	Эксперт 3
	Критерии качества эффективности: высокий уровень (полностью соответствует показателю) средний уровень (в основном соответствует показателю) низкий уровень (в основном не соответствует показателю)		
1. Нормативно-правовая составляющая: соответствие разработанных рекомендаций требованиям действующих в России законодательных и нормативных документов по по орагниазции системы резервного копирования при обеспечении защиты информации.			
2. Методическая составляющая рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты.			

Продолжение таблицы 8

3. Технологическая составляющая комплекса: характер предложенных программно-технических средств резервного копирования и рекомендаций по внедрению предложений.			
Итоговая оценка экспертов:			

Каждому эксперту предлагались рекомендации рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации и информационно-оценочный лист с одинаковыми показателями оценки.

По итогам оценки эксперт представляет отчет, который содержит следующие сведения: заполненную информационно-оценочную карту; общие выводы.

В состав экспертной комиссии вошли: заведующий отделением информационных технологий, техник-программист, системный администратор отдела технической поддержки и связи техникума.

Результаты экспертной оценки представлены в таблице 9.

Таблица 9 – Результаты экспертной оценки эффективности предложенных рекомендаций

Показатели оценки эффективности	**Эксперты**		
	Эксперт М.И.	Эксперт К.С.	Эксперт З.Г.
	Критерии качества эффективности: высокий уровень (полностью соответствует показателю) средний уровень (в основном соответствует показателю) низкий уровень (в основном не соответствует показателю)		
1. Нормативно-правовая составляющая: соответствие разработанных рекомендаций требованиям действующих в России законодательных и нормативных документов по по орагниазции системы резервного копирования при обеспечении защиты информации.	Высокий уровень	Высокий уровень	Высокий уровень

Продолжение таблицы 9

2. Методическая составляющая рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты.	Высокий уровень	Средний уровень	Высокий уровень
3. Технологическая составляющая комплекса: характер предложенных программно-технических средств резервного копирования и рекомендаций по внедрению предложений.	Высокий уровень	Средний уровень	Высокий уровень
Итоговая оценка экспертов:	***Высокий уровень эффективности предложенных рекомендаций***		

Результаты экспертной оценки эффективности представлены на результирующей диаграмме (рис. 9).

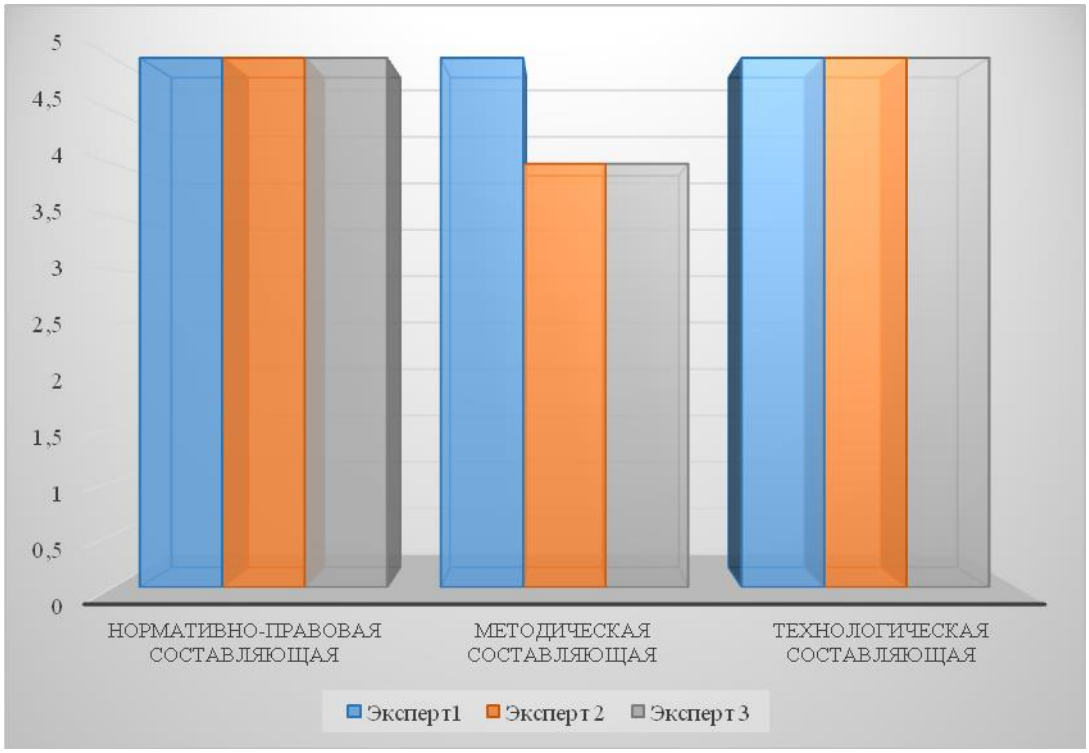

Рисунок 9 – Сводные результаты экспертной оценки эффективности разработанных рекомендаций

Проведенный анализ позволяет сделать вывод, что мнения экспертов относительно совпадают.

Далее составим статьи расходов (таблица 10).

Таблица 10 – Расходы на предложенные программно-технические средства резервного копирования

Статьи расходов	Сумма, руб
Постоянные расходы:	
1. Расходы электроэнергии	374,76
2. Заработная плата персонала	3400
3. Обслуживание FTP-сервера	1000
Итого:	4774,76
Переменные расходы:	
1. Покупка оборудования	17199
2. Покупка программного средства Acronis Защита Данных (Cyber Backup).	5459
Итого:	27432,76

Рассмотрим постоянные расходы.

1. Расход электроэнергии.

Усредненный тариф (городское население, дневная зона с 7-00 до 23-00 часов) на электроэнергию на 01.01.2022 - 3,47 руб./кВт ч.

Примерный расход кВт в час для сервера резервного копирования (не пиковая загруженность сервера) - 0,15 кВт.

Время работы сервера (в месяц) - 720 часов, предполагается постоянная работа сервера.

ИТОГО: 0,15 х 720 х 3,47 = 374,76 руб.

2. Заработная плата персонала.

1 сотрудник на полставки техника-программиста 11 разряда (почасовая форма расчета з/п):

52,5 руб. - час, норма - 80 ч./месяц.

52,5 руб. х 80 ч = 3400 руб.

ИТОГО: 3 400 руб.

Рассмотрим переменные расходы.

1. Покупка оборудования: Сетевое хранилище (NAS) QNAP D2.

Цена на 01.01.2022: 17 199 руб.

2. Покупка программного обеспечения: стоимость одной лицензии на Acronis Защита Данных – 5459 руб.

Необходимое количество зависит от конкретного учебного заведения, ориентировочно 10 штук.

10 шт. х 5459 руб. = 54590 руб.

Сведем полученные результаты в таблицу 11.

Таблица 11 – Инвестиции в проект

Сумма начальных инвестиции	76563,76 руб.
Ежемесячное содержание	4774,76 руб.

Итак, в результате анализа совокупных показателей существует возможность сделать обоснованный выбор в пользу предложенных мероприятий по совершенствованию организаций системы резервного копирования при обеспечении защиты информации в ИСПДн.

Таким образом, предложенные рекомендации по организации системы резервного копирования при обеспечении защиты информации несут в себе не только положительные моменты, такие как устранение основных проблем в организации среднего профессионального образования, касающихся информационной безопасности, но при этом они потребуют дополнительных вложений на приобретение оборудования.

Всегда будет иметь место человеческий фактор, форс-мажорные обстоятельства. Но если такие меры не предпринять затраты на восстановление информации, потерянные возможности по стоимости превзойдут те затраты, что требуются для разработки системы безопасности.

Таким образом, по результатам экспертной оценки эффективности и статьи расходов на программно-технические средства рекомендации по организации системы резервного копирования при обеспечении защиты информации находится в стадии исполнения в техникуме.

Выводы по главе 3

В третьей главе магистерской диссертации были предложены рекомендации по организации системы резервного копирования при обеспечении защиты информации в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего», выполнение которых позволит повысить эффективность средств защиты и сократит риск потери и искажения информации.

Рекомендации по организации системы резервного копирования при обеспечении защиты информации состоят из 3 этапов.

Этап 1. Разработка регламента копирования персональных данных субъектов ГБПОУ «ЧТПиГХ им. Я.П. Осадчего».

Настоящий Регламент определяет порядок резервирования данных для последующего восстановления работоспособности автоматизированных систем ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего» при полной или частичной потере информации, вызванной сбоями или отказами аппаратного, или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.); восстановления информации в случае возникновения такой необходимости; упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации, обрабатываемой в техникуме.

В настоящем документе регламентируются действия при выполнении следующих мероприятий: резервное копирование; контроль резервного копирования; хранение резервных копий; полное или частичное восстановление данных и приложений.

Этап 2. Выбор технологий. В качестве устройства NAS было выбрано для техникума: сетевое хранилище QNAP D2. Преимущество Накопителя NAS заключается в том, что можно будет использовать диски с сервера,

который компания планирует отключать после развертывание архивной копии через FTP.

Для выполнения резервного копирования по FTP была выбрана утилита Duplicity. Эта утилита находится в свободном доступе.

В результате необходимо будет только приобрести NAS-бокс и заплатить ежемесячную плату за работу FTP-сервера.

Этап 3. Усовершенствование программно-технических средств резервного копирования. В качестве программного продукта была выбрана система Защита Данных (Cyber Backup**)** и Acronis Защита Данных Облачная (Cyber Backup Cloud) компании Acronis.

По итогам вышеописанных манипуляций составляется протокол оценки эффективности рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации в техникуме. Он служит основой составления итогового заключения о состоянии защиты данных.

В процессе проведения экспертизы, рекомендации оценивались по следующим критериям:

1. Нормативно-правовая составляющая: соответствие разработанных рекомендаций требованиям действующих в России законодательных и нормативных документов по по орагниазции системы резервного копирования при обеспечении защиты информации.

2. Методическая составляющая рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты.

3. Технологическая составляющая комплекса: характер предложенных программно-технических средств резервного копирования и рекомендаций по внедрению предложений.

Описаны экономические затраты и план внедрения системы резервного копирования.

Таким образом, по результатам экспертной оценки эффективности и статьи расходов на программно-технические средства рекомендации по организации системы резервного копирования при обеспечении защиты информации находится в стадии исполнения в техникуме.

ЗАКЛЮЧЕНИЕ

На основании изученных информационных источников по теме исследования можно сделать вывод о практической необходимости организации системы резервного копирования при обеспечении защиты информации в образовательных организациях.

В первой главе магистерской диссертации решались следующие задачи: проанализировано понятие, назначение, функции и особенности систем резервного копирования. Изучены технологии резервного копирования и хранения резервных копий и данных, проанализированы программно-технические средства резервного копирования, наиболее подходящие для реализации систем резервного копирования в организации профессионального образования;

Вопрос по защите и резервному копированию информации стоит сегодня очень актуально ввиду безусловного развития информационных технологий и влечет за собой большой рост количества обрабатываемой и сохраняемой информации. Поэтому исследования и разработки в сфере хранения и резервного копирования информации всегда будут востребованы, аппаратно-программные средства и в дальнейшем будут развиваться, совершенствоваться и подстраиваться под потребности пользователей.

Система резервного копирования предназначена для создания резервных копий и восстановления данных. Она позволяет защитить данные от разрушения не только в случае сбоев или выхода из строя аппаратуры, но и в результате ошибок программных средств и пользователей.

На основании всего вышеизложенного можно сделать вывод, что организация системы резервного копирования безусловно необходимо при организации политики информационной безопасности образовательной организации.

Во второй главе магистерской диссертации проведен анализ информационных систем ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего».

В ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» эксплуатируются следующие информационные системы персональных данных (далее - ИСПДн) с использованием средств криптографической защиты информации (далее - СКЗИ, криптосредства):

1. ИСПДн «Бухгалтерия и кадры» в составе следующих подсистем:

- «Система дистанционного банковского обслуживания «Клиент-Банк», АО «Уральский банк реконструкции и развития» (далее - СДБО «Клиент-Банк УБРиР»);

- «Информационная система электронного документооборота «Интернет отчетность - Контур-Экстерн» (далее - ИС ЭДО «Контур-Экстерн»).

Для ИСПДн «Бухгалтерия и кадры» разработана ООО «СИБ Альпикс» и утверждена директором ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» «Модель угроз безопасности персональных данных ...» № СИБА.МУ.59 от 09.06.2016.

2. ИСПДн «ФИС ГИА и Приема».

Система защиты персональных данных при их обработке в информационных системах персональных данных в техникуме создана, но необходимо усовершенствовать систему резервного копирования при обеспечении защиты информации.

В третьей главе магистерской диссертации были предложены рекомендации по организации системы резервного копирования при обеспечении защиты информации в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего», в результате выполнения которых позволит повысить эффективность средств защиты и сократит риск потери и искажения информации.

Рекомендации по организации системы резервного копирования при обеспечении защиты информации состоят из 3 этапов.

Этап 1. Разработка регламента копирования персональных данных субъектов ГБПОУ «ЧТПиГХ им. Я.П. Осадчего».

В настоящем документе регламентируются действия при выполнении следующих мероприятий: резервное копирование; контроль резервного копирования; хранение резервных копий; полное или частичное восстановление данных и приложений.

Этап 2. Выбор технологий. В качестве устройства NAS было выбрано для техникума: сетевое хранилище QNAP D2. Преимущество Накопителя NAS заключается в том, что можно будет использовать диски с сервера, который компания планирует отключать после развертывание архивной копии через FTP.

Для выполнения резервного копирования по FTP была выбрана утилита Duplicity. Эта утилита находится в свободном доступе.

В результате необходимо будет только приобрести NAS-бокс и заплатить ежемесячную плату за работу FTP-сервера.

Этап 3. Усовершенствование программно-технических средств резервного копирования. В качестве программного продукта была выбрана система Защита Данных (Cyber Backup**)** и Acronis Защита Данных Облачная (Cyber Backup Cloud) компании Acronis.

По итогам вышеописанных манипуляций составляется протокол оценки эффективности рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации в техникуме. Он служит основой составления итогового заключения о состоянии защиты данных.

В процессе проведения экспертизы, рекомендации оценивались по следующим критериям:

1. Нормативно-правовая составляющая: соответствие разработанных рекомендаций требованиям действующих в России законодательных и нормативных документов по по орагниазции системы резервного копирования при обеспечении защиты информации.

2. Методическая составляющая рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты.

3. Технологическая составляющая комплекса: характер предложенных программно-технических средств резервного копирования и рекомендаций по внедрению предложений.

Описаны экономические затраты и план внедрения системы резервного копирования.

Таким образом, по результатам экспертной оценки эффективности и статьи расходов на программно-технические средства рекомендации по организации системы резервного копирования при обеспечении защиты информации находится в стадии исполнения в техникуме.

Таким образом, цель работы достигнута, задачи выполнены, гипотеза исследования подтвердилась.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативно – правовые акты

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введ. 2006-12-27. – М.: Изд-во стандартов, 2006. – 9 с.

2. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. – Введ. 2006-12-27. – М.: Изд-во стандартов, 2006. – 7 с.

3. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности. Основные термины и определения. – URL: http://www.opengost.ru/iso/35_gosty_iso/35020_gost_iso/11522-gost-r-53114-2008-zaschita-informacii.-obespechenie-informacionnoy-bezopasnosti.-osnovnye-terminy-i-opredeleniya.html. Дата обращения: 16.12.2020.

4. ГОСТ РВ 50600-93. Защита секретной информации от технической разведки. Система документов. Общие положения. - М.: Изд-во стандартов, 1993.

5. Доктрина информационной безопасности Российской Федерации от 09.09.2000: утверждена Президентом РФ В. Путиным // Известия. - 10 декабря 2002. - С.2

6. Конституция Российской Федерации: офиц. текст. - М.: Право, 2002. - 39 с.

7. О государственной тайне: ФЗ по состоянию на 22.08.2004. / Федер. Собр. Рос. Федерации. - М.: ГД РФ, 2004. - 12 с.

8. О коммерческой тайне: ФЗ от 29 июля 2004 № 98 // Собрание актов Президента и Правительства РФ. - № 7. - С.5.

9. О персональных данных: ФЗ от 27 июля 2006 № 152 - ФЗ // Бюллетень нормативных актов министерств и ведомств. - № 7. - 2006. - С.15.

10. Об архивном деле в Российской Федерации: ФЗ от 01 октября 2004 № 125 - ФЗ // Собрание актов Президента и Правительства РФ. - № 11. - С.12.

11. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 № 149 - ФЗ // СЗ РФ. – 2006. - №31

12. Об утверждении Перечня сведений конфиденциального характера от 06.03.97 № 188: указ Президента РФ // Собрание актов Президента и Правительства РФ. - 1993. - № 23. С.12 – 14.

13. Об утверждении Перечня сведений, которые не могут составлять коммерческую тайну: постановление правительства РФ от 03.10.2002 № 731 // Собрание актов Президента и Правительства РФ. - 2003. - № 11. - 140 с.

14. Об утверждении Перечня сведений, отнесенных к государственной тайне от 30.11.95 № 1203: с измен. и доп. от 24.01.98 № 61, от 06.06.2001 № 659, от 10.09.2001 № 1114, от 29.05.2002 № 518, от 11 февраля 2006: указ Президента РФ // Собрание актов Президента и Правительства РФ. - 2006. - № 11.

15. Об утверждении положения о государственной системе защиты информации от иностранной технической разведки и от ее утечки по техническим каналам от 15.09.93 № 912 - 51: постановление Правительства РФ // Собрание актов Президента и Правительства РФ. - 1993. - № 15. - 125 с.

16. Об утверждении Положения о лицензировании деятельности по технической защите конфиденциальной информации от 30.04.02. № 290: постановление Правительства РФ // Собрание актов Президента и Правительства РФ. - 2002. - № 8. - С.102.

17. Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 17 ноября 2007 г. № 781. URL - https://base.garant.ru/192223/. Дата обращения: 21.09.2020.

18. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти: постановление Правительства РФ от 3 ноября 1994 г. № 1233. // Собрание актов Президента и Правительства РФ. - 1995. - № 10. - С.56.

19. Трудовой кодекс Российской Федерации: федер. закон от 30.12.2001 N 197-ФЗ (ред. от 25.05.2020). URL - https://clck.ru/B8yGj. Дата обращения: 14.12.2020.

Литература

20. Ажмухамедов, И.М., Ханжина, Т.Б. Оценка экономической эффективности мер по обеспечению информационной безопасности [Текст] / И.М. Ажмухамедов, Т.Б. Ханжина // Вестник АГТУ. Серия: «Экономика» №1/2011, С.185-190.

21. Астахова Л.В., Завадский А.О. Особенности организации защиты персональных данных в образовательной организации // Вестник УрФО. Безопасность в информационной сфере. – 2013 – № 3(9). – С.4-10.

22. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) [Электронный ресурс]: [Утверждена заместителем директора ФСТЭК РФ 15.02.2008 г.]. - Режим доступа: www.fstec.ru (дата обращения: 15.12.2021).

23. Бугров А. Международные стандарты для построения системы информационной безопасности / А. Бугров // Финансовая газета. - 2017. - №10.

24. Галатенко В.А. Основы информационной безопасности: курс лекций / В.А. Галатенко. URL - https://www.intuit.ru/studies/courses/10/10/info (дата обращения: 20.12.2021).

25. Ильгова О. Этапы организации защиты ПДн в ОО (для администратора). – URL: https://help.dnevnik.ru/hc/ru/articles/203475268 (дата обращения: 16.12.2021).

26. Мельник Н.Ю. Защита персональных данных в профессиональном образовании // Современные технологии: актуальные вопросы, достижения и инновации. – 2018. – С. 55-57.

27. Мельников, В.П. Информационная безопасность и защита информации [Текст]: учеб. пособие / В.П. Мельников, С.А. Клейменов, А.М. Петраков. – М.: Издательский центр «Академия», 2013. – 336 с.

28. Меры по защите от угроз нарушения доступности [Электронный ресурс]. - URL: www.sha-danis.narod.ru (дата обращения: 20.12.2021).

29. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке информационных системах персональных данных с использованием средств автоматизации [Электронный ресурс]: [Утверждены руководством 8 центра ФСБ России 21.02.2008 г. №149/54-144]. - Режим доступа: www.consultant.ru. (дата обращения: 15.12.2021).

30. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (утв. ФСБ России 31.03.2015 N 149/7/2/6-432). Электронный документ. Режим доступа: http://docs.cntd.ru/document/420336137 (дата обращения: 16.01.2021).

31. Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014). Электронный документ. Режим доступа: http://fstec.ru/ (дата обращения: 16.12.2021).

32. Методы организации защиты информации [Текст]: учебное пособие для студентов 3–4 курсов всех форм обучения направлений подготовки 230400.55, 230701.51, 090300.65, 220100.55 / Ю.Ю. Громов и др. – Тамбов: Изд-во ФГБОУ ВО «ТГТУ», 2013. – 80 с.

33. Милютина О.В. Особенности защиты информации в образовательном учреждении / О.В. Милютина. – URL: http://www.fcoit.ru/internet_conference/information_security_training_process/fea

tures_information_security_in_an_educational_institution.php (дата обращения: 10.12.2021).

34. Официальный сайт ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего». – URL: http://chtpgh.ru/ (дата обращения: 19.12.2021).

35. Политика обработки и защиты персональных данных Государственного бюджетного профессионального образовательного учреждения «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего» – URL: http://chtpgh.ru/ (дата обращения: 19.12.2021).

36. Положение об обработке и защите персональных данных в ГБПОУ «Челябинский техникум промышленности и городского хозяйства им. Я.Г1. Осадчего» – URL: http://chtpgh.ru/ (дата обращения: 19.12.2021).

37. Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

38. Постановление Правительства РФ от 03.02.2012 N 79 (с изм. от 15.06.2016) «О лицензировании деятельности по технической защите конфиденциальной информации». – Режим доступа: http://www.garant.ru/ (дата обращения: 16.12.2021).

39. Постановление Правительства РФ от 03.03.2012 N 171 (с изм. от 15.06.2016) «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации». [Электронный ресурс]. Режим доступа: http://www.garant.ru/ (дата обращения: 16.12.2021).

40. Постановление Правительства РФ от 06.07.2008 № 512 (ред. от 27.12.2012) «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» от 06.07.2008 № 512 // «Российская газета», № 148, 11.07.2008.

41. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // «Российская газета», № 200, 24.09.2008.

42. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) Федеральной службы безопасности Российской Федерации (ФСБ России) Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. N 55/86/20 г. Москва «Об утверждении Порядка проведения классификации информационных систем персональных данных» // «Российская газета», № 4637, 12.04.2008.

43. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ России и Министерства связи и массовых коммуникаций РФ от 31 декабря 2013 г. № 151/786/461 «О признании утратившим силу приказа Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных». - Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/815-sovmestnyj-prikaz-fstek-rossii-fsb-rossii-i-minkomsvyazi-rossii-ot-31-dekabrya-2013-g-n-151-786-461. Дата обращения: 16.12.2021.

44. Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн при использовании средств криптографической защиты информации» // «Российская газета» от 17 сентября 2014 г. N 211.

45. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению

безопасности персональных данных при их обработке в информационных системах персональных данных» // «Российская газета», № 107, 22.05.2013.

46. Резервное копирование и синхронизация данных между компьютерами [Электронный ресурс]. Режим доступа: http://www.root.cz/clanky/dropbox-zaloha-a-synchronizace-datmezi-pocitaci/ (дата обращения: 13.12.2021).

47. Система резервного копирования (безопасность) – URL: https://www.tadviser.ru/index.php (дата обращения: 15.01.2022).

48. Техническая документация с официальных источников (сайт разработчиков продуктов Acronis) [Электронный ресурс]. Режим доступа: www.acronis.ru (дата обращения: 15.01.2022).

49. Фионова Л.Р Положение о защите персональных данных работников / Л.Р. Фионова, О.В. Касперская // Секретарское дело. - 2015. - № 10. - С.40 - 49.

50. Ширманов А. Законодательные требования к информационной безопасности процесса резервного копирования информации / А. Ширманов. – URL: https://www.veeam.com/ru/wp_regulatory_requirements_for_backup_wp.pdf (дата обращения: 15.01.2022).

51. Ярочкин В.Н. Информационная безопасность / В.Н. Ярочкин. - М.: Трикста, Академ. проект, 2015. - 542 с.

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА АВТОМОБИЛЬНОГО ТРАНСПОРТА, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ТЕХНИЧЕСКИМ ДИСЦИПЛИНАМ

Организация системы резервного копирования при обеспечении защиты информации в образовательной организации

Выпускная квалификационная работа по направлению
44.04.04 Профессиональное обучение (по отраслям)
Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном образовании»
Форма обучения заочная

Проверка на объем заимствований:
80,47% авторского текста

Работа рекомендована к защите
«17» января 2022 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Белов Алексей Иванович

Научный руководитель:
д.т.н., профессор
Дмитриев Михаил Сергеевич

Челябинск
2022

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность исследования. Усиление роли информационных технологий в процессах управления образовательных организаций обусловливает повышение требований к целостности и доступности данных в течение их жизненного цикла. В последние годы возросло внимание к системам резервного копирования — наиболее распространенному средству обеспечения сохранности данных. Проводится большое количество исследований, нацеленных на их совершенствование. Одно из основных направлений исследований связано с улучшением процессов управления хранением данных, разработкой новых алгоритмов резервного копирования, совершенствованием процесса восстановления данных.

Резервное копирование - это процесс создания когерентной (непротиворечивой) копии данных. Резервное копирование становится все более важным на фоне значительного увеличения объема данных в компьютерной индустрии. Подсистема резервного копирования - очень важная часть любой информационной системы.

При правильной ее организации она способна решить сразу же две задачи. Во-первых, надежно защитить весь спектр важных данных от утери. Во-вторых, организовать быструю миграцию с одного ПК на другой в случае необходимости, то есть, фактически обеспечить бесперебойную работу сотрудников. Только в этом случае можно говорить об эффективной работе резервного копирования. Овладение тактикой резервного копирования - неотъемлемый атрибут профессионализма пользователя и системного администратора.

Создание системы резервного копирования является немаловажной задачей при построении ИТ-инфраструктуры и реализации политики информационной безопасности организации профессионального образования. Но почему-то важность резервирования данных многие осознают только после потери критически важной информации.

Сложность проблемы эффективного хранения усугубляется наблюдаемым экспоненциальным ростом количества данных, который, согласно исследованиям, ведущего международного аналитического агентства IDC, составляет 50-100 % ежегодно. Планирование ожидаемых объемов данных является необходимой составляющей процесса управления их хранением. Инструментарий оценки роста объема хранилищ для резервирования данных практически не представлен в современных системах. Требуется разработка способа прогнозирования объема хранимых резервных копий.

В общем случае в хранилище может существовать несколько наборов элементарных резервных копий, пригодных для восстановления. Это обусловливает проблему нахождения оптимального набора копий для восстановления независимо от использованного алгоритма с учетом утраченных и дополнительно созданных копий.

Для выполнения процедуры резервного копирования обычно создаются специальные программно-аппаратные подсистемы, называемые подсистемами резервного копирования. Они как раз и предназначены как для проведения регулярного автоматического копирования системных и пользовательских данных, так и для оперативного восстановления данных. Хранение информации отдельно от системных файлов уже является обязательным правилом. В случае обычного пользователя это означает, как минимум, разделение HDD на три логических диска: для системы, для приложений, для данных. В случае образовательной организации с большим объемом конфиденциальной информации - размещение информации на других, не системных физических дисках. Эта мера облегчает и саму операцию архивирования данных. Принцип раздельного хранения информации относится и к файловым архивам и к образам дисков. Их необходимо также хранить как минимум на несистемных разделах одного HDD. Принцип раздельного хранения информации должен реализовываться еще жестче: как минимум одна из копий должна храниться в отдельном

месте, чтобы не потерять информацию в случае непредвиденных обстоятельств.

Это определяет актуальность создания системы защиты информации на объекте, ориентированной на угрозы безопасности, представленные в документах ФСТЭК и ФСБ России.

Анализ состояния проблемы информационной безопасности в организациях профессионального образования позволил выявить *противоречие* между целесообразностью использования комплексных мер при реализации политики ИБ образовательного учреждения и недостаточной защищенностью от потери или искажения данных.

Это определило проблему исследования, заключающуюся в необходимости внедрения системы резервного копирования для реализации политики безопасности в организации профессионального образования.

Таким образом, можно сделать вывод, что тема исследования «Организация системы резервного копирования при обеспечении защиты информации в образовательной организации» является актуальной, а полученные результаты имеют важное практическое значение.

Цель исследования: теоретико-методическое обоснование и разработка рекомендаций по организации системы резервного копирования при обеспечении защиты информации в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего».

Объект исследования: процесс обеспечения информационной безопасности в организации профессионального образования.

Предмет исследования: организация системы резервного копирования.

Гипотеза исследования: разработка рекомендаций по организации системы резервного копирования и их внедрение позволит повысить уровень информационной безопасности в организации профессионального образования.

Задачи исследования:

– проанализировать понятие, назначение, функции и особенности систем резервного копирования;

– изучить технологии резервного копирования и хранения резервных копий и данных, проанализировать программно-технические средства резервного копирования, наиболее подходящие для реализации систем резервного копирования в организации профессионального образования;

– проанализировать информационные системы в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего»;

– разработать рекомендации по организации системы резервного копирования при обеспечении защиты информации в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего»;

– произвести оценку эффективности разработанных рекомендаций и экономических затрат на их реализацию.

Для решения поставленных задач были использованы следующие *методы исследования:* изучение и анализ теоретико-методической литературы по теме исследования; документоведческий метод (анализ документации образовательной организации); анализ и сопоставление имеющихся средств для защиты данных; анализ и классификация собранных данных с последующим моделированием и проектированием системы защиты персональных данных; метод апробации результатов; метод экспертной оценки качества разработанных мер защиты.

Теоретической и методологической базой исследования явились нормативно-правовые акты законодательства Российской Федерации, а также труды следующих авторов: Авдеев М.Ю., Алексеев С.С., Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С., Бадьина А., Бархатова Е.Ю., Беспалов Ю.Ф., Сенаторова Н.В., Терещенко Л.К. Хужокова И.М., Якушев В.С.

Состояние изученности проблемы.

Общетеоретические аспекты исследования информационной безопасности представлены в публикациях Е. Б. Белова, Е. А. Ерофеева, В.Н. Лопатина, А. А. Стрельцова, В. А. Тихонова, В. В. Райх, Ю. С. Уфимцева.

Крупный вклад в развитие теории и практики информационной безопасности внесли И.И. Быстров, В.А. Герасименко, О.Ю. Гаценко, А.А. Грушо, В.С. Заборовский, П.Д. Зегжда, Д.П. Зегжда, В.А. Конявский, А.А. Малюк, А.А. Молдовян и др.

Ряд работ посвящен системно-управленческому аспекту информационной безопасности: А. А. Кононова, А. В. Манойло, С. А. Мелина, Ю. А. Родичева, Д. И. Правикова, А. С. Устинова, Д. Б. Фролова.

Практическая значимость работы заключается в анализе имеющихся на рынке систем резервного копирования и выборе наиболее подходящей для внедрения в систему информационной безопасности ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего»; возможности применения разработанных рекомендаций в других учебных заведениях СПО.

База исследования: ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего».

Ход исследования и его результаты докладывались и обсуждались на международных конференциях: Международная научно-практическая конференция «Синтез науки и образования в решении глобальных проблем современности», г. Стерлитамак, февраль 2022 года; Международная научно-практическая конференция «Научно-технический прогресс и инновационные технологии», г. Ижевск, декабрь 2021 г.

Структура магистерской диссертации: работа состоит из введения, трех глав, заключения, списка использованных источников, состоящего из 51 наименования.

ГЛАВА 1 ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ РАЗРАБОТКИ И ПРИМЕНЕНИЯ СИСТЕМ РЕЗЕРВНОГО КОПИРОВАНИЯ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ

1.1 Понятие, назначение, функции и особенности систем резервного копирования

Термины и определения.

Резервное копирование (англ. backup copy) — процесс создания копии данных на носителе (жестком диске, дискете и т. д.), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

Система резервного копирования – это программный или программно-аппаратный комплекс для создания копий данных с определенной периодичностью для их последующего восстановления.

Стратегия резервного копирования - одна или несколько операций резервного копирования данных.

Резервное копирование или бэкап - процесс создания копии данных на носителе (оптический диск, жесткий диск и другие) с целью восстановления данных в первоначальном месте их расположения в случае их повреждения или разрушения. Резервное копирование предназначено для быстрого и недорогого восстановления информации (документов, приложений, настроек) в случае утери рабочей копии по какой-либо причине.

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

Наиболее частыми причинами потери информации могут быть:

- аппаратные сбои;
- сбои операционной системы и прикладного программного обеспечения;
- вирусы, черви и троянские кони;

– непреднамеренное уничтожение информации, ошибки пользователей;

– преднамеренное уничтожение информации.

Реализация основной задачи резервного копирования способствует также упорядочению информации и процедур ее использования. В частности, становится ясно, какая информация хранится на том или ином рабочем месте, как она используется пользователями и программным обеспечением, появляется возможность оценить ее количественные характеристики, например, объемы и частоту использования.

Жизненный цикл информации включает:

– создание;

– копирование;

– использование;

– хранение: текущее (требуется резервное копирование); долговременное (требуется архивирование).

Резервное копирование снимает зависимость информации от конкретного рабочего места, она становится перемещаемой и не привязанной к одному компьютеру или помещению. При возникновении критических ситуаций, которые могут привести к потере работоспособности оборудования или программного обеспечения, можно в краткие сроки перенести данные и ПО в другое место, на другой компьютер или в другое помещение.

Основные функции системы резервного копирования:

– создания резервных копий файлов, баз данных, приложений, системной информации и других необходимых данных;

– восстановление данных в случае утери информации;

– регулярное автоматизированное создание резервных копий на основании политик бэкапа;

– возможность восстановления нескольких версий файлов;

– надежное хранение резервных копий в течение установленного периода времени;

– обеспечение требуемого времени восстановления информации из резервных копий.

Места хранения электронной информации:

- сервера;
- рабочие станции.

Объекты хранения информации:

- ОС и утилиты;
- прикладное (специализированное) ПО;
- данные.

Методы резервного копирования:

1) клонирование (point-in-time), т.е. создание нескольких физических копий томов (клонов);

2) создание мгновенной копии (snapshot), т.е. создание логической копии диска, его образа;

3) 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).

К системам резервного хранения информации применяют три критерия и требования:

– предельная простота и быстрота внедрения данных технологий в любых масштабах предприятия - от небольшой фирмы до больших корпораций;

– надежность хранения информации – об этом критерии мы говорили выше;

– предельная простота и автоматизация эксплуатации внедренных систем.

Резервному копированию подлежит информация следующих основных категорий:

- персональная информация пользователей (личные каталоги на файловых серверах);
- групповая информация пользователей (общие каталоги отделов);
- информация, необходимая для восстановления серверов и систем управления базами данных (далее – СУБД);
- персональные профили пользователей сети;
- информация автоматизированных систем, в т.ч. баз данных;
- данные справочно-информационных систем общего использования («Гарант», «Консультант+» и т.п.);
- рабочие копии установочных компонент программного обеспечения рабочих станций;
- регистрационная информация системы информационной безопасности автоматизированных систем.

Машинным носителям информации, содержащим резервную копию, присваивается гриф конфиденциальности по наивысшему грифу содержащихся на них сведений в соответствии с «Перечнем сведений составляющих коммерческую тайну».

Существует два основных способа резервного копирования данных.

1. Создание бэкапа. В этом случае пользователь сам выбирает для копирования определенные файлы и / или папки. Так, к примеру, можно сделать резервную копию папки «Мои документы». При этом существует возможность выбора для копирования файлов определенных форматов, к примеру всех MP3-файлов или всех изображений в формате JPEG, которые хранятся в одной папке.

2. Создание образа - точной копии всего жесткого диска или одного из его разделов (включая операционную систему Windows, все установленные в системном разделе программы и данные). Основное преимущество данного способа: при полном выходе компьютера из строя операционную систему можно восстановить из образа. Кроме того, хорошая программа резервного копирования позволяет выполнять поиск внутри образа и последующее восстановление отдельных папок и файлов, ошибочно удаленных с компьютера.

В начале необходимо выбрать место для сохранения резервной копии, к примеру внешний жесткий диск, на котором достаточно свободного места. При полном резервном копировании программа создает из выбранных файлов один большой файл, содержащий резервные копии всех данных. Впоследствии при выполнении дифференциального или инкрементного копирования туда же записываются дополнительные данные.

Выбор накопителя. Встроенный жесткий диск - худший вариант: при возникновении механических дефектов винчестера резервная копия данных будет безвозвратно утеряна. Оптимальный вариант - приобретение внешнего жесткого диска, который будет использоваться исключительно для хранения копий.

График резервного копирования. При его составлении выполняйте следующие правила.

1. При покупке нового компьютера рекомендуется, не откладывая, выполнить полное резервное копирование. Так в случае возникновения

проблем вы всегда сможете восстановить первоначальное состояние системы.

2. Повторное полное резервное копирование необходимо произвести тогда, когда вы установите все программы, с которыми обычно работаете, и драйверы для всех компонентов компьютера, а также настроите доступ в Интернет.

3. Перед проведением на компьютере важных изменений, независимо от того, касаются они аппаратного или программного обеспечения, также необходимо выполнять резервное копирование данных.

4. Выполняйте резервное копирование регулярно, через небольшие промежутки времени.

Способ резервного копирования. Вы можете регулярно выполнять полное резервное копирование данных. Однако не все файлы постоянно изменяются. Кроме того, на это уходит много времени и места на диске, так как сохраняется содержимое всех дорожек диска. Существует два различных способа регулярного обновления резервных копий файлов. Поэтому при слежении за актуальностью данных вы можете выбирать между дифференциальным и инкрементным копированием.

Под дифференциальным копированием понимается копирование изменившейся информации за определенный отрезок времени. Причем каждое последующее копирование включает в себя как изменившиеся файлы, так и те, которые остались неизмененными со времени полного бэкапа. То есть дифференциальное копирование - это копирование всей разницы между первым и последним копированием.

Инкрементный бэкап копирует только новые и изменившиеся файлы со времен предыдущего копирования, а не первого. Поэтому, как правило, дифференциальный бэкап занимает больше места на носителе, чем инкрементальный. Но инкрементальный бэкап сложнее восстанавливать, так как приходится учитывать не только первый и последний бэкап-файлы, но и все промежуточные инкременты.

Хорошие программы резервного копирования сжимают данные для экономии места на диске и предоставляют следующие функции резервного копирования, такие как планировщик, возможность шифрования данных и дополнительную защиту бэкапа паролем.

Потеря информации возможна вследствие непреодолимых обстоятельств – разгул стихии, землетрясение. Так что и нужно предусмотреть возможность восстановления информации вследствие всего этого. Лучше всего хранить информацию, которая была зарезервирована, в другом помещении.

Если же информация повредилась в результате вирусной атаки или действия вредоносного программного обеспечения, нужно установить хорошую антивирусную защиту на все компьютеры, входящие в локальную сеть, и периодически обновлять антивирусные базы сигнатур. При этом нужно еще и хранить копии важной информации в таком месте, до которого вредоносное программное обеспечение даже теоретически добраться не сможет.

При сбое или уничтожении информации по вине человеческого фактора нужно тщательнейшим образом распределить все права доступа к ресурсам в сети, организовать регулярное резервное копирование информации, и регулярно обновлять используемое на компьютерах программное обеспечение.

1.2 Технологии резервного копирования и хранения резервных копий и данных

В зависимости от важности хранимой на компьютере информации и от частоты её использования, выполняют несколько видов резервного копирования данных:

1. Полное резервное копирование (Full backup).
2. Дифференциальное резервное копирование (Differential backup).
3. Инкрементное резервное копирование (Incremental backup).

1. Полное резервное копирование.

Является главным и основополагающим методом создания резервных копий, при котором выбранный массив данных копируется целиком. Это наиболее полный и надежный вид резервного копирования, хотя и самый затратный. В случае необходимости сохранить несколько копий данных общий хранимый объем будет увеличиваться пропорционально их количеству. Для предотвращения большого объёма использованных ресурсов используют алгоритмы сжатия, а также сочетание этого метода с другими видами резервного копирования: инкрементным или дифференциальным. И, конечно, полное резервное копирование незаменимо в случае, когда нужно подготовить резервную копию для быстрого восстановления системы с нуля.

Достоинства метода:

– легкий поиск файлов - Поскольку выполняется резервное копирование всех данных, содержащихся на устройстве, для поиска нужного файла не требуется просматривать несколько носителей;

– текущая резервная копия всей системы всегда расположена на одном носителе или наборе носителей - Если потребуется восстановить всю систему, то всю необходимую информацию можно найти в последней полной резервной копии.

Недостатки метода:

– избыточная защита данных - поскольку большинство файлов системы изменяются достаточно редко, то каждая последующая полная резервная копия представляет собой копию данных, сохраненных в ходе первого полного резервного копирования. Для полного резервного копирования требуется большой объём носителя.

– полное резервное копирование занимает больше времени - Для создания полных резервных копий может потребоваться длительное время, в особенности, если для хранения выбраны устройства в сети.

2. Дифференциальное резервное копирование.

Отличается от инкрементного тем, что копируются данные с

последнего момента выполнения Full backup. Данные при этом помещаются в архив «нарастающим итогом». В системах семейства Windows этот эффект достигается тем, что архивный бит при дифференциальном копировании не сбрасывается, поэтому измененные данные попадают в архивную копию, пока полное копирование не обнулит архивные биты.В силу того, что каждая новая копия, созданная таким образом, содержит данные из предыдущей, это более удобно для полного восстановления данных на момент аварии. Для этого нужны только две копии: полная и последняя из дифференциальных, поэтому вернуть к жизни данные можно гораздо быстрее, чем поэтапно накатывать все инкременты. К тому же этот вид копирования избавлен от вышеперечисленных особенностей инкрементного, когда при полном восстановлении старые файлы, возрождаются из пепла. Возникает меньше путаницы. Но дифференциальное копирование значительно проигрывает инкрементному в экономии требуемого пространства. Так как в каждой новой копии хранятся данные из предыдущих, суммарный объем зарезервированных данных может быть сопоставим с полным копированием. И, конечно, при планировании расписания (и расчетах, поместится ли процесс бэкапа во временное «окно») нужно учитывать время на создание последней, самой большой, дифференциальной копии.

Достоинства метода:

– легкий поиск файлов - Для восстановления системы, защищенной с помощью стратегии дифференциального резервного копирования требуются две резервные копии - последняя полная резервная копия и последняя дифференциальная резервная копия. Время восстановления значительно меньше по сравнению со стратегиями резервного копирования, для которых требуются последняя полная резервная копия и все инкрементальные резервные копии, созданные с момента последнего полного резервного копирования;

– меньшее время резервного копирования и восстановления - Дифференциальное резервное копирование занимает меньше времени, чем

полное резервное копирование. Восстановление после аварии выполняется быстрее, поскольку для полного восстановления устройства необходимы только последняя полная резервная копия и дифференциальная резервная копия.

Недостаток метода: избыточная защита данных (сохраняются все файлы, измененные с момента последнего инкрементального резервного копирования. Таким образом, создаются избыточные резервные копии).

3. Инкрементное резервное копирование.

В отличие от полного резервного копирования в этом случае копируются не все данные (файлы, сектора и т.д.), а только те, что были изменены с момента последнего копирования. Для выяснения времени копирования могут применяться различные методы, например, в системах под управлением операционных систем семейства Windows используется соответствующий атрибут файла (архивный бит), который устанавливается, когда файл был изменен, и сбрасывается программой резервного копирования. В других системах может использоваться дата изменения файла. Понятно, что схема с применением данного вида резервного копирования будет неполноценной, если время от времени не проводить полное резервное копирование. При полном восстановлении системы нужно провести восстановление из последней копии, созданной Full backup, а потом поочередно восстановить данные из инкрементных копий в порядке их создания. Данный вид используется для того, чтобы в случае создания архивных копий сократить расходуемые объемы на устройствах хранения информации (например, сократить число используемых ленточных носителей). Также это позволит минимизировать время выполнения заданий резервного копирования, что может быть крайне важно в условиях, когда машина работает постоянно, или прокачивать большие объемы информации. У инкрементного копирования есть один нюанс: поэтапное восстановление возвращает и нужные удаленные файлы за период восстановления. Например: допустим, по выходным дням выполняется полное копирование, а

по будням инкрементное. Пользователь в понедельник создал файл, во вторник его изменил, в среду переименовал, в четверг удалил. Так вот при последовательном поэтапном восстановлении данных за недельный период мы получим два файла: со старым именем за вторник до переименования, и с новым именем, созданным в среду. Это произошло потому, что в разных инкрементных копиях хранились разные версии одного и того же файла, и в итоге будут восстановлены все варианты. Поэтому при последовательном восстановлении данных из архива «как есть» имеет смысл резервировать больше дискового пространства, чтобы смогли поместиться в том числе и удаленные файлы.

Достоинства метода:

– эффективное использование носителей - поскольку сохраняются только файлы, измененные с момента последнего полного или инкрементального резервного копирования, резервные копии занимают меньше места;

– меньшее время резервного копирования и восстановления - инкрементальное резервное копирование занимает меньше времени, чем полное и дифференциальное резервное копирование.

Недостаток метода: данные резервного копирования сохраняются на нескольких носителях.

Поскольку резервные копии расположены на нескольких носителях, восстановление устройства после аварии может занять больше времени. Кроме того, для эффективного восстановления работоспособности системы носители должны обрабатываться в правильном порядке.

В процессе выполнения резервного копирования данных появляется проблема выбора технологии хранения резервных копий и данных. В настоящее время особой популярностью пользуются следующие виды носителей:

1. Накопители на магнитных лентах.

2. Дисковые накопители.

3. Сетевые технологии.

1. Накопители на магнитных лентах.

Не только в крупных корпорациях, но и на предприятиях малого бизнеса хорошо понимают необходимость резервного копирования и восстановления информации. В системах масштаба предприятия и сетях крупных департаментов, в небольших компаниях и у индивидуальных пользователей одинаковым успехом пользуются потоковые накопители, или стримеры. В основе их конструкции лежит лентопротяжный механизм, работающий в инерционном режиме. Для обоснованного выбора системы резервного копирования надо ясно представлять себе достоинства и недостатки разных устройств, которые во многом определяются емкостью системы, ее быстродействием, надежностью и ценой. Основные стимулы к повышению производительности ленточных устройств среднего и старшего класса - это широкое использование Интернета и распространение корпоративных интрасетей, увеличение числа серверов (нужных, чтобы обеспечить рост этих сетей), а также ужесточение требований к хранению информации и ее восстановлению в случае аварий. Спрос на системы резервного копирования и хранения данных особенно подстегивается все более активным использованием таких приложений, как мультимедиа, видео по запросу, звуковое информационное наполнение, обработка изображений и т.п.

Применяются два метода записи на магнитную ленту: наклонный и линейный серпантинный. В системах наклонной записи несколько считывающих/записывающих головок размещают на вращающемся барабане, установленном под углом к вертикальной оси (аналогичная схема применяется в бытовой видеоаппаратуре). Движение ленты при записи/чтении возможно только в одном направлении. В системах линейной серпантинной записи считывающая/записывающая головка при движении ленты неподвижна. Данные на ленте записываются в виде множества параллельных дорожек (серпантина). Головка размещается на специальной

подставке; по достижении конца ленты она сдвигается на другую дорожку. Движение ленты при записи/чтении идет в обоих направлениях. На самом деле таких головок обычно устанавливается несколько, чтобы они обслуживали сразу несколько дорожек (они образуют несколько каналов записи/чтения).

Плюсы хранения данных на ленточном носителе:

– низкая стоимость;

– низкое энергопотребление накопителя;

– большие объемы данных;

– простой способ увеличения объема хранимых данных без значительных инвестиций.

Минусы хранения данных на ленточном носителе:

– низкая скорость доступа к данным;

– сложный процесс обработки параллельных запросов к данным.

2. Дисковые накопители.

Существует два наиболее часто встречающихся вида дисковых накопителей: накопители на жёстких магнитных дисках и накопители на оптических дисках.

Накопители на жестких магнитных дисках (Hard Disk Drive, HDD) являются основными устройствами оперативного хранения информации. Для современных одиночных накопителей характерны объемы от сотен мегабайт до нескольких гигабайт при времени доступа 5-15 мс и скорости передачи данных 1-10 Мбайт/с. Относительно корпуса сервера различают внутренние и внешние накопители. Внутренние накопители существенно дешевле, но их максимальное количество ограничивается числом свободных отсеков корпуса, мощностью и количеством соответствующих разъемов блока питания сервера. Установка и замена обычных внутренних накопителей требует выключения сервера, что в некоторых случаях недопустимо. Внутренние накопители с возможностью "горячей" замены (Hot Swap) представляют собой обычные винчестеры, установленные в специальные

кассеты с разъемами. Кассеты обычно вставляются в специальные отсеки со стороны лицевой панели корпуса, конструкция позволяет вынимать и вставлять дисководы при включенном питании сервера. Для стандартных корпусов существуют недорогие приспособления (Mobile Rack), обеспечивающие оперативную съемность стандартных винчестеров. Внешние накопители имеют собственные корпуса и блоки питания, их максимальное количество определяется возможностями интерфейса. Обслуживание внешних накопителей может производиться и при работающем сервере, хотя может требовать прекращения доступа к части дисков сервера.

Для больших объемов хранимых данных применяются блоки внешних накопителей - дисковые массивы и стойки, представляющие собой сложные устройства с собственными интеллектуальными контроллерами, обеспечивающими, кроме обычных режимов работы, диагностику и тестирование своих накопителей. Более сложными и надежными устройствами хранения являются RAID-массивы (Redundant Array of Inexpensive Disks - избыточный массив недорогих дисков). Для пользователя RAID представляет собой один (обычно SCSI) диск, в котором производится одновременная распределенная избыточная запись (считывание) данных на несколько физических накопителей (типично 4-5) по правилам, определяемым уровнем реализации (0-10). Например, RAID Level 5 позволяет при считывании исправлять ошибки и осуществлять замену любого диска без остановки обращения к данным.

Устройства считывания компакт-дисков CD-ROM расширяют возможности системы хранения данных NetWare. Существующие накопители обеспечивают скорость считывания от 150 кбайт/с до 300/600/900/1500 Кбайт/с для 2-,4-,6- и 10-скоростных моделей при времени доступа 200-500 мс. NetWare позволяет монтировать компакт-диск как сетевой том, доступный пользователям для чтения. Объем тома может достигать 682 Мбайт (780 Мбайт для Mode 2). Устройства CD-ROM

выпускаются с различными интерфейсами, как специфическими (Sony, Panasonic, Mitsumi), так и общего применения: IDE и SCSI. Сервер NetWare обслуживает только CD-ROM с интерфейсами SCSI, новые драйверы существуют и для IDE; устройства со специфическими интерфейсами могут использоваться только в DOS для инсталляции системы. С точки зрения повышения производительности предпочтительнее использование CD-ROM SCSI, однако они существенно дороже аналогичных IDE-устройств. В сервере с дисками SCSI применение CD-ROM с интерфейсом IDE может оказаться невозможным из-за конфликтов адаптеров.

Достоинствами таких накопителей является:

– быстрый доступ к данным;

– возможность параллельного доступа к данным без значительной потери скорости.

Недостатки дисковых накопителей:

– более высокая стоимость чем ленты;

– более высокое энергопотребление;

– более дорогое расширение системы хранения данных;

– невозможность обеспечения высокой безопасности копий.

3. Сетевые технологии.

Сетевое хранение данных построено на трех фундаментальных компонентах: коммутации, хранении и файлах. Все продукты хранения можно представить в виде комбинации функций данных компонентов. Поначалу это может вызвать замешательство: поскольку продукты хранения разрабатывались по совершенно разным направлениям, функции часто перекрывают друг друга.

В сети работает множество приложений типа «клиент-сервер» и различных видов распределенных приложений, но в то же время хранение является уникальным и специализированным типом приложения, которое может функционировать в нескольких сетевых средах. Поскольку процессы хранения тесно интегрированы с сетями, будет уместно напомнить, что

сетевые хранилища представляют собой системные приложения. Сервисами, которые предоставляются сетевыми приложениями хранения, могут пользоваться сложные корпоративные программы и пользовательские приложения. Как и в случае со многими технологиями, некоторые типы систем лучше отвечают требованиям сложных приложений высокого уровня.

Термин «коммутация» применяется ко всему программному и аппаратному обеспечению и к службам, которые обеспечивают транспортировку хранения и управление ею в сетевом хранилище. Сюда входят такие различные элементы, как разводка кабелей, сетевые контроллеры ввода-вывода, коммутаторы, концентраторы, аппаратура выборки адресов, контроль связи данных, транспортные протоколы, безопасность и резервы ресурсов. В сетевых хранилищах все еще широко используются технологии шин данных SCSI и ATA, и, скорее всего, они будут использоваться еще долго. Фактически продукты SCSI и ATA сегодня применяются гораздо чаще в технологии NAS. Существуют два важных различия между сетями хранения SAN и обычными локальными сетями LAN. Сети хранения SAN автоматически синхронизируют данные между отдельными системами и хранилищами. В сетевых хранилищах необходимы компоненты высокой степени точности для обеспечения надежной и предсказуемой среды. Несмотря на ограничения по расстоянию, параллельная SCSI -- чрезвычайно надежная и предсказуемая технология. Если новые технологии коммутации, такие как Fibre Channel, Ethernet и InfiniBand, сменят SCSI, они должны будут продемонстрировать аналогичный или лучший уровень надежности и предсказуемости. Имеется и такая точка зрения, которая рассматривает коммутацию как канал хранилища. Сам термин «канал», берущий свое начало в среде больших вычислительных машин, предполагает высокую надежность и работоспособность.

Хранение в основном затрагивает блочные операции адресного пространства, включая создание виртуальной среды, когда адреса

логического блока хранения отображаются из одного адресного пространства в другое. Вообще говоря, в сетевых хранилищах функция хранения почти не изменилась, если не считать двух заметных отличий. Первое -- это возможность нахождения технологий виртуализации устройства, например управление устройством внутри оборудования сетевого хранения. Этот вид функции иногда называют контроллером домена хранения или виртуализацией LUN. Второе главное отличие хранения заключается в масштабируемости. Продукты хранения, такие как подсистемы хранения, имеют значительно больше контроллеров/интерфейсов, чем предыдущие поколения шинной технологии, а также намного больший объем хранения.

Функция организации файлов представляет абстрактный объект конечному пользователю и приложениям, а также организует разметку данных на реальных или виртуальных устройствах хранения. Основную часть функциональности файлов в сетевых хранилищах обеспечивают файловые системы и базы данных; их дополняют приложения управления хранением, например операции резервного копирования, также являющиеся файловыми приложениями. Сетевое хранение к настоящему времени почти не изменило файловые функции, за исключением разработки файловых систем NAS, в частности файловой системы WAFL компании Network Appliance. Кроме упомянутых технологий хранения данных NAS и SAN, ориентированных на крупные и глобальные сети, в небольших локальных сетях доминирующее положение занимает технология DAS, в соответствии с которой хранилище находится внутри сервера, обеспечивающего объем хранилища и необходимую вычислительную мощность.

Простейшим примером DAS может служить накопитель на жестком диске внутри персонального компьютера или ленточный накопитель, подключенный к единственному серверу. Запросы ввода-вывода (называемые также командами или протоколами передачи данных) непосредственно обращаются к этим устройствам. Однако такие системы плохо масштабируются, и компании с целью расширения объема хранилища

вынуждены приобретать дополнительные серверы. Эта архитектура очень дорогая и может использоваться только для создания небольших по объему хранилищ данных.

Технология RAID.

RAID (избыточный массив недорогих / независимых дисков) - это технология, используемая для защиты данных в случае отказа диска. Эта технология имеет несколько уровней, из которых каждый защищает данные по-разному.

RAID может быть реализован с помощью аппаратного или программного обеспечения, либо их комбинации. Аппаратный RAID обычно проще в использовании, потому что он предоставляет его сразу после запуска аппаратного устройства.

Программный RAID использует программное обеспечение, что означает нагрузку на процессор.

RAID 0.

RAID 0 - это просто комбинация нескольких дисков в один блок (рис. 1). Фактически эта технология служит только для увеличения производительности дисководов, при этом вероятность выхода из строя увеличивается, потому что есть больше юнитов, которые могут выйти из строя и сделать недоступными определенную часть данных. Для реализации RAID 0 требуется минимум два диска. Лучшая производительность достигается, когда у каждого устройства есть собственный контроллер, даже если в этом нет необходимости.

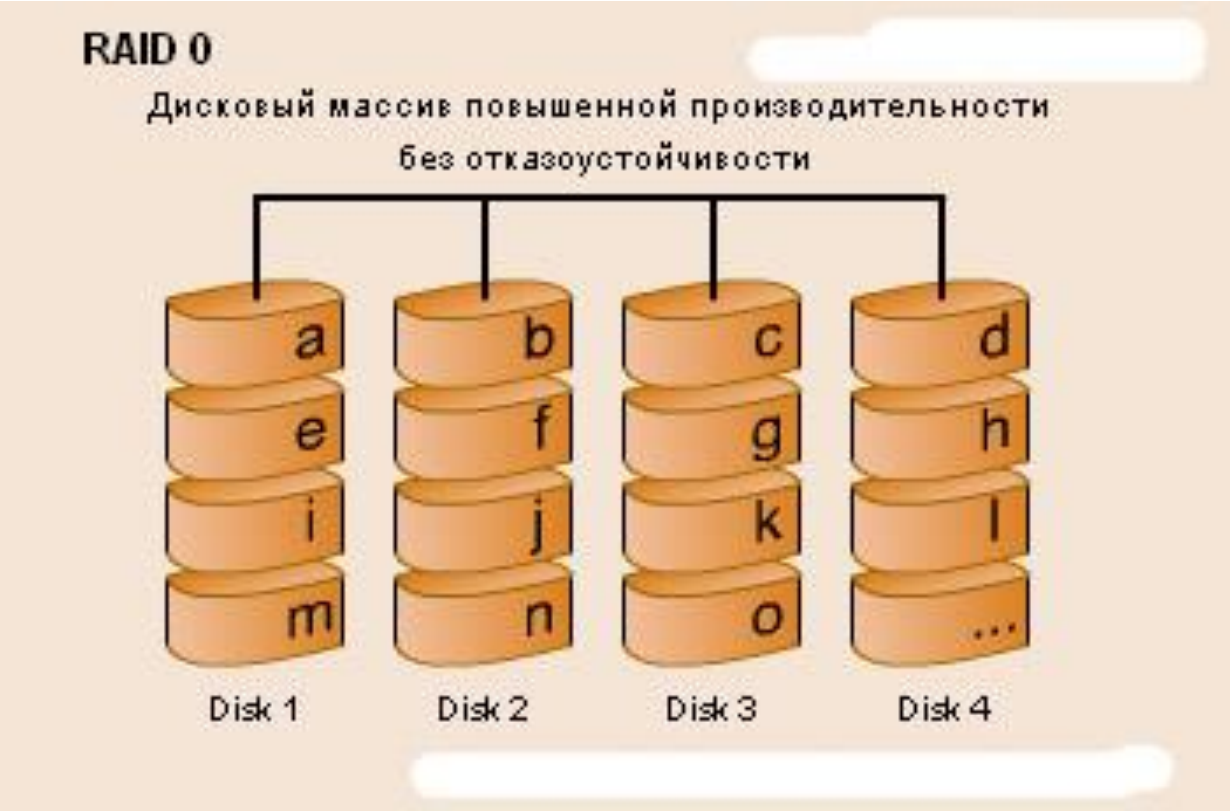

Рисунок 1 – RAID 0

RAID 1.

RAID 1, часто также называемый зеркалированием, повторяет запись с одного диска на другой диск. Это увеличивает отказоустойчивость, так как под рукой есть текущая резервная копия. Выход из строя одного из дисков, что является одним из наиболее частых отказов оборудования RAID 1, не является критичной проблемой, так как достаточно заменить поврежденный диск и диски снова синхронизируются. Скорость записи здесь слабее, потому что данные записываются в большее количество секторов одновременно. Для реализации RAID 1 требуется минимум два диска (рис. 2).

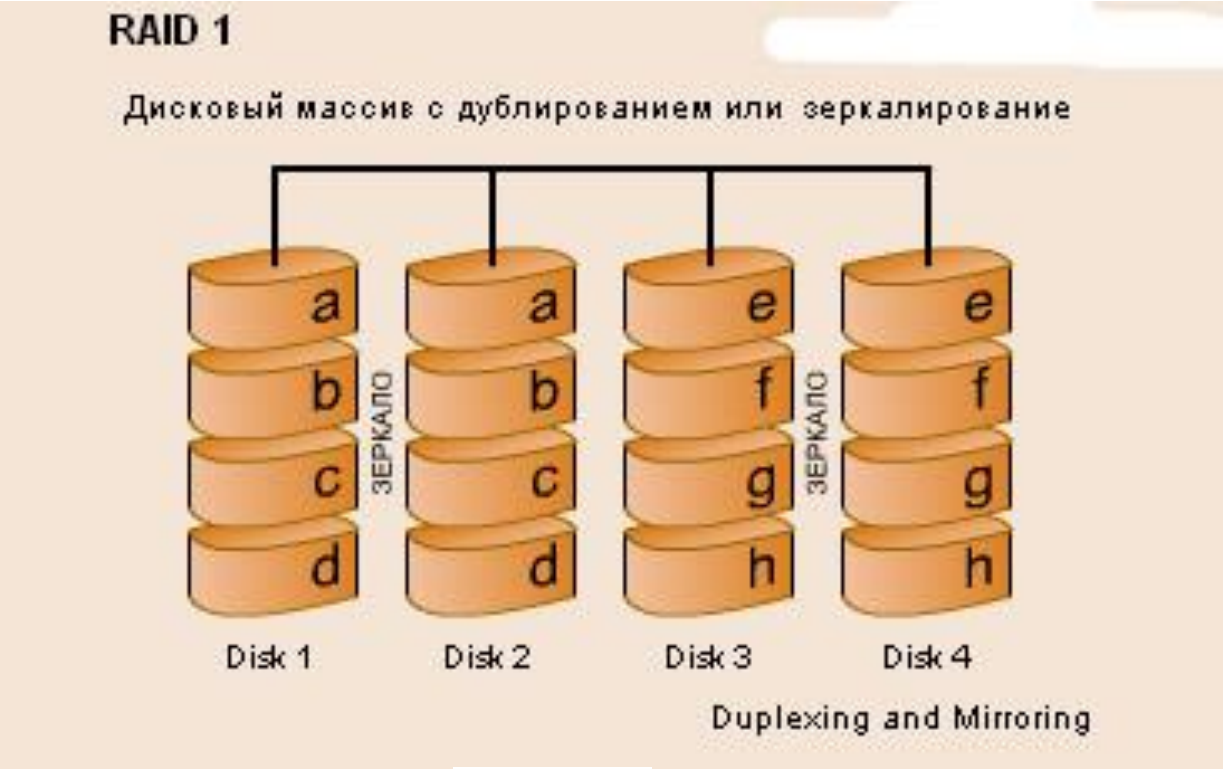

Рисунок 2 – RAID 1

RAID 2.

RAID 2 - отказоустойчивый дисковый массив с использованием кода Хемминга Hamming Code ECC (рис. 3).

RAID 2 - использует коды исправления ошибок Хемминга (Hamming Code ECC). Коды позволяют исправлять одиночные и обнаруживать двойные неисправности.

Преимущества:

– быстрая коррекция ошибок («на лету»);

– очень высокая скорость передачи данных больших объемов;

– при увеличении количества дисков, накладные расходы уменьшаются;

– достаточно простая реализация.

Недостатки:

– высокая стоимость при малом количестве дисков;

– низкая скорость обработки запросов (не подходит для систем ориентированных на обработку транзакций).

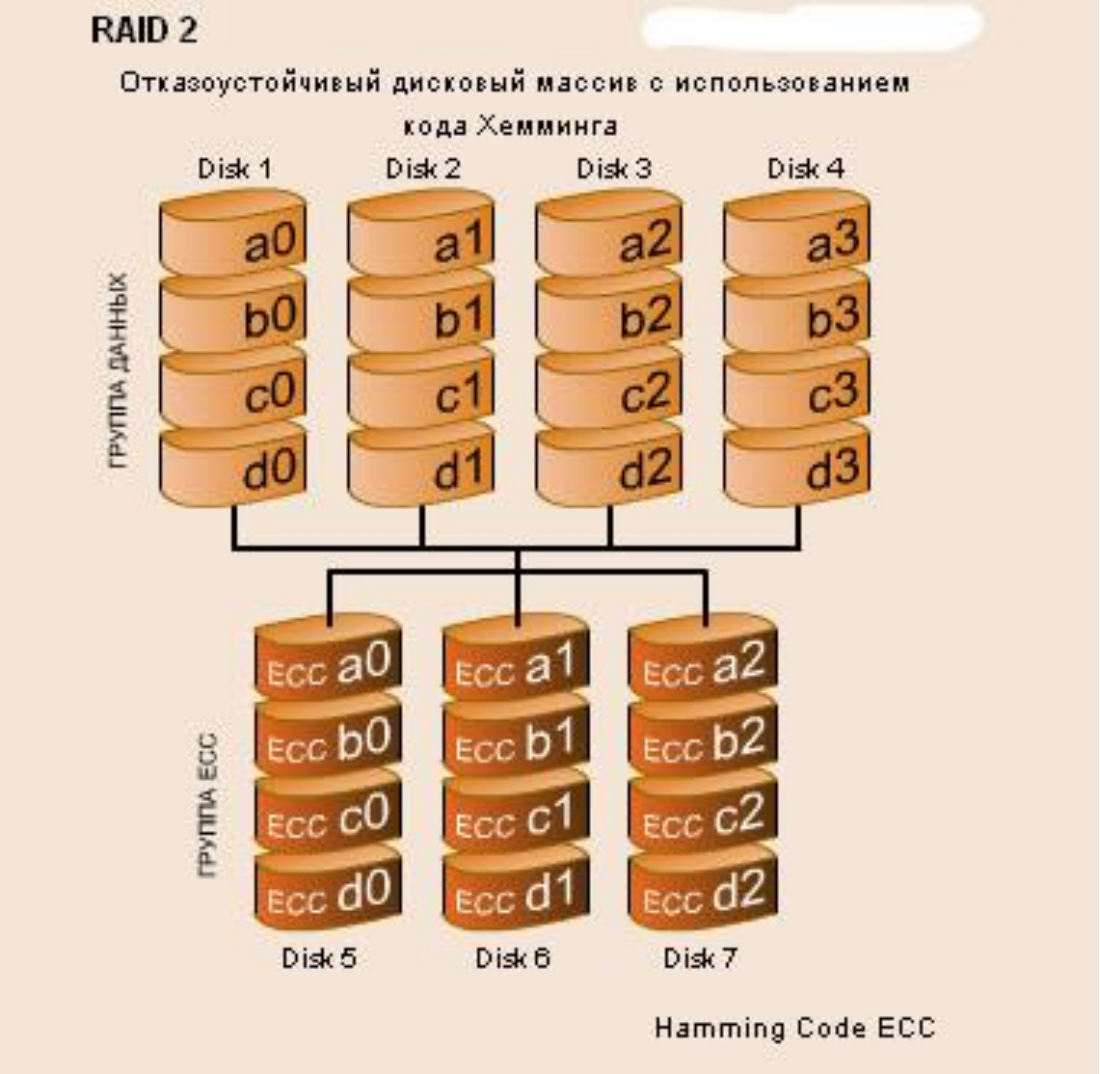

Рисунок 3 – RAID 2

RAID 3.

Отказоустойчивый массив с параллельной передачей данных и четностью Parallel Transfer Disks with Parity.

RAID 3 - данные хранятся по принципу striping на уровне байтов с контрольной суммой на одном из дисков (рис. 4). Массив не имеет проблему некоторой избыточности как в RAID 2-го уровня. Диски с контрольной суммой используемые в RAID 2, необходимы для определения ошибочного заряда. Однако большинство современных контроллеров способны определить, когда диск отказал при помощи спец сигналов или дополнительного кодирования информации, записанной на диск и используемой для исправления случайных сбоев.

Преимущества:

– очень высокая скорость передачи данных;

– отказ диска мало влияет на скорость работы массива;

– малые накладные расходы для реализации избыточности.

Недостатки:

– непростаяреализация;

– низкая производительность при большой интенсивности запросов данных небольшого объема.

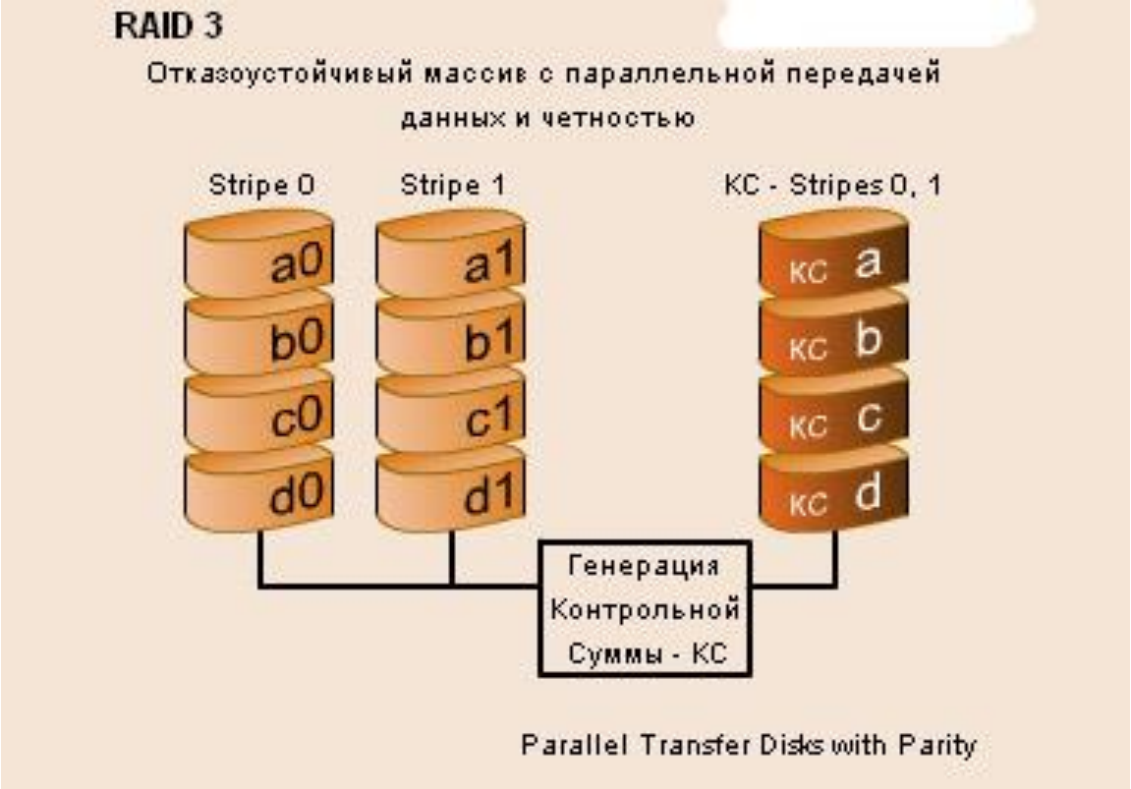

Рисунок 4 – RAID 3

RAID 4.

RAID 4 - это решение, очень похожее на RAID 3. Он отличается от RAID 3 тем, что читает на уровне блока вместо байтов. Показания менее одного блока обычно очень быстрые и обычно эта скорость увеличивается с каждой добавленной единицей. Для реализации RAID 4, как и в случае с RAID 3, требуется минимум три диска.

RAID 5.

RAID 5 похож на RAID 4. Он также позволяет разбивать на разделы и записывать данные для исправления ошибок, которые приводят к

повышению производительности и отказоустойчивости. Данные о четности хранятся на каждом блоке. Скорость записи выше, чем у RAID 4, а скорость чтения наоборот медленнее, потому что информация о четности занимает место на каждом блоке, и эти данные необходимо пропускать при чтении.

RAID 5 очень подходит для серверов баз данных. Для реализации RAID 5 требуется минимум три диска

RAID 10.

RAID 10 представляет собой комбинацию RAID 1 и RAID 0. Он предлагает все преимущества в производительности разделения и также повысить отказоустойчивость за счет зеркалирования. Минус здесь - более высокая цена, поскольку реализация этого варианта требует использования как минимум четырех дисков. RAID 10 подходит для серверов баз данных, поскольку обеспечивает высокую производительность и отказоустойчивость.

RAID 0 + 1.

Вариант RAID 0 + 1 часто путают с вариантом RAID 10. RAID 10 - это многораздельный массив. диски с зеркальными сегментами, где RAID 0 + 1 - зеркальный массив сегментированные единицы. Этот вариант подходит в ситуациях, когда больше делается упор на производительность, чем на надежность. Как и RAID 10, это решение относительно дорогое и для реализации требуется минимум четыре диска.

1.3 Программно-технические средства резервного копирования

Существующие в настоящее время программы резервного копирования избавляют пользователей и системных администраторов от необходимости «вручную» отслеживать периодичность создания и обновления резервных копий, замены носителей и т. п. Правда, перечень предоставляемых такими программами сервисных возможностей существенно зависит от категории программы.

Все программы резервного копирования можно условно разделить на три категории:

1. Системы начального уровня, включаемые в состав операционных систем. К ним можно также отнести большинство бесплатных и условно-бесплатных программ резервного копирования. Эти программы предназначены для индивидуальных пользователей и небольших организаций.

2. Системы среднего уровня; при относительно невысокой цене они обладают широкими возможностями по резервному копированию и архивации данных. Подобных систем довольно много (в частности, ARCserveIT компании Computer Associates, Backup Exec от Seagate Software и Net Worker компании Legato Systems).

3. Системы верхнего уровня предназначены для резервного копирования и архивирования в сложных гетерогенных средах. Они поддерживают разнообразные аппаратные платформы, операционные системы, базы данных и приложения корпоративного уровня, имеют средства интеграции с системами управления сетью и обеспечивают возможность резервного копирования/архивирования с использованием разнообразных типов накопителей. К подобным системам можно отнести ADSM компании ЮМ и OpenView OmniBack II от Hewlett Packard. Однако для многих организаций (не говоря уже об индивидуальных пользователях) они весьма дороги.

Одной из важных характеристик программ резервного копирования является перечень поддерживаемых типов сменных носителей. Вместе с тем, при создании резервной копии в «ручном» режиме, можно использовать любое из существующих на сегодняшний день устройств хранения данных. Перечень с краткой характеристикой приведен в таблице 1.

Таблица 1 – Устройства хранения данных, применяемые при резервном копировании

Тип устройства	Достоинства	Недостатки
Жесткий диск (HDD)	емкость, быстродействие, высокая надежность, долговечность, многократная перезапись, низкая стоимость, возможность загрузки резервной копии	Ненадежность при транспортировке, воздействие ЭМ излучений, (подключение ..)
CD-R, CD-RW	Приемлемое быстродействие и скорость, н. стоимость, надежность, долговечность	Емкость, не все виды ПК оснащены
DVD	Большая емкость, тоже что CD	Специализация, не все виды ПК оснащены
Карты памяти SD, MS, (CF), MMC	Емкость, скорость, надежность, приемлемое быстродействие и скорость, возможность использования для переноса между разнотипными устройствами	
Модули флеш памяти	То же	
Внешний жесткий Диск Mobile Rack, Стример, флоппи, ZIP, ZIV, магнитооптические	USB	

Программы для резервного копирования позволяют сохранять любую информацию на вашем персональном компьютере или сервере, а так позволяют поднять на новый уровень безопасность корпоративной сети. Вот краткий перечень документов, программ и настроек, которые можно резервировать и восстанавливать с помощью бэкап приложений:

1. Операционная система и все системные настройки, включая настройки и содержимое рабочего стола, документы, записи регистра. С помощью программы можно создавать образ жесткого диска и восстанавливать систему полностью.

2. Электронная почта, то есть учетные записи, письма, структура папок, адресные книги и любые другие элементы. Так же можно резервировать серверные системы управления корпоративной электронной почтой.

3. Базы данных и системы управления базами данных. Многие базы данных можно резервировать без остановки сервера.

4. Приложения для обмена мгновенными сообщениями и IP-телефонии.

5. Популярные приложения и их настройки. Например, графические пакеты Adobe Photoshop и Corel Draw.

Программы резервного копирования позволяют легко управлять данными, всегда поддерживая копии в актуальном состоянии. Они смогут выручить вас даже при полном отказе жесткого диска, а также при разрушительном действии вирусов или ошибочном удалении файлов. С их помощью также упрощается процесс переноса данных с одного жесткого диска на другой.

Хорошие программы резервного копирования сжимают данные для экономии места на диске и предоставляют следующие функции резервного копирования, такие как планировщик, возможность шифрования данных и дополнительную защиту бэкапа паролем.

True Image Home, разработчик Acronis, давно является лидером среди программ резервного копирования. При создании образа или резервных копий отдельных файлов этот продукт работает очень скрупулезно.

Достоинства: имеет расширенные возможности планировщика и возможны все способы резервного копирования.

Недостатки: нет поддержки записи на DVD-RW и Blue-ray-диски, а также необходима обязательная регистрация обновлений программы.

BackltUp & Burn, разработчик Nero, позволяет создавать полные резервные копии жестких дисков и разделов.

Достоинства: расширенные возможности планировщика и встроенная программа для записи дисков.

Недостатки: отсутствует возможность обновления образа путем дифференциального или инкрементного копирования.

Backup & Recoveri 10 Suite, разработчик Paragon - Software, копирование всего жесткого диска и отдельных файлов и папок делает одинаково хорошо, но имеет запутанный интерфейс.

Достоинства: расширенные возможности планировщика.

Недостатки: нет функции шифрования резервной копии и не поддерживает инкрементное резервное копирование.

Perfekt Image 12, разработчик Awanquest, создает только полный или дифференциальный образ жесткого диска.

Достоинства: расширенные возможности планировщика.

Недостатки: нет возможности просмотра файлов в созданном образе и необходимость обязательной регистрации.

R - Drive Image 4.6, разработчик Drive Image, может восстанавливать отдельные файлы, извлекая их из образа.

Достоинства: высокая степень сжатия резервных копий и расширенные возможности планировщика.

Недостатки: нет функции создания резервных копий отдельных файлов и необходимость обязательной регистрации.

NovaBACKUP 11, разработчик Novastor, имеет сложный интерфейс.

Достоинства: эффективное резервное копирование дисков и разделов.

Недостатки: нет возможности создания дифференциального и инкрементного образов, обязательная регистрация и высокая цена.

DiskImage 4.1, разработчик Oo - software, хорошо копирует образы и восстанавливает файлы из них и имеет низкую стоимость.

Достоинства: расширенные возможности планировщика.

Недостатки: нет функции создания резервных копий отдельных файлов и папок и низкая скорость работы при высокой степени сжатия.

ShadowProtekt Desktop Edition 3.5, разработчик Storagecraft, может найти отдельные файлы и восстановить их из образа.

Достоинства: высокая скорость работы.

Недостатки: необходимость обязательной регистрации, высокая стоимость и нет функции создания резервных копий отдельных файлов и папок.

Таким образом, существует множество программ резервного копирования. Кроме того, было рассмотрено 8 таких программ. Все они

имеют свои достоинства и недостатки по сравнению друг с другом. Такие программы находят широкое применение как в домашних условиях, так и в образовательных организациях. В основном эти программы распространяются за деньги, правда, некоторые компании, производящие данный продукт распространяют бесплатные версии своих программ в качестве рекламы. В этом случае такие рекламные версии имеют ограниченный срок действия и очень ограниченный функционал. Но существую программы распространяемые абсолютно бесплатно.

Среди программ для резервного копирования без труда можно выбрать ту, которая подойдет конкретному пользователю, в зависимости от решаемых им задач. Но каким именно продутом все-таки воспользоваться, должен решить сам пользователь.

При выборе продукта резервного копирования необходимо выполнить анализ информационной системы заказчика с целью определения факта необходимости использования, в силу действующего законодательства, сертифицированного продукта резервного копирования. Использование сертифицированных продуктов позволяет снизить расходы заказчика на оценку соответствия своей информационной системы в целом, так как в отношении сертифицированного продукта не требуется проводить оценочные испытания в составе информационной системы.

Выводы по главе 1

По итогам первой главы магистерской диссертации можно сделать следующие выводы.

Дано определение понятия «система резервного копирования» и выделены её основные функции. Система резервного копирования – это программный или программно-аппаратный комплекс для создания копий данных с определенной периодичностью для их последующего восстановления и выполняющий следующие функции: защиту от потери

критически важной информации; быстрое восстановление, как отдельных данных, так и всей системы полностью.

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

Описаны технологии резервного копирования и хранения резервных копий и данных.

Проанализированы программно-технические средства резервного копирования.

Все программы резервного копирования можно условно разделить на три категории:

1. Системы начального уровня, включаемые в состав операционных систем. К ним можно также отнести большинство бесплатных и условно-бесплатных программ резервного копирования. Эти программы предназначены для индивидуальных пользователей и небольших организаций.

2. Системы среднего уровня; при относительно невысокой цене они обладают широкими возможностями по резервному копированию и архивации данных.

3. Системы верхнего уровня предназначены для резервного копирования и архивирования в сложных гетерогенных средах. Они поддерживают разнообразные аппаратные платформы, операционные системы, базы данных и приложения корпоративного уровня, имеют средства интеграции с системами управления сетью и обеспечивают возможность резервного копирования/архивирования с использованием разнообразных типов накопителей.

При выборе продукта резервного копирования необходимо выполнить анализ информационной системы заказчика с целью определения факта необходимости использования, в силу действующего законодательства, сертифицированного продукта резервного копирования. Использование

сертифицированных продуктов позволяет снизить расходы заказчика на оценку соответствия своей информационной системы в целом, так как в отношении сертифицированного продукта не требуется проводить оценочные испытания в составе информационной системы.

ГЛАВА 2 АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГБПОУ «ЧЕЛЯБИНСКИЙ ТЕХНИКУМ ПРОМЫШЛЕННОСТИ И ГОРОДСКОГО ХОЗЯЙСТВА ИМЕНИ Я.П. ОСАДЧЕГО»

2.1 Общие сведения о ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего»

Базой исследования является Государственное бюджетное профессиональное образовательное учреждение «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего», располагающегося по адресу: 454129, Российская Федерация, Уральский федеральный округ, город Челябинск, ул. Масленникова, 21.

Структура управления техникума относится к линейно-функциональной, то есть к такой структуре, где связи и отношения субъектов характеризуются одновременно и субординацией, и координацией. Непосредственное управление учреждением осуществляет директор.

Директор — Худолей Елена Сергеевна.

Структура управления ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего» представлена на рисунке 5.

Рисунок 5 – Структура управления ГБПОУ «ЧТПиГХ имени Я.П. Осадчего»

ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего» представляет собой комплекс из нескольких зданий различного назначения: два учебных корпуса, учебно-производственные мастерские, общежитие для студентов.

В ЧТПиГХ имеются следующие лаборатории и мастерские**:** лаборатория технического обслуживания и ремонта автомобилей и двигателей внутреннего сгорания, электрооборудования автомобилей; лаборатория – учебный кулинарный цех, учебный кондитерский цех, технологического оборудования кулинарного и кондитерского производства; лаборатория по профессии «Мастер по обработке цифровой информации»; лаборатория Электротехники с основами электроники; лаборатория технических измерений, и инженерной графики; лаборатория товароведения продовольственных товаров; слесарная мастерская; сварочная № 1, № 2; электромонтажная мастерская.

Учебные корпуса техникума (ул. Масленникова, 21 и Энергетиков, 2) оснащены столовыми. Обе столовые рассчитаны на 120 мест. На сегодняшний день техникум располагает тремя общежитиями, рассчитанными на 536 человек.

Профессии и специальности ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего».

В настоящее время в техникуме работает 118 человек, в том числе 56 педагогических работников. Контингент обучающихся составляет 882 человека, обучающихся по десяти программам, в т.ч. две из числа наиболее востребованных и перспективных на современном рынке труда ТОП-50.

Номенклатура программ базового образования согласно лицензии представлена в таблице 2.

Таблица 2 – Программы подготовки квалифицированных рабочих кадров и специалистов среднего звена

КОД специальности	Наименование специальности, профессии
46.01.03	Делопроизводитель
19.01.17	Повар. Кондитер
15.01.05	Сварщик (ручной и частично механизированной сварки (наплавки)
19.01.03	Мастер по обработке цифровой информации
19.01.03	Монтажник сантехнических, вентиляционных систем и оборудования
18.02.07	Монтаж и эксплуатация внутренних сантехнических устройств, кондиционирования воздуха и вентиляции
23.02.03	Техническое обслуживание и ремонт автомобильного транспорта
19.02.10	Технология продукции общественного питания
08.02.08	Монтаж и эксплуатация оборудования и систем газоснабжения

На базе техникума действует ресурсный центр по подготовке рабочим профессиям. Перечень программ дополнительного образования, по которым идет обучение в ресурсном центре, представлен в таблице 3.

Таблица 3 – Программы дополнительного образования

№ п/п	Код	Наименование	Уровень	Срок обучения	Квалификация
1	**2**	**3**	**4**	**5**	**6**
1	16199	Оператор ЭВМ	Профессиональная подготовка	5 месяцев	2 разряд
			Переподготовка	2,5 месяцев	2 разряд
			Повышение квалификации	80 часов	3,4 разряды
2	18560	Слесарь-сантехник	Профессиональная подготовка	4 месяцев	2 разряд
			Переподготовка	2 месяцев	2 разряд
			Повышение квалификации	80 часов	3-6 разряды
3	19149	Токарь	Профессиональная подготовка	5 месяцев	2 разряд
			Переподготовка	2,5 месяцев	2 разряд
			Повышение квалификации	80 часов	3-6 разряды

Продолжение таблицы 3

4	16675	Повар	Профессиональная подготовка	5 месяцев	2 разряд
			Переподготовка	2,5 месяцев	2 разряд
			Повышение квалификации	80 часов	3-6 разряды
5	12901	Кондитер	Профессиональная подготовка	5 месяцев	2 разряд
			Переподготовка	2,5 месяцев	2 разряд
			Повышение квалификации	80 часов	3-6 разряды
6	18554	Слесарь по эксплуатации и ремонту газового оборудования	Профессиональная подготовка	4 месяцев	2 разряд
			Переподготовка	2 месяцев	2 разряд
			Повышение квалификации	80 часов	3-5 разряды
7	19756	Электрогазосварщик	Профессиональная подготовка	6 месяцев	2 разряд
			Переподготовка	3 месяцев	2 разряд
			Повышение квалификации	80 часов	3-6 разряды
8	18511	Электромонтёр по ремонту и обслуживанию электрооборудования	Профессиональная подготовка	5 месяцев	2,3 разряды
			Переподготовка	2,5 месяцев	2,3 разряды
			Повышение квалификации	80 часов	3-6 разряды
9	18559	Слесарь-ремонтник	Профессиональная подготовка	5 месяцев	2 разряд
			Переподготовка	2,5 месяцев	2 разряд
			Повышение квалификации	80 часов	3-7 разряды
10	11176	Бармен	Переподготовка	160 часов	4 разряд
			Повышение квалификации	80 часов	5 разряд
11	16399	Официант	Профессиональная подготовка	4 месяцев	3 разряд
			Переподготовка	2 месяцев	3 разряд
			Повышение квалификации	80 часов	4,5 разряды

Продолжение таблицы 3

12	18466	Слесарь механосборочных работ	Профессиональная подготовка	5 месяцев	2 разряд
13	18809	Станочник широкого профиля	Профессиональная подготовка	5 месяцев	2,3 разряды
			Переподготовка	2,5 месяцев	2,3 разряды
			Повышение квалификации	80 часов	разряд
			Переподготовка	2 месяцев	2 разряд
14	19479	Фрезеровщик	Профессиональная подготовка	5 месяцев	2 разряд
			Переподготовка	2 месяцев	2 разряд

В настоящее время подготовка специалистов осуществляется по очной форме обучения:

Подготовка квалифицированных рабочих кадров:

– 46.01.03 Делопроизводитель;

– 19.01.17 Повар. Кондитер;

– 15.01.05 Сварщик (ручной и частично механизированной сварки (наплавки); - 19.01.03 Мастер по обработке цифровой информации;

– 19.01.03 Монтажник сантехнических, вентиляционных систем и оборудования.

Подготовка специалистов среднего звена:

– 18.02.07 Монтаж и эксплуатация внутренних сантехнических устройств, кондиционирования воздуха и вентиляции;

– 23.02.03 Техническое обслуживание и ремонт автомобильного транспорта;

– 19.02.10 Технология продукции общественного питания;

– 18.02.08 Монтаж и эксплуатация оборудования и систем газоснабжения.

В образовательном процессе ЧТПиГХ им. Я.П. Осадчего используются такие средства обучения и воспитания, как:

1. Печатные (учебники и учебные пособия, книги для чтения, хрестоматии, рабочие тетради, атласы, раздаточный материал, энциклопедии, словари и др.).

2. Электронные образовательные ресурсы (образовательные мультимедийные учебники, сетевые образовательные ресурсы, мультимедийные универсальные энциклопедии и т.п.).

3. Аудиовизуальные (презентации, слайд – фильмы, видеофильмы образовательные, учебные кинофильмы, учебные фильмы на цифровых носителях и др.).

4. Наглядные плоскостные (плакаты, карты настенные, иллюстрации настенные, магнитные доски и др.).

5. Демонстрационные (муляжи, макеты, стенды, модели в разрезе, модели демонстрационные и др.)

В техникуме имеются следующие средства обучения и воспитания, достаточные для организации образовательного процесса в соответствии с обязательными требованиями.

В техникуме проводится систематическая работа по расширению и обновлению компьютерного парка, разработке и внедрению программно-информационного обеспечения учебного процесса.

В техникуме оборудовано 4 компьютерных аудитории. Программное обеспечение, используемое в учебном процессе, основано как на требованиях ГОС СПО, так и требованиях высокотехнологичных производств и компьютеризации управленческой деятельности базового предприятия и организаций города, на которых проходят производственную практику обучающиеся и включает:

- операционную систему Windows;
- операционную систему MS DOS;
- операционную оболочку NC;
- операционную оболочку FAR;
- антивирусные программы Dr.Web, Sp|DerGuard;

– архиваторы MS RAR, WIN RAR;

– программное обеспечение Microsoft Word;

– электронные таблицы Excel;

– процессор презентаций Power Point.

В техникуме имеются мультимедийные проекторы, телевизоры. В учебном процессе используется интерактивные доски, переносные мультимедийные проекторы, обеспечение бесплатным выходом в Интернет.

Оснащенность учебных помещений вычислительной техникой - 82%.

Локальная вычислительная сеть (ЛВС): имеется.

Характеристики:

1. Физическая среда: кабель UTP5, Ethernet.
2. Транспортный уровень передачи информации - протокол TCP/IP.
3. Логическая организация ЛВС - рабочие группы MS Windows.
4. Средство обмена файлами и сетевой печати - протокол SMB.
5. Подключение к интернет – есть.
6. Эффективность использования сети - 55-60%.

Количество аудиторий, обеспеченных АРМ (компьютер, проектор, выход в интернет) – 25 шт.

Количество разработанных электронных образовательных ресурсов – 28 шт.

Техникум располагает также фондом информационных ресурсов в количестве 180 экз. и подписан на виртуальный абонемент ЧОУНБ (2 доступа), всероссийский методический интернет-портал «Росметод», ЭБС IPRbooks.

Таким образом, информационно-методические материалы по реализуемым образовательным программам среднего профессионального образования соответствуют требованиям федеральных государственных образовательных стандартов среднего профессионального образования по профессиям и специальностям.

2.2 Анализ информационных систем в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего»: структура, функционирование, средства защиты

В ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» действует политика обработки и защиты персональных данных.

При обработке персональных данных в Техникуме соблюдаются конституционные права и свободы человека и гражданина на неприкосновенность частной жизни, личную и семейную тайну.

Персональные данные субъектов в Техникуме обрабатываются как на бумажных носителях, так и в электронном виде - в компьютерных программах и электронных базах данных (в ИСПДн) с передачей по локальной компьютерной сети и по сети Internet.

Безопасность персональных данных достигается путем обеспечения их конфиденциальности, целостности и доступности.

В Техникуме функционирует комплексная система защиты персональных данных, которая включает:

1. Организационные мероприятия

- действующие организационно-распорядительные документы по защите ПДн, регламентирующие порядок обработки ПДн и ответственность должностных лиц;
- осуществление внутреннего периодического контроля;
- учет машинных носителей персональных данных;
- физическая охрана зданий и помещений;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- обучение сотрудников вопросам защиты ПДн.

2. Технические меры защиты

- модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- техническое задание для ИСПДн, содержащее требования к системе защиты;
- подсистема резервного копирования информации;
- подсистема парольной защиты;
- подсистема антивирусной защиты;
- подсистема криптографической защиты;
- средства защиты информации от несанкционированного доступа;
- средства межсетевого экранирования;
- сейфы и запирающиеся шкафы для хранения носителей персональных данных;
- пожарная и охранная сигнализация.

Допуск к персональным данным субъекта имеют только те сотрудники Техникума, которым персональные данные необходимы в связи с исполнением ими своих служебных (трудовых) обязанностей.

Каждый сотрудник имеет доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения служебных (трудовых) обязанностей.

В состав информационных систем персональных данных ГБПОУ «Челябинский техникум промышленности и городского хозяйства им. Я.П. Осадчего» входит: 1С:Колледж, 1С:Зарплата и кадры 8.2, 1С Предприятие 8.3, Контур-Экстерн, официальный сайт учреждения http://chtpgh.ru/.

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно- вычислительные комплекты и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации, применяемые в информационных системах.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение,

блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Средства защиты информации, применяемые в информационных системах, в обязательном порядке проходят процедуру оценки соответствия в установленном законодательством РФ порядке.

Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер, а также применения технических и (или) программных средств.

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Безопасность персональных данных при их обработке в информационной системе персональных данных обеспечивает специалист, ответственный за организацию обработки информационных систем персональных данных.

При обработке персональных данных в информационной системе должно быть обеспечено:

– проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

– своевременное обнаружение фактов несанкционированного доступа к персональным данным;

– недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

– возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– постоянный контроль над обеспечением уровня защищенности персональных данных.

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают:

– определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

– проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

– установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

– обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

– учет лиц, допущенных к работе с персональными данными в информационной системе;

– контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документации;

– разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

– описание системы защиты персональных данных.

Иные требования по обеспечению безопасности информации и средств защиты информации в ГБПОУ «Челябинский техникум промышленности и городского хозяйства им. Я.П. Осадчего» выполняются в соответствии с требованиями федеральных органов исполнительной власти и органов исполнительной власти Челябинской области.

В ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» эксплуатируются следующие информационные системы персональных данных (далее - ИСПДн) с использованием средств криптографической защиты информации (далее - СКЗИ, криптосредства):

1. ИСПДн «Бухгалтерия и кадры» в составе следующих подсистем:

- «Система дистанционного банковского обслуживания «Клиент-Банк», АО «Уральский банк реконструкции и развития» (далее - СДБО «Клиент-Банк УБРиР»);

- «Информационная система электронного документооборота «Интернет отчетность - Контур-Экстерн» (далее - ИС ЭДО «Контур-Экстерн»).

Для ИСПДн «Бухгалтерия и кадры» разработана ООО «СИБ Альпикс» и утверждена директором ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» «Модель угроз безопасности персональных данных ...» № СИБА.МУ.59 от 09.06.2016.

2. ИСПДн «ФИС ГИА и Приема».

Для ИСПДн «ФИС ГИА и Приема» разработана ООО «СИБ Альпикс» и утверждена директором ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» «Модель угроз безопасности персональных данных ...» № СИБА.МУ.61 от 09.06.2016.

Документы обучающихся вносятся в 1С:Колледж, Контур-Экстерн.

Согласно актам определения уровня защищенности ИСПДн «Бухгалтерия и кадры» и «ФИС ГИА и Приема», №№ б/н от 28.06.2016, комиссия установила:

- ИСПДн являются информационными системами, обрабатывающими иные категории персональных данных (менее чем 100 000 субъектов персональных данных);

- для ИСПДн актуальны угрозы 3-го типа;

- 4-ый уровень защищенности персональных данных при их обработке в ИСПДн.

Для защиты информации в ИСПДн ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» используются следующие СКЗИ:

- ПАК «ViPNet Terminal 3.0», сертификат соответствия ФСБ России имеется;

- ПАК «КриптоПро CSP» версии 3.6, сертификат соответствия ФСБ России имеется.

Схема информационных потоков в ИСПДн представлена в таблице 4.

Таблица 4 – Схема информационных потоков в ИСПДн

Субъекты ПДн	Цели обработки	Категории ПДн	Правовые основания обработки
Сотрудники Техникума	Реализация трудовых отношений, начисление заработной платы, передача информации в налоговые органы. Пенсионный Фонд	– фото; – фамилия, имя, отчество; – паспортные данные; – дата и место рождения; – сведения о месте регистрации, проживания; – контактная информация (телефон домашний, телефон мобильный, e-mail); – сведения об образовании; – семейное положение (состав семьи, копия св-ва о браке, копия св-в о рождении детей);	Гражданский кодекс РФ от 30.11.1994 № 51-ФЗ; Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ; Налоговый Кодекс РФ часть первая от 31 июля 1998 г. № 146-ФЗ и часть вторая от 5 августа 2000 г. № 117-ФЗ; Согласие на обработку персональных данных

Продолжение таблицы 4

Кандидаты на вакантную должность	Принятие решения о трудоустройстве, формирование кадрового резерва	– фамилия, имя, отчество; – дата; – контактная информация (телефон мобильный, e-mail); – сведения об образовании; – опыт работы.	Согласие на обработку персональных данных
Практиканты	Прохождение практики (учебной, производственной)	– фамилия, имя. отчество; – контактная информация (телефон мобильный); – сведения об месте учебы.	Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ; Согласие на обработку персональных данных

В случаях, когда на виртуальных машинах обрабатывается информация ограниченного доступа, не относящаяся к государственной тайне, в обязательном порядке должны выполняться требования законодательства РФ к используемому программному обеспечению, выполняющему резервное копирование такой информации: такое программное обеспечение должно пройти процедуру оценки соответствия, как правило, в форме сертификации по требованиям ФСТЭК.

Для обеспечения физической целостности данных, во избежание умышленного или неумышленного уничтожения, или искажения защищаемой информации и конфигураций информационных систем организуется резервное копирование баз данных, конфигураций, файлов настроек, конфигурационных файлов. Порядок резервного копирования, дублирования, хранения архивов и восстановления информации определен Порядком резервирования и восстановления информации. Для обеспечения гарантированного восстановления особо важной информации, которая может быть утеряна вследствие аппаратных сбоев, воздействия вирусов-шифровальщиков производится ежедневное резервное копирование содержимого дисков. Данный процесс запускается по служебной записке сотрудника на имя директора ГБПОУ «ЧТПиГХ им. Я.П. Осадчего».

Ответственными за организацию резервного копирования, хранения копий и восстановления информации являются администраторы ИС, ответственные сотрудники ГБПОУ «ЧТПиГХ им. Я.П. Осадчего».

Выводы по главе 2

Во второй главе магистерской диссертации проведен анализ информационных систем ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего».

В ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» действует политика обработки и защиты персональных данных.

В ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» эксплуатируются следующие информационные системы персональных данных (далее - ИСПДн) с использованием средств криптографической защиты информации (далее - СКЗИ, криптосредства):

1. ИСПДн «Бухгалтерия и кадры» в составе следующих подсистем:

- «Система дистанционного банковского обслуживания «Клиент-Банк», АО «Уральский банк реконструкции и развития» (далее - СДБО «Клиент-Банк УБРиР»);

- «Информационная система электронного документооборота «Интернет отчетность - Контур-Экстерн» (далее - ИС ЭДО «Контур-Экстерн»).

Для ИСПДн «Бухгалтерия и кадры» разработана ООО «СИБ Альпикс» и утверждена директором ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» «Модель угроз безопасности персональных данных ...» № СИБА.МУ.59 от 09.06.2016.

3. ИСПДн «ФИС ГИА и Приема».

Для ИСПДн «ФИС ГИА и Приема» разработана ООО «СИБ Альпикс» и утверждена директором ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» «Модель угроз безопасности персональных данных ...» № СИБА.МУ.61 от 09.06.2016.

Документы обучающихся вносятся в 1С:Колледж, Контур-Экстерн.

Таким образом, система защиты персональных данных при их обработке в информационных системах персональных данных в техникуме создана, но необходимо усовершенствовать систему резервного копирования при обеспечении защиты информации.

ГЛАВА 3 РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ОРГАНИЗАЦИИ СИСТЕМЫ РЕЗЕРВНОГО КОПИРОВАНИЯ В ГБПОУ «ЧЕЛЯБИНСКИЙ ТЕХНИКУМ ПРОМЫШЛЕННОСТИ И ГОРОДСКОГО ХОЗЯЙСТВА ИМЕНИ Я.П. ОСАДЧЕГО»

3.1 Рекомендации по организации системы резервного копирования при обеспечении защиты информации в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего»

Одной из важных задач при эксплуатации информационных систем является обеспечение целостности и сохранности данных, ведь даже в самой надежной из них существует риск потери информации, жизненно важной для предприятия. Поэтому необходимо иметь механизм для быстрого восстановления потерянных данных. Это может быть обеспечено путем построения развитой системы резервного копирования, периодически создающей копии информации с целью ее последующего восстановления в случае частичного или полного разрушения. Кроме того, такая система может собирать и обслуживать архив корпоративных данных.

В большинстве случаев требуется, чтобы система резервного копирования функционировала в вычислительной сети, причем умела манипулировать данными и устройствами независимо от их расположения в этой сети. Такая полноценная сетевая система должна обеспечивать восстановление данных, распределенных по всем узлам вычислительной сети.

Требования к резервному копированию информации, обрабатываемой в государственных информационных системах, информационных системах персональных данных содержатся в перечне законов РФ, подзаконных актов, постановлений правительства, нормативных актов федеральных органов исполнительной власти представлены в таблице 5.

Таблица 5 – Законодательные требования к информационной безопасности процесса резервного копирования информации

Законы	
Закон «Об информации, информационных технологиях и о защите информации»	Статья 16. Защита информации Обладатель информации, оператор информационной системы в случаях, установленных законодательством, обязаны обеспечить: … 5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие НСД
	Статья 13.12. Нарушение правил защиты информации 6. Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами РФ (с 14.12.2013)
Закон 152-ФЗ «О персональных данных»	Статья 19. Меры по обеспечению безопасности персональных данных при их обработке 1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от … неправомерных действий в отношении персональных данных
	Статья 19. Меры по обеспечению безопасности персональных данных при их обработке 2. Обеспечение безопасности персональных данных достигается, в частности: … 7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Продолжение таблицы 5

Приказы ФСТЭК и ФСБ	
Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн»	– организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от класса (уровня) защищенности, угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать: доступность информации… – меры по защите среды виртуализации должны исключать НСД к обрабатываемым данным и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к … системе хранения данных, сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям. – меры ЗСВ.8, ОДТ.4 и ОДТ.5.
Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»	
Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды	
Приказ ФСБ № 416, ФСТЭК № 489 от 31.08.2010	11. В информационных системах общего пользования должны быть обеспечены: …; возможность оперативного восстановления информации, модифицированной или уничтоженной вследствие неправомерных действий… 15. ... Подсистема информационной безопасности должна обеспечивать восстановление информации в ИСОП, модифицированной или уничтоженной вследствие неправомерных действий в отношении такой информации. Время восстановления процесса предоставления информации пользователям не должно превышать 8 часов

Согласно законодательным актам были разработаны рекомендации по организации системы резервного копирования при обеспечении защиты информации.

Рекомендации состоят из 3 этапов.

Этап 1. Разработка регламента копирования персональных данных субъектов ГБПОУ «ЧТПиГХ им. Я.П. Осадчего».

Регламент о порядке резервного копирования персональных данных субъектов Государственное бюджетное профессиональное образовательное учреждение «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего» (далее – Регламент) разработан в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом Российской Федерации от 27.06.2006 г. N 152-ФЗ «О персональных данных», Доктриной информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации от 09.09.2000 г. № Пр-1895.

Настоящий Регламент определяет порядок резервирования данных для последующего восстановления работоспособности автоматизированных систем ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего» при полной или частичной потере информации, вызванной сбоями или отказами аппаратного, или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.); восстановления информации в случае возникновения такой необходимости; упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации, обрабатываемой в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего» (далее – Техникум»).

В настоящем документе регламентируются действия при выполнении следующих мероприятий:

– резервное копирование;

– контроль резервного копирования;

– хранение резервных копий;

– полное или частичное восстановление данных и приложений.

Резервному копированию подлежит информация следующих основных категорий:

– персональная информация пользователей (личные каталоги на файловых серверах);

– групповая информация пользователей (общие каталоги отделов);

– информация, необходимая для восстановления серверов и систем управления базами данных (далее – СУБД);

– персональные профили пользователей сети;

– информация автоматизированных систем, в т.ч. баз данных;

– справочно-информационная информация систем общего использования;

– рабочие копии установочных компонент программного обеспечения рабочих станций;

– регистрационная информация системы информационной безопасности автоматизированных систем.

Порядок резервного копирования.

Ответственным за организацию резервного копирования персональных данных является администратор информационной безопасности.

Резервное копирование автоматизированных систем производится на основании следующих данных:

– состав и объем копируемых данных, периодичность проведения резервного копирования;

– максимальный срок хранения резервных копий - 1 месяц;

– хранение 3-х следующих архивов;

– архив на 1-е число текущего месяца;

– архив среда-четверг, либо пятница-суббота текущей недели;

– архив сделанный в текущую ночь.

Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации.

О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается директору Техникума в течение рабочего дня после обнаружения указанного события.

Контроль результатов резервного копирования.

Контроль результатов всех процедур резервного копирования осуществляется администратором информационной безопасности в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур.

В случае обнаружения ошибки в резервном копировании, администратор информационно безопасности устраняет ошибку и повторяет процедуру.

На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для ее хранения.

Ротация носителей резервной копии.

Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации автоматизированных систем в случае отказа любого из устройств резервного копирования.

В случае необходимости замены испорченных носителей информации новыми, администратор информационной безопасности заблаговременно за

10 рабочих дней согласовывает с поставщиком спецификации новых носителей информации.

Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются администратором информационной безопасности по графику или по запросу других сотрудников.

В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

Конфиденциальная информация с носителей, которые перестают использоваться в системе резервного копирования, должна стираться с использованием программного обеспечения PGP.

Восстановление информации из резервных копий.

В случае необходимости восстановление данных из резервных копий производится на основании Заявки сотрудника Техникума, согласованной с Ответственным за организацию обработки персональных данных.

Процедура восстановления информации из резервной копии осуществляется в соответствии с методикой восстановления информации.

После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

Этап 2. Выбор технологий.

Устройство NAS.

В качестве устройства NAS было выбрано для техникума: сетевое хранилище QNAP D2 (рис. 6).

Код: 470545; отсеков для дисков: 2; интерфейс: SATA III; форм-фактор: 2.5"/3.5"; LAN: 2 x 10/100/1000 Мбит/с; портов USB3.0: 3; RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, горячая замена дисков; совместимо с IP-камерами.

Это внешний бокс для 2 жестких дисков 3,5 дюйма SATA II/III, поддерживающих RAID 0 и RAID 1. Коробка поставляется без установленного жесткого диска и в настоящее время доступен через интернет-магазин https://www.dns-shop.ru/ по цене 17199 руб.

Рисунок 6 – Сетевое хранилище QNAP D2

Преимущество Накопителя NAS заключается в том, что можно будет использовать диски с сервера, который компания планирует отключать после развертывание архивной копии через FTP.

FTP сервер.

FTP-сервер с емкостью будет предоставлен https://lancloud.ru, поэтому покупать не нужно. В этом случае нет оборудования. Организация будет платить только ежемесячную плату за работу FTP-сервера. Эти ежемесячные платежи должны составлять около 1000 рублей в месяц. в зависимости объёма резервных копий.

Программа для выполнения дифференциального резервного копирования по FTP.

Для выполнения резервного копирования по FTP была выбрана утилита Duplicity. Эта утилита находится в свободном доступе.

В результате необходимо будет только приобрести NAS-бокс и заплатить ежемесячную плату за работу FTP-сервера.

Этап 3. Усовершенствование программно-технических средств резервного копирования.

На рынке программных продуктов для организации резервного копирования уже появились признанные лидеры. Наиболее функционально полным и развитым продуктом является, по нашему мнению, система Защита Данных (Cyber Backup**)** и Acronis Защита Данных Облачная (Cyber Backup Cloud) компании Acronis.

*Acronis Защита Данных (Cyber Backup)***.** Единое решение для защиты данных любых поддерживаемых систем: физических серверов, виртуальных машин, приложений, рабочих станций.

*Acronis Защита Данных Облачная (Cyber Backup Cloud)***.** Для защиты виртуальных, физических и облачных сред, позволяет быстро получить дополнительный доход без первоначальных инвестиций и предлагает бизнес-модель с оплатой по мере использования.

Компоненты Acronis Backup:

1. Компоненты для управляемой машины (агенты). Приложения, которые выполняют резервное копирование данных, их восстановление и другие операции на машинах под управлением Acronis Backup. Агентам необходима лицензия для выполнения операций на каждой управляемой машине.

2. Компоненты для централизованного управления. Эти компоненты в составе Acronis Backup Advanced обеспечивают возможности централизованного управления. Использование этих компонентов не лицензируется.

3. Консоль. Консоль обеспечивает графический интерфейс пользователя для работы с другими компонентами Acronis Backup. Использование консоли не лицензируется.

4. Мастер создания загрузочных носителей. Мастер создания загрузочных носителей создает загрузочные носители, которые позволяют использовать агенты и другие утилиты в среде аварийного восстановления. Лицензия для мастера создания загрузочных носителей не требуется при установке мастера вместе с агентом. Для использования мастера создания загрузочных носителей на машине без агента необходим лицензионный ключ или хотя бы одна лицензия на сервере лицензий. Лицензия может быть свободной или назначенной.

Технические характеристики, функционал.

В таблице 6 представлена информация о поддержке в Acronis Backup различных платформ виртуализации.

Таблица 6 – Поддержка в Acronis Backup различных платформ виртуализации (источник: acronis.com)

Платформа	Резервное копирование на уровне гипервизора	Резервное копирование изнутри гостевой ОС
VMware		
Версии VMware vSphere: 4.0, 4.1, 5.0, 5.1, 5.5 и 6.0 **Выпуски VMware vSphere:** VMware vSphere Essentials VMware vSphere Essentials Plus VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	+	+
VMware vSphere Hypervisor (бесплатная низкоуровневая оболочка ESXi)**		+
VMware Server (VMware Virtual Server) VMware Workstation VMware ACE VMware Player		+

Продолжение таблицы 6

Microsoft		
Windows Server 2008 (x64) с Hyper-V Windows Server 2008 R2 с Hyper-V Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 с Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1 (x64) с Hyper-V Windows 10 с Hyper-V Windows Server 2016 с Hyper-V Microsoft Hyper-V Server 2016	+	+
Microsoft Virtual PC 2004 и 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Citrix		
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2 и 6.5		Только полностью виртуализированные (известные также как HVM) гостевые системы
Red Hat и Linux		
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5 и 3.6		+
Виртуальные машины на основе ядра (KVM)		+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0 и 3.3		+
Oracle VM VirtualBox 4.x		+

* Стандартный выпуск не поддерживает «горячее» подключение, поэтому резервное копирование может выполняться медленнее.

** Резервное копирование на уровне гипервизора не поддерживается для vSphere Hypervisor, так как в этом продукте доступ к удаленному интерфейсу командной строки (RCLI) возможен исключительно в режиме «только для чтения». Агент работает в течение пробного периода vSphere Hypervisor до введения серийного ключа. После введения серийного ключа агент перестает работать.

Сценарии применения.

Локальное развертывание. Установка всех компонентов решения в локальной сети, доступно по бессрочной лицензии (рис. 7).

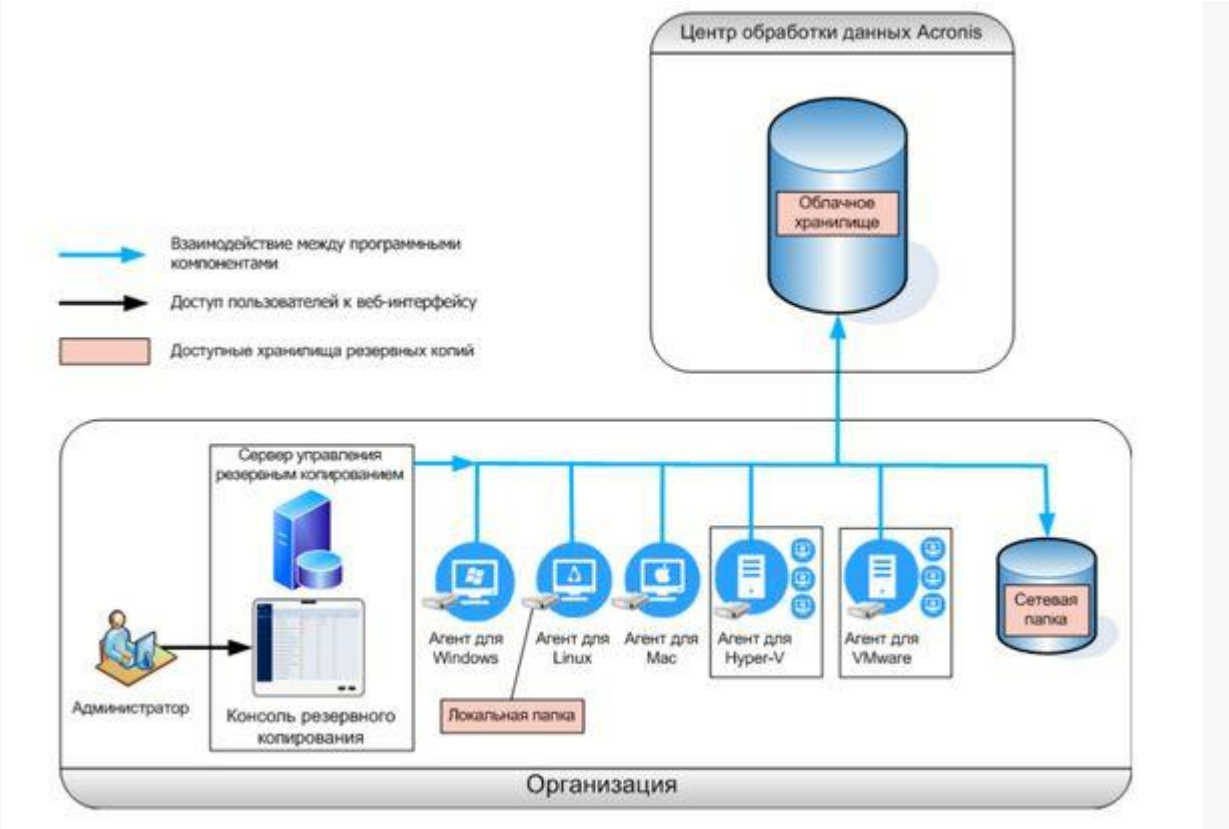

Рисунок 7 – Локальное развертывание Acronis Backup (источник: acronis.com)

Облачное развертывание**.** Сервер управления находится в одном из центров обработки данных Acronis. Преимущество этого подхода состоит в том, что не нужно обслуживать сервер управления в локальной сети. Acronis Backup можно представить, как сервис резервного копирования, предоставляемый Acronis (рис. 8).

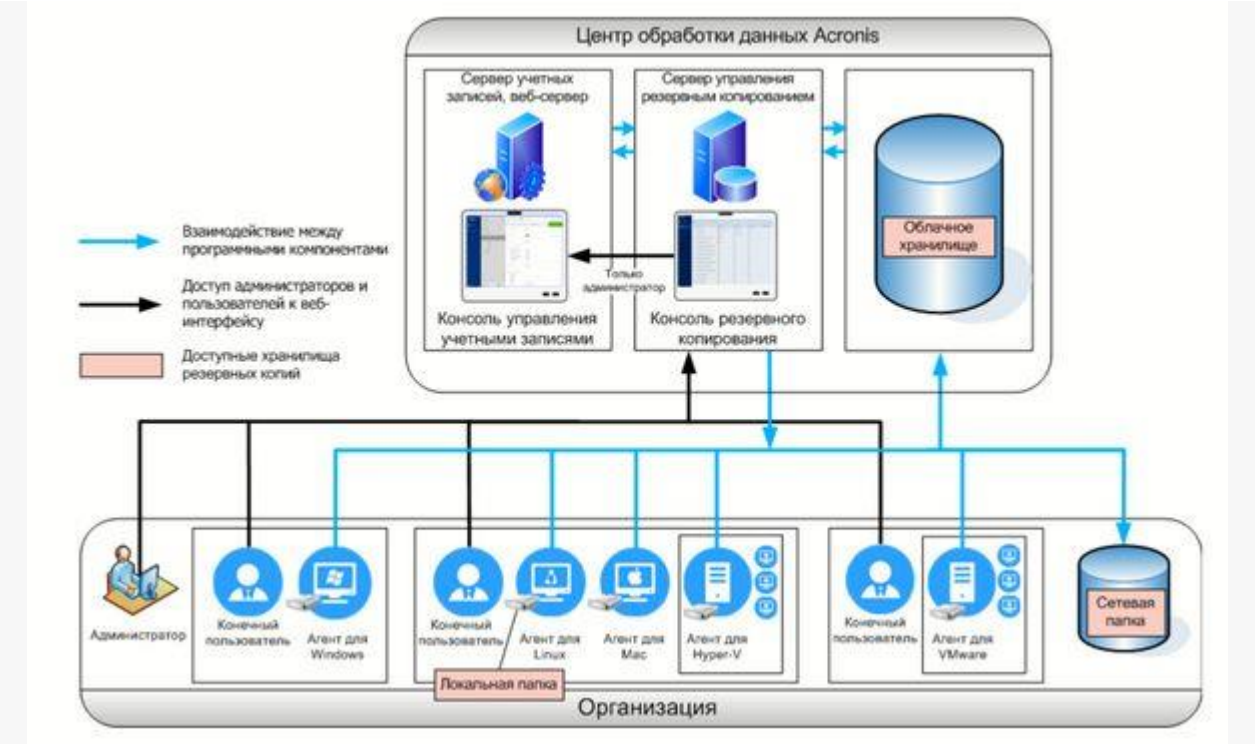

Рисунок 8 – Облачное развертывание Acronis Backup (источник: acronis.com)

Особенности. Детальное сравнение технологий бэкапа VMware vs Veeam vs Symantec vs Acronis представлены в таблице 7.

Таблица 7 – Сравнение технологий бэкапа VMware vs Veeam vs Symantec vs Acronis

Функции и возможности	**Data Recovery + vCenter**	**Veeam**	**Symantec**	**Acronis**
Бэкап данных	+	+	+	+
Создание снимков	+	+	+	+
Бэкап по времени	+	+	+	+
Отправка логов по e-mail	-	+	+	+
Откат машин к предыдущему состоянию	+	+	+	+
Централизованный интерфейс управления	+	+	+	+
Полная совместимость с решениями Vmware	+	+	+	+

Продолжение таблицы 7

Режим дедупликации[1]	+	+	-[2]	-[3]
Инкрементное резервное копирование[4]	+	+	+	+
Настраиваемые параметры для нескольких vCenter в режиме LinkedMode	+	+	+	+
Восстановление отдельных данных	+	+	+	+
Служба теневого копирования томов (VSS)	+	+	+	+
Управление политиками	+	-[5]	+	+
Совмещение со службами vMotion, HA, DRS	+	+	+	+
Поддержка типов хранения данных (Локальное, NFS, Share, iSCSI, Fibre Channel, NAS SAN, USB, DAS, облачные сервисы)	Локальное, NFS, Share, iSCSI, Fibre Channel, NAS	Локальное, NFS, Share, iSCSI, Fibre Channel, NAS, SAN	Локальное, NFS, Share, iSCSI, Fibre Channel, NAS, SAN, USB, DAS	Локальное, NFS, Share, iSCSI, Fibre Channel, NAS, SAN, DAS, облачные сервисы
Требование наличия vCenter	+	-	-	-
Возможность восстановления на другой аппаратной платформе[6]	-	-	+	+
Работа с базами SQL	-	+	-[7]	-
Работа с сервером Exchange	-	+	-[8]	-
Работа с Active Directory	-	+	-[9]	-
Возможность преобразования виртуальных сред в физические (V2P)	-	-	+	+

Продолжение таблицы 7

Возможность преобразования физических сред в виртуальные (P2V)	+	-	+	+
Рекомендация наличия vCenter	+	+	+	+
Моментальное восстановление после сбоя	-	+	+	+
Функция восстановления на «голое железо»[10]	-	-	+	+
Защита файлов шаблонов	-	+	+	-
Репликация данных	-	+	-	-
Проверка восстановления[11]	-	+	-	-
Работа с несколькими версиями ESX	Раздел идет по первой цифре версии	+	+	+
Поддержка ОС	Копирует всю машину, независимо от того какая ОС стоит	Копирует всю машину, независимо от того какая ОС стоит	Windows, Linux	Поддержка большинства ОС
Поддержка платформ	Только VMware	Только VMware	VMware, Microsoft Hyper-V, Citrix Xen, физические	VMware, Microsoft Hyper-V, Citrix Xen, Parallels, физические

Режим дедупликации позволяет сохранять бэкап не всей машины, а лишь данные, которые были изменены с момента последнего бэкапа. Это дает два существенных преимущества:

– существенная экономия места под резервное хранение данных;

– экономия трафика при расположении серверов на дальних друг от друга дистанциях (географическая составляющая).

Функция доступна с дополнительной опцией Deduplication Option.

Функция доступна с дополнительной опцией Deduplication.

Инкрементное резервное копирование позволяет сначала выполнить резервное копирование всего исходного каталога и потом «добавлять» к нему те файлы, которые изменились со времени последнего резервного копирования. Данная функция позволяет делать бэкап машины без перевода ее в режим обслуживания.

Функция, доступная с дополнительной программой Veeam Monitor.

Технология Symantec Restore Anyware позволяет пользователям перенести систему на другой компьютер, не выполняя установки заново.

Для базы данных SQL рекомендуется наличие Symantec Backup Exec Agent for Microsoft SQL Server, добавляющего функцию восстановление структуры базы данных.

Для сервера Exchange рекомендуется наличие Agent for Exchange Server, добавляющего функцию восстановление отдельных сообщений, папок и почтовых ящиков Exchange (устраняет необходимость резервного копирования почтовых ящиков).

Для сервера Active Directory рекомендуется наличие Agent for Active Directory, добавляющего функцию восстановление пользователей Active Directory, а также их свойств и атрибутов.

При утере файлов машины позволяет создать новую ВМ с такими же характеристиками и восстановить на нее старую.

После создания бэкапа данная технология проверяет, сможет ли поднять машину сразу после ее сбоя.

3.2 Оценка эффективности рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации и экономические затраты на их реализацию

Оценка эффективности является важным элементом разработки проектных и плановых решений, позволяющим определить уровень прогрессивности действующей структуры, разрабатываемых проектов или плановых мероприятий и проводится с целью выбора наиболее

рационального варианта структуры или способа ее совершенствования. Эффективность защитных мероприятий (ЗМ) должна оцениваться на стадии проектирования, для получения наилучших показателей работоспособности системы в целом.

При разработке проекта важны экономические показатели, которые наряду с техническими результатами будут определять эффективность системы. В состав затрат на разработку и исследование включаются затраты на проведение всех этапов работ.

Затраты на обеспечение информационной безопасности следует считать эффективными, если они обеспечивают выполнение требований нормативных документов и стандартов, принятых государством, а также концепции информационной безопасности организации.

Оценка эффективности рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего» проводится с использованием технических и программных средств контроля на предмет соответствия установленным действующим законодательством Российской Федерации требованиям.

После разработки рекомендаций по организации системы резервного копирования при обеспечении защиты информации в ИСПДн необходимо оценить эффективность их защиты. Сначала составляются общие критерии гипотетической оценки с указанием средств, которые обеспечат беспристрастный и полноценный анализ.

Программа и методика оценивания.

В программе обязательно должны быть:

- оцениваемый объект;
- запротоколированная очередность мероприятий, включая список и содержание проводимых процедур;
- итоговые оценочные критерии.

Критерии проверки:

1. Емкость хранения.

2. Пропускная способность.

3. Вычислительная мощность.

4. Временные рамки резервирования.

5. Время и точка восстановления.

По итогам вышеописанных манипуляций составляется протокол оценки эффективности рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации в техникуме. Он служит основой составления итогового заключения о состоянии защиты данных.

Расчет показателей эффективности может производиться с помощью различных методов: методы моделирования процессов защиты информации; экспертные оценки; статистический анализ; метод минимизации рисков и т.д.

В рамках исследовательской работы мы выбрали метод экспертной оценки.

Экспертная оценка – основана на компетентном мнении экспертов, знающих данную область и имеющих научно-практический потенциал для принятия решения.

Экспертная оценка эффективности рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации проводилась на базе в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего».

В процессе проведения экспертизы, рекомендации оценивались по следующим критериям:

1. Нормативно-правовая составляющая: соответствие разработанных рекомендаций требованиям действующих в России законодательных и нормативных документов по по орагниазции системы резервного копирования при обеспечении защиты информации.

2. Методическая составляющая рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации: содержательная и функциональная валидность предложенных мер, полнота

разработанных предложений и рекомендаций для совершенствования системы защиты.

3. Технологическая составляющая комплекса: характер предложенных программно-технических средств резервного копирования и рекомендаций по внедрению предложений.

Данные критерии были преобразованы в информационно-оценочную карту, которая представлена в таблице 8.

Перед проведением экспертизы была согласована система баллов, которые выставлялись экспертом при заполнении информационно-оценочной карты. Это было сделано для того, чтобы получаемая оценка обладала свойством надежности. То есть, чтобы разные эксперты, получив одни и те же данные, используя единую систему баллов и методы для их анализа, приходили к близким или одинаковым выводам.

Таблица 8 – Показатели оценки эффективности рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации в техникуме

Показатели оценки эффективности	**Эксперты**		
	Эксперт 1	Эксперт 2	Эксперт 3
	Критерии качества эффективности: высокий уровень (полностью соответствует показателю) средний уровень (в основном соответствует показателю) низкий уровень (в основном не соответствует показателю)		
1. Нормативно-правовая составляющая: соответствие разработанных рекомендаций требованиям действующих в России законодательных и нормативных документов по по орагниазции системы резервного копирования при обеспечении защиты информации.			
2. Методическая составляющая рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты.			

Продолжение таблицы 8

3. Технологическая составляющая комплекса: характер предложенных программно-технических средств резервного копирования и рекомендаций по внедрению предложений.			
Итоговая оценка экспертов:			

Каждому эксперту предлагались рекомендации рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации и информационно-оценочный лист с одинаковыми показателями оценки.

По итогам оценки эксперт представляет отчет, который содержит следующие сведения: заполненную информационно-оценочную карту; общие выводы.

В состав экспертной комиссии вошли: заведующий отделением информационных технологий, техник-программист, системный администратор отдела технической поддержки и связи техникума.

Результаты экспертной оценки представлены в таблице 9.

Таблица 9 – Результаты экспертной оценки эффективности предложенных рекомендаций

Показатели оценки эффективности	**Эксперты**		
	Эксперт М.И.	Эксперт К.С.	Эксперт З.Г.
	Критерии качества эффективности: высокий уровень (полностью соответствует показателю) средний уровень (в основном соответствует показателю) низкий уровень (в основном не соответствует показателю)		
1. Нормативно-правовая составляющая: соответствие разработанных рекомендаций требованиям действующих в России законодательных и нормативных документов по по орагниазции системы резервного копирования при обеспечении защиты информации.	Высокий уровень	Высокий уровень	Высокий уровень

Продолжение таблицы 9

2. Методическая составляющая рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты.	Высокий уровень	Средний уровень	Высокий уровень
3. Технологическая составляющая комплекса: характер предложенных программно-технических средств резервного копирования и рекомендаций по внедрению предложений.	Высокий уровень	Средний уровень	Высокий уровень
Итоговая оценка экспертов:	***Высокий уровень эффективности предложенных рекомендаций***		

Результаты экспертной оценки эффективности представлены на результирующей диаграмме (рис. 9).

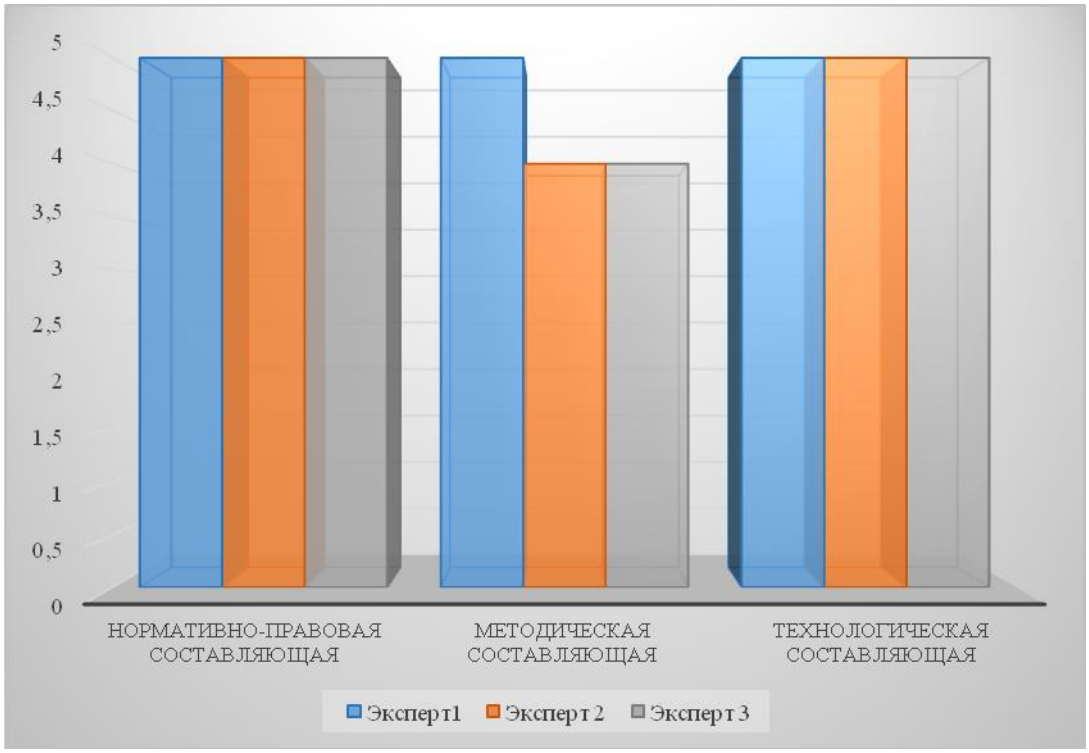

Рисунок 9 – Сводные результаты экспертной оценки эффективности разработанных рекомендаций

Проведенный анализ позволяет сделать вывод, что мнения экспертов относительно совпадают.

Далее составим статьи расходов (таблица 10).

Таблица 10 – Расходы на предложенные программно-технические средства резервного копирования

Статьи расходов	Сумма, руб
Постоянные расходы:	
1. Расходы электроэнергии	374,76
2. Заработная плата персонала	3400
3. Обслуживание FTP-сервера	1000
Итого:	4774,76
Переменные расходы:	
1. Покупка оборудования	17199
2. Покупка программного средства Acronis Защита Данных (Cyber Backup).	5459
Итого:	27432,76

Рассмотрим постоянные расходы.

1. Расход электроэнергии.

Усредненный тариф (городское население, дневная зона с 7-00 до 23-00 часов) на электроэнергию на 01.01.2022 - 3,47 руб./кВт ч.

Примерный расход кВт в час для сервера резервного копирования (не пиковая загруженность сервера) - 0,15 кВт.

Время работы сервера (в месяц) - 720 часов, предполагается постоянная работа сервера.

ИТОГО: 0,15 х 720 х 3,47 = 374,76 руб.

2. Заработная плата персонала.

1 сотрудник на полставки техника-программиста 11 разряда (почасовая форма расчета з/п):

52,5 руб. - час, норма - 80 ч./месяц.

52,5 руб. х 80 ч = 3400 руб.

ИТОГО: 3 400 руб.

Рассмотрим переменные расходы.

1. Покупка оборудования: Сетевое хранилище (NAS) QNAP D2.

Цена на 01.01.2022: 17 199 руб.

2. Покупка программного обеспечения: стоимость одной лицензии на Acronis Защита Данных – 5459 руб.

Необходимое количество зависит от конкретного учебного заведения, ориентировочно 10 штук.

10 шт. х 5459 руб. = 54590 руб.

Сведем полученные результаты в таблицу 11.

Таблица 11 – Инвестиции в проект

Сумма начальных инвестиции	76563,76 руб.
Ежемесячное содержание	4774,76 руб.

Итак, в результате анализа совокупных показателей существует возможность сделать обоснованный выбор в пользу предложенных мероприятий по совершенствованию организаций системы резервного копирования при обеспечении защиты информации в ИСПДн.

Таким образом, предложенные рекомендации по организации системы резервного копирования при обеспечении защиты информации несут в себе не только положительные моменты, такие как устранение основных проблем в организации среднего профессионального образования, касающихся информационной безопасности, но при этом они потребуют дополнительных вложений на приобретение оборудования.

Всегда будет иметь место человеческий фактор, форс-мажорные обстоятельства. Но если такие меры не предпринять затраты на восстановление информации, потерянные возможности по стоимости превзойдут те затраты, что требуются для разработки системы безопасности.

Таким образом, по результатам экспертной оценки эффективности и статьи расходов на программно-технические средства рекомендации по организации системы резервного копирования при обеспечении защиты информации находится в стадии исполнения в техникуме.

Выводы по главе 3

В третьей главе магистерской диссертации были предложены рекомендации по организации системы резервного копирования при обеспечении защиты информации в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего», выполнение которых позволит повысить эффективность средств защиты и сократит риск потери и искажения информации.

Рекомендации по организации системы резервного копирования при обеспечении защиты информации состоят из 3 этапов.

Этап 1. Разработка регламента копирования персональных данных субъектов ГБПОУ «ЧТПиГХ им. Я.П. Осадчего».

Настоящий Регламент определяет порядок резервирования данных для последующего восстановления работоспособности автоматизированных систем ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего» при полной или частичной потере информации, вызванной сбоями или отказами аппаратного, или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.); восстановления информации в случае возникновения такой необходимости; упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации, обрабатываемой в техникуме.

В настоящем документе регламентируются действия при выполнении следующих мероприятий: резервное копирование; контроль резервного копирования; хранение резервных копий; полное или частичное восстановление данных и приложений.

Этап 2. Выбор технологий. В качестве устройства NAS было выбрано для техникума: сетевое хранилище QNAP D2. Преимущество Накопителя NAS заключается в том, что можно будет использовать диски с сервера,

который компания планирует отключать после развертывание архивной копии через FTP.

Для выполнения резервного копирования по FTP была выбрана утилита Duplicity. Эта утилита находится в свободном доступе.

В результате необходимо будет только приобрести NAS-бокс и заплатить ежемесячную плату за работу FTP-сервера.

Этап 3. Усовершенствование программно-технических средств резервного копирования. В качестве программного продукта была выбрана система Защита Данных (Cyber Backup**)** и Acronis Защита Данных Облачная (Cyber Backup Cloud) компании Acronis.

По итогам вышеописанных манипуляций составляется протокол оценки эффективности рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации в техникуме. Он служит основой составления итогового заключения о состоянии защиты данных.

В процессе проведения экспертизы, рекомендации оценивались по следующим критериям:

1. Нормативно-правовая составляющая: соответствие разработанных рекомендаций требованиям действующих в России законодательных и нормативных документов по по орагниазции системы резервного копирования при обеспечении защиты информации.

2. Методическая составляющая рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты.

3. Технологическая составляющая комплекса: характер предложенных программно-технических средств резервного копирования и рекомендаций по внедрению предложений.

Описаны экономические затраты и план внедрения системы резервного копирования.

Таким образом, по результатам экспертной оценки эффективности и статьи расходов на программно-технические средства рекомендации по организации системы резервного копирования при обеспечении защиты информации находится в стадии исполнения в техникуме.

ЗАКЛЮЧЕНИЕ

На основании изученных информационных источников по теме исследования можно сделать вывод о практической необходимости организации системы резервного копирования при обеспечении защиты информации в образовательных организациях.

В первой главе магистерской диссертации решались следующие задачи: проанализировано понятие, назначение, функции и особенности систем резервного копирования. Изучены технологии резервного копирования и хранения резервных копий и данных, проанализированы программно-технические средства резервного копирования, наиболее подходящие для реализации систем резервного копирования в организации профессионального образования;

Вопрос по защите и резервному копированию информации стоит сегодня очень актуально ввиду безусловного развития информационных технологий и влечет за собой большой рост количества обрабатываемой и сохраняемой информации. Поэтому исследования и разработки в сфере хранения и резервного копирования информации всегда будут востребованы, аппаратно-программные средства и в дальнейшем будут развиваться, совершенствоваться и подстраиваться под потребности пользователей.

Система резервного копирования предназначена для создания резервных копий и восстановления данных. Она позволяет защитить данные от разрушения не только в случае сбоев или выхода из строя аппаратуры, но и в результате ошибок программных средств и пользователей.

На основании всего вышеизложенного можно сделать вывод, что организация системы резервного копирования безусловно необходимо при организации политики информационной безопасности образовательной организации.

Во второй главе магистерской диссертации проведен анализ информационных систем ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего».

В ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» эксплуатируются следующие информационные системы персональных данных (далее - ИСПДн) с использованием средств криптографической защиты информации (далее - СКЗИ, криптосредства):

1. ИСПДн «Бухгалтерия и кадры» в составе следующих подсистем:

- «Система дистанционного банковского обслуживания «Клиент-Банк», АО «Уральский банк реконструкции и развития» (далее - СДБО «Клиент-Банк УБРиР»);

- «Информационная система электронного документооборота «Интернет отчетность - Контур-Экстерн» (далее - ИС ЭДО «Контур-Экстерн»).

Для ИСПДн «Бухгалтерия и кадры» разработана ООО «СИБ Альпикс» и утверждена директором ГБПОУ «ЧТПиГХ им. Я.П. Осадчего» «Модель угроз безопасности персональных данных ...» № СИБА.МУ.59 от 09.06.2016.

2. ИСПДн «ФИС ГИА и Приема».

Система защиты персональных данных при их обработке в информационных системах персональных данных в техникуме создана, но необходимо усовершенствовать систему резервного копирования при обеспечении защиты информации.

В третьей главе магистерской диссертации были предложены рекомендации по организации системы резервного копирования при обеспечении защиты информации в ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего», в результате выполнения которых позволит повысить эффективность средств защиты и сократит риск потери и искажения информации.

Рекомендации по организации системы резервного копирования при обеспечении защиты информации состоят из 3 этапов.

Этап 1. Разработка регламента копирования персональных данных субъектов ГБПОУ «ЧТПиГХ им. Я.П. Осадчего».

В настоящем документе регламентируются действия при выполнении следующих мероприятий: резервное копирование; контроль резервного копирования; хранение резервных копий; полное или частичное восстановление данных и приложений.

Этап 2. Выбор технологий. В качестве устройства NAS было выбрано для техникума: сетевое хранилище QNAP D2. Преимущество Накопителя NAS заключается в том, что можно будет использовать диски с сервера, который компания планирует отключать после развертывание архивной копии через FTP.

Для выполнения резервного копирования по FTP была выбрана утилита Duplicity. Эта утилита находится в свободном доступе.

В результате необходимо будет только приобрести NAS-бокс и заплатить ежемесячную плату за работу FTP-сервера.

Этап 3. Усовершенствование программно-технических средств резервного копирования. В качестве программного продукта была выбрана система Защита Данных (Cyber Backup**)** и Acronis Защита Данных Облачная (Cyber Backup Cloud) компании Acronis.

По итогам вышеописанных манипуляций составляется протокол оценки эффективности рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации в техникуме. Он служит основой составления итогового заключения о состоянии защиты данных.

В процессе проведения экспертизы, рекомендации оценивались по следующим критериям:

1. Нормативно-правовая составляющая: соответствие разработанных рекомендаций требованиям действующих в России законодательных и нормативных документов по по орагниазции системы резервного копирования при обеспечении защиты информации.

2. Методическая составляющая рекомендаций по орагниазции системы резервного копирования при обеспечении защиты информации: содержательная и функциональная валидность предложенных мер, полнота разработанных предложений и рекомендаций для совершенствования системы защиты.

3. Технологическая составляющая комплекса: характер предложенных программно-технических средств резервного копирования и рекомендаций по внедрению предложений.

Описаны экономические затраты и план внедрения системы резервного копирования.

Таким образом, по результатам экспертной оценки эффективности и статьи расходов на программно-технические средства рекомендации по организации системы резервного копирования при обеспечении защиты информации находится в стадии исполнения в техникуме.

Таким образом, цель работы достигнута, задачи выполнены, гипотеза исследования подтвердилась.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативно – правовые акты

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введ. 2006-12-27. – М.: Изд-во стандартов, 2006. – 9 с.

2. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. – Введ. 2006-12-27. – М.: Изд-во стандартов, 2006. – 7 с.

3. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности. Основные термины и определения. – URL: http://www.opengost.ru/iso/35_gosty_iso/35020_gost_iso/11522-gost-r-53114-2008-zaschita-informacii.-obespechenie-informacionnoy-bezopasnosti.-osnovnye-terminy-i-opredeleniya.html. Дата обращения: 16.12.2020.

4. ГОСТ РВ 50600-93. Защита секретной информации от технической разведки. Система документов. Общие положения. - М.: Изд-во стандартов, 1993.

5. Доктрина информационной безопасности Российской Федерации от 09.09.2000: утверждена Президентом РФ В. Путиным // Известия. - 10 декабря 2002. - С.2

6. Конституция Российской Федерации: офиц. текст. - М.: Право, 2002. - 39 с.

7. О государственной тайне: ФЗ по состоянию на 22.08.2004. / Федер. Собр. Рос. Федерации. - М.: ГД РФ, 2004. - 12 с.

8. О коммерческой тайне: ФЗ от 29 июля 2004 № 98 // Собрание актов Президента и Правительства РФ. - № 7. - С.5.

9. О персональных данных: ФЗ от 27 июля 2006 № 152 - ФЗ // Бюллетень нормативных актов министерств и ведомств. - № 7. - 2006. - С.15.

10. Об архивном деле в Российской Федерации: ФЗ от 01 октября 2004 № 125 - ФЗ // Собрание актов Президента и Правительства РФ. - № 11. - С.12.

11. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 № 149 - ФЗ // СЗ РФ. – 2006. - №31

12. Об утверждении Перечня сведений конфиденциального характера от 06.03.97 № 188: указ Президента РФ // Собрание актов Президента и Правительства РФ. - 1993. - № 23. С.12 – 14.

13. Об утверждении Перечня сведений, которые не могут составлять коммерческую тайну: постановление правительства РФ от 03.10.2002 № 731 // Собрание актов Президента и Правительства РФ. - 2003. - № 11. - 140 с.

14. Об утверждении Перечня сведений, отнесенных к государственной тайне от 30.11.95 № 1203: с измен. и доп. от 24.01.98 № 61, от 06.06.2001 № 659, от 10.09.2001 № 1114, от 29.05.2002 № 518, от 11 февраля 2006: указ Президента РФ // Собрание актов Президента и Правительства РФ. - 2006. - № 11.

15. Об утверждении положения о государственной системе защиты информации от иностранной технической разведки и от ее утечки по техническим каналам от 15.09.93 № 912 - 51: постановление Правительства РФ // Собрание актов Президента и Правительства РФ. - 1993. - № 15. - 125 с.

16. Об утверждении Положения о лицензировании деятельности по технической защите конфиденциальной информации от 30.04.02. № 290: постановление Правительства РФ // Собрание актов Президента и Правительства РФ. - 2002. - № 8. - С.102.

17. Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 17 ноября 2007 г. № 781. URL - https://base.garant.ru/192223/. Дата обращения: 21.09.2020.

18. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти: постановление Правительства РФ от 3 ноября 1994 г. № 1233. // Собрание актов Президента и Правительства РФ. - 1995. - № 10. - С.56.

19. Трудовой кодекс Российской Федерации: федер. закон от 30.12.2001 N 197-ФЗ (ред. от 25.05.2020). URL - https://clck.ru/B8yGj. Дата обращения: 14.12.2020.

Литература

20. Ажмухамедов, И.М., Ханжина, Т.Б. Оценка экономической эффективности мер по обеспечению информационной безопасности [Текст] / И.М. Ажмухамедов, Т.Б. Ханжина // Вестник АГТУ. Серия: «Экономика» №1/2011, С.185-190.

21. Астахова Л.В., Завадский А.О. Особенности организации защиты персональных данных в образовательной организации // Вестник УрФО. Безопасность в информационной сфере. – 2013 – № 3(9). – С.4-10.

22. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) [Электронный ресурс]: [Утверждена заместителем директора ФСТЭК РФ 15.02.2008 г.]. - Режим доступа: www.fstec.ru (дата обращения: 15.12.2021).

23. Бугров А. Международные стандарты для построения системы информационной безопасности / А. Бугров // Финансовая газета. - 2017. - №10.

24. Галатенко В.А. Основы информационной безопасности: курс лекций / В.А. Галатенко. URL - https://www.intuit.ru/studies/courses/10/10/info (дата обращения: 20.12.2021).

25. Ильгова О. Этапы организации защиты ПДн в ОО (для администратора). – URL: https://help.dnevnik.ru/hc/ru/articles/203475268 (дата обращения: 16.12.2021).

26. Мельник Н.Ю. Защита персональных данных в профессиональном образовании // Современные технологии: актуальные вопросы, достижения и инновации. – 2018. – С. 55-57.

27. Мельников, В.П. Информационная безопасность и защита информации [Текст]: учеб. пособие / В.П. Мельников, С.А. Клейменов, А.М. Петраков. – М.: Издательский центр «Академия», 2013. – 336 с.

28. Меры по защите от угроз нарушения доступности [Электронный ресурс]. - URL: www.sha-danis.narod.ru (дата обращения: 20.12.2021).

29. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке информационных системах персональных данных с использованием средств автоматизации [Электронный ресурс]: [Утверждены руководством 8 центра ФСБ России 21.02.2008 г. №149/54-144]. - Режим доступа: www.consultant.ru. (дата обращения: 15.12.2021).

30. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (утв. ФСБ России 31.03.2015 N 149/7/2/6-432). Электронный документ. Режим доступа: http://docs.cntd.ru/document/420336137 (дата обращения: 16.01.2021).

31. Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014). Электронный документ. Режим доступа: http://fstec.ru/ (дата обращения: 16.12.2021).

32. Методы организации защиты информации [Текст]: учебное пособие для студентов 3–4 курсов всех форм обучения направлений подготовки 230400.55, 230701.51, 090300.65, 220100.55 / Ю.Ю. Громов и др. – Тамбов: Изд-во ФГБОУ ВО «ТГТУ», 2013. – 80 с.

33. Милютина О.В. Особенности защиты информации в образовательном учреждении / О.В. Милютина. – URL: http://www.fcoit.ru/internet_conference/information_security_training_process/fea

tures_information_security_in_an_educational_institution.php (дата обращения: 10.12.2021).

34. Официальный сайт ГБПОУ «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего». – URL: http://chtpgh.ru/ (дата обращения: 19.12.2021).

35. Политика обработки и защиты персональных данных Государственного бюджетного профессионального образовательного учреждения «Челябинский техникум промышленности и городского хозяйства имени Я.П. Осадчего» – URL: http://chtpgh.ru/ (дата обращения: 19.12.2021).

36. Положение об обработке и защите персональных данных в ГБПОУ «Челябинский техникум промышленности и городского хозяйства им. Я.Г1. Осадчего» – URL: http://chtpgh.ru/ (дата обращения: 19.12.2021).

37. Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

38. Постановление Правительства РФ от 03.02.2012 N 79 (с изм. от 15.06.2016) «О лицензировании деятельности по технической защите конфиденциальной информации». – Режим доступа: http://www.garant.ru/ (дата обращения: 16.12.2021).

39. Постановление Правительства РФ от 03.03.2012 N 171 (с изм. от 15.06.2016) «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации». [Электронный ресурс]. Режим доступа: http://www.garant.ru/ (дата обращения: 16.12.2021).

40. Постановление Правительства РФ от 06.07.2008 № 512 (ред. от 27.12.2012) «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» от 06.07.2008 № 512 // «Российская газета», № 148, 11.07.2008.

41. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // «Российская газета», № 200, 24.09.2008.

42. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) Федеральной службы безопасности Российской Федерации (ФСБ России) Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. N 55/86/20 г. Москва «Об утверждении Порядка проведения классификации информационных систем персональных данных» // «Российская газета», № 4637, 12.04.2008.

43. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ России и Министерства связи и массовых коммуникаций РФ от 31 декабря 2013 г. № 151/786/461 «О признании утратившим силу приказа Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных». - Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/815-sovmestnyj-prikaz-fstek-rossii-fsb-rossii-i-minkomsvyazi-rossii-ot-31-dekabrya-2013-g-n-151-786-461. Дата обращения: 16.12.2021.

44. Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн при использовании средств криптографической защиты информации» // «Российская газета» от 17 сентября 2014 г. N 211.

45. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению

безопасности персональных данных при их обработке в информационных системах персональных данных» // «Российская газета», № 107, 22.05.2013.

46. Резервное копирование и синхронизация данных между компьютерами [Электронный ресурс]. Режим доступа: http://www.root.cz/clanky/dropbox-zaloha-a-synchronizace-datmezi-pocitaci/ (дата обращения: 13.12.2021).

47. Система резервного копирования (безопасность) – URL: https://www.tadviser.ru/index.php (дата обращения: 15.01.2022).

48. Техническая документация с официальных источников (сайт разработчиков продуктов Acronis) [Электронный ресурс]. Режим доступа: www.acronis.ru (дата обращения: 15.01.2022).

49. Фионова Л.Р Положение о защите персональных данных работников / Л.Р. Фионова, О.В. Касперская // Секретарское дело. - 2015. - № 10. - С.40 - 49.

50. Ширманов А. Законодательные требования к информационной безопасности процесса резервного копирования информации / А. Ширманов. – URL: https://www.veeam.com/ru/wp_regulatory_requirements_for_backup_wp.pdf (дата обращения: 15.01.2022).

51. Ярочкин В.Н. Информационная безопасность / В.Н. Ярочкин. - М.: Трикста, Академ. проект, 2015. - 542 с.