

Дрожжинова П.Л., студ. гр. 337 БГУКИ

Науч. рук. – Петренко Б.В.,

кандидат технических наук, доцент

ТЕХНОЛОГИЧЕСКАЯ ПОДСИСТЕМА СОХРАНЕНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ АБИС

Информационные ресурсы АБИС это совокупность определённым образом организованных данных содержащихся в полнотекстовых, фактографических, библиографических базах данных, которые пополняются на протяжении многих лет. Однако в случае технических неполадок, программных сбоев и механического повреждения ЭВМ, информация содержащаяся в электронном каталоге и других базах данных может быть искажена или утеряна. Приведение электронного каталога в нерабочее состояние приведёт к тому, что ориентация в фонде станет затруднительна или невозможна. Особенно эта проблема актуальна в связи с тем, что на современном этапе в библиотеках не формируются каталоги на бумажных носителях и электронный каталог становится единственным средством ориентации в фонде.

С целью избежания подобных инцидентов при создании АБИС предусматривается подсистема сохранения информационных ресурсов. Важнейшей частью данной подсистемы являются архивы, под которыми подразумевается упорядоченная совокупность массивов данных или программ, длительно хранимых на внешних машиночитаемых носителях. Также в эту подсистему должны входить документы регламентирующие организационные, технологические и технические решения, сотрудников, осуществляющих функционирование данной подсистемы и программно-аппаратные и другие технические средства создания, сохранения и использования архивов.

Создание архива включает в себя следующие этапы:

1) Копирование массива информации – копированию могут подлежать все файлы или только те, которые были изменены со времени последнего резервного копирования.

2) Сжатие физической длины записей с использованием специальных прикладных программ-архиваторов. Под сжатием физической длины понимается технический приём сокращения объёма данных, который реализуется как правило посредством кодирования данных. Массив информации в сжатом состоянии удобен для длительного хранения так как занимает мало места на материальном носителе. Вместе с тем в таком виде использовать массив информации невозможно. Исходная запись восстанавливается после процесса разархивации, который также осуществляется с помощью программ-архиваторов.

3) Перенесение информации на материальный носитель. Архивы нужно хранить отдельно от массивов информации, которые они отражают. Материальные носители могут быть энергозависимые – магнитные накопители, которые также известны нам как винчестеры, жесткие диски или HDD. Также в последние годы используются жесткие диски на основе технологии SSD, однако они являются более дорогостоящими. Среди не энергозависимых носителей информации целесообразно использовать оптические диски, запись-чтение с которых осуществляется оптическим методом. При этом в качестве устройства чтения-записи используется лазерный луч, который, считывает информацию, закодированную на оптический диск. Преимуществом данного носителя является долговечность и относительно малая стоимость. Скорость чтения-записи для оптических носителей заметно уступает технологии магнитного и электрического кодирования. Однако оптические диски идеально подходят для долговременного хранения архивов. Перспективным энергонезависимым носителем информации является флэш-память – подобные устройства миниатюрны, но обладают большим объёмом памяти. Скорость чтения-записи при этом значительно опережает оптические диски, но уступает

магнитным носителям информации. Однако во флэш-картах полностью отсутствует механическая составляющая, что делает этот носитель информации значительно более надежным по сравнению с магнитным жестким диском.

Совокупность вышеперечисленных процессов называется архивацией. Архивации как правило подлежат электронные каталоги, базы и банки данных, базы и банки данных отдельных подразделений библиотек, массивы записей документов текущей обработки. Также архивации могут подлежать программы и данные, потребность в оперативном использовании которых частично, полностью или временно отпала – это позволяет освободить память ЭВМ от ненужных данных.

Архивы должны актуализироваться по мере изменения информации в массивах данных которые они отражают.

В подсистему сохранения информационных ресурсов АБИС входит комплекс аппаратно-программных средств защищающих информационные ресурсы от несанкционированного доступа, вмешательства в процесс функционирования системы посторонних лиц, что может привести к модификации, фальсификации, уничтожению данных. Эти аппаратно-программные средства должны осуществлять идентификацию и аутентификацию пользователей при входе в систему путём сравнения введённого им пароля с паролем сохранённым в базе данных при регистрации. Также осуществляется разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам АБИС, то есть предоставление пользователям возможности доступа только к тем ресурсам и выполнению только тех операций, которые необходимы по роду деятельности, авторизацию привилегированных операций для пользователей, обладающих привилегиями. Пользователям-читателям необходимо предоставлять доступ к электронному каталогу и базам данных с целью ознакомления с хранящейся в них информацией, при этом лишая их возможности вносить

какие-либо изменения в массив данных. Для предотвращения непреднамеренной несанкционированной модификации системы сотрудниками посредством запуска программ, способных при некомпетентном использовании вызвать потерю работоспособности системы или осуществить необратимые изменения как то – форматирование или реструктуризацию носителей информации или удаление данных, необходимо регламентировать действия осуществляемые при работе с системой и ввести запреты на потенциально опасные операции.

Кроме защиты информационных ресурсов от преднамеренного или случайного искажения пользователями, массивам данных АБИС необходима защита от вредоносных вирусных программ выполняющих несанкционированные деструктивные действия. Источниками подобных программ могут быть съемные носители и системы телекоммуникаций. Результатом заражения вирусом может стать медленная работа системы, зависания и сбои, изменение размеров файлов, значительное увеличение количества файлов, исчезновение файлов и каталогов или искажение их содержимого. Для предотвращения внедрения вирусов в систему необходимо проверять все внешние носители на наличие вирусов, прежде чем копировать или открывать содержащиеся на них файлы. Такой же проверке должны подлежать файлы, полученные с помощью сети Интернет. Для обнаружения и уничтожения вредоносных программ существуют антивирусные программы, которые должны входить в подсистему сохранения информационных ресурсов АБИС. Необходимо регулярно сканировать жесткие диски в поисках вирусов. Сканирование обычно выполняется автоматически при каждом включении персонального компьютера и при размещении внешнего диска в считывающем устройстве. При сканировании антивирусная программа ищет вирус путем сравнения кода программ с кодами известных ей вирусов, хранящихся в базе данных. Нужно оперативно пополнять базу данных антивирусной программы набором файлов сигнатур вирусов, как только появляются новые сигнатуры.

-
1. Борзенко, А. Методы сжатия данных / А. Борзенко // Компьютер-пресс.– 1995. – № 8. – С. 155 – 158.
 2. Воройский, Ф.С. Основы проектирования автоматизированных библиотечно-информационных систем / Ф.С. Воройский. – М. : ГПНТБ России, 2002. – 389 с.
 3. Воройский, Ф.С. Пока гром не грянет. Организация, технология и технические средства сохранения информационных ресурсов АБИС / Ф.С. Воройский // С компьютером на Ты. – М., 2000. – Вып. 3. – С.10 – 19.
 4. Шрайберг, Я.Л. Избранные труды / Я.Л. Шрайберг. – М. : ГПНТБ России, 2002. – 624 с.

РЕПОЗИТОРИЙ БГУКИ