CZU 027.7(478):004.6

Методы сохранности электронных информационных ресурсов в научной библиотеке

Igor AFATIN,
Biblioteca Științifică a Universității de Stat „Alecu Russo”, or. Bălți

Rezumat: *Articolul analizează modalităţile de păstrare a informaţiei, restricţionarea accesului la servere şi fişiere, instalarea unui software de rezervă, crearea arhivelor electronice, stocarea în reţea şi în cloud, proiectarea sistemelor de stocare. Autorul acordă o atenţie deosebită politicii de securitate a datelor, implementării unor metode inovaţionale în vederea protecţiei informaţiei din Biblioteca Ştiinţifică USARB: configurarea serverului terminal, setarea computerilor locale ale utilizatorilor şi a infrastructurii reţelei locale de calculatoare, setarea reţelei locale (Local Area Network), configurarea arhivării serverului etc.*
Cuvinte cheie: *securitatea informaţiei, securitatea datelor, controlul datelor, arhive electronice, stocare în cloud, politica de securitate a datelor, setarea LAN (Local Area Network), server terminal, steamer*

Abstract: *The article describes ways to store data: restricting access to servers and files, installing backup software, creating electronic archives, network and cloud storage, designing storage systems. The author pays special attention to the data security policy and the introduction of new methods of information security in the Scientific Library of the A. Russo Balti State University: deployment of a terminal server, setting up local users' computers, local computer network infrastructure, setting up server archiving and much more.*
Keywords: *information protection, data control, electronic archives, cloud storage, data security policy, setting up a local network, terminal server, steamers*

Абстракт: *В статье описываются способы сохранения информации: ограничение доступа к серверам и файлам, установка ПО для резервного копирования, создание электронных архивов, сетевых и облачных хранилищ, проектирование системы хранения данных. Особое внимание автор уделяет политике безопасности данных и внедрению новых методов сохранности информации в Научной Библиотеке БГУ им. Алеку Руссо: развёртывание терминального сервера, настройки локальных компьютеров пользователей, инфраструктуры локальной компьютерной сети, настройка архивирования серверов и многое другое.*
Ключевые слова: *защита информации, контроль данных, электронные архивы, облачные хранилища, политика безопасности данных, настройка локальной сети, терминальный сервер, стимеры.*

Необходимо всё время стремиться к минимизации последствий мелких неприятностей, средних проблем и крупных катастроф, и надо быть к ним готовыми постоянно.

Любая информация, хранящаяся в одном месте, будет потеряна раньше или позже, как бы надёжно это место не было. Поэтому единственное решение проблемы состоит в размножении данных, как можно более частом и регулярном, а пути реализации сильно зависят от имеющихся в распоряжении технических средств.

Меры и способы сохранения информации

Любая социальная деятельность людей построена на создании, передаче, обработке и хранении информации. Обеспечение сохранности информации производится на основе применения специальных мер организации хранения и подготовки, восстановления и регенерации информации, специальных устройств резервирования. Качество обеспечения сохранности информации зависит от её целостности (точности, полноты) и готовности к постоянному использованию.

Как не допустить потери информации?

Тот, кто владеет информацией, в той или иной степени заботится о сохранности этой информации. К сожалению, иногда бывает, что информация пропадает или теряется. В большинстве случаев по вине человека, работающего с информацией - случайно перенес не в ту папку или удалил; в более редких случаях по вине оборудования.

Существует ряд мер, призванных свести к минимуму риск потери информации:

- Физически ограничить доступ человека от компьютеров и серверов. Необходимо полностью исключить возможность физического воздействия на системные блоки, чтобы никто не мог об них споткнуться, или того хуже – зацепив, сбросить со стола. Максимум, какой доступ может иметь человек к системному блоку – нажать кнопку питания.
- Ограничить доступ пользователей к файлам – установить пароли на вход в Windows, чтобы посторонний человек не получил доступ к файлам и разделам жесткого диска. Ограничить права доступа к общим папкам в сети.
- Корректно завершать работу операционной системы и приложений. Не допускать аварийного завершения работы (Шляхтина, Светлана 2013).
- Установить программное обеспечение для ежедневного резервного копирования данных в автоматическом режиме. В ОС Windows имеются штатные средства для создания архивов выбранной пользователем информации по расписанию (в идеале ежедневно). Так же существует множество отдельных программ, благодаря которым автоматически создаются архивные копии важных файлов и папок.

Использование хранилищ информации. Одна из главных задач хранилищ информации – интеграция всех сведений из разнообразных источников в единую централизованную структуру, которая обеспечивала бы процесс превращения «сырых» фактов в полезную информацию. При этом должны использоваться обширные возможности электронной обработки и хранения данных. По признанию экспертов, в течение последних лет наблюдается процесс активного перехода от бумажных архивов к электронным. Удешевление и увеличение емкости систем хранения такой информации привели к тому, что предприятия и организации промышленно развитых стран мира оперативно переводят массивы хранящихся документов в новую форму и используют в повседневной работе вместо бумажных оригиналов их точные электронные образы со всеми печатями, визами, резолюциями и т.д.

Самый сложный вопрос в создании электронного архива заключается в его наполнении, ибо приходится переводить в надлежащий вид как уже существующий массив документов, так и текущих поступлений. Зато электронные системы способны записывать ко-

лоссальные объемы информации на очень малых площадях и обеспечивать мгновенный поиск. Они также позволяют обеспечить санкционированным пользователям дистанционный доступ к базам данных. Правда, всегда нужно помнить об уязвимости запоминающих устройств компьютеров и о необходимости дублирования материалов путем записи их на альтернативный носитель.

Ожидаемые сроки службы различных носителей информации, используемых для хранения правительственных документов, примерно следующие: магнитная лента – от 5 до 15 лет; CD-ROM – до 50 лет; пленка для микрофильмирования – до 20 лет; пленка для архивного микрофильмирования – от 100 до 200 лет; газетная бумага – от 10 до 20 лет; высококачественная бумага – до 100 лет; специальная бумага – до 500 лет. Учет этого фактора, а также контроль данных требует наличия нормативов на сроки хранения и защиты информации. Специалисты полагают, что документ нужно считать «неактивным», если к нему обращаются менее, чем 15 раз в год. Если же документы используются дважды в месяц, их можно отнести к «полуактивным», если же документы используются три и более раз в месяц, то их надо считать «активными». Указанный показатель является одним из важнейших факторов, влияющим на определения судьбы и места дальнейшего хранения документов. Некоторые материалы могут быть уничтожены после определенного времени, другие необходимо хранить в течение длительного периода времени или без указания конкретного срока, если по своей природе информация представляет архивный интерес. Профессионалов нисколько не удивил случай, когда с досье одного из высокопоставленных шведских агентов отечественная разведка ознакомила широкую публику через четыреста лет после происходивших событий.

Контроль данных - одна из мер сохранности

Целями контроля данных являются:

1) обеспечение точной и полной информацией соответствующих должностных лиц в требуемые сроки;

2) эффективная обработка, введение в память компьютера и распространение информации;

3) обеспечение сохранности сведений с учетом критерия «стоимость- эффективность»;

4) представление максимальных информационных услуг санкционированным пользователям.

Для того, чтобы одновременно обеспечить эффективность и безопасность информации, жизненно важен жесткий контроль за сохранностью документов. Необходимо также уделять внимание защите информации. Немалую помощь здесь может оказать знание возможных угроз компьютерной информации. Непреднамеренные ошибки, т.е. безграмотность и расхлябанность, неправильное введение данных, ошибки в программах, некорректная переинсталляция операционной системы с потерей данных и т.д., являются причинами 55% всех потерь. Деятельность конкурентов и шпионов, утечка информации, несанкционированный доступ, вторжение хакеров, кражи, подлоги и т.п., дают 30% всех потерь. Сбои из-за нарушения кабельной системы и низкого качества электропитания приносят 13% всех потерь. Остальные потери связаны со стихийными бедствиями, пожарами и компьютерными вирусами (Проскуряков, Н. Е., Ануфриева, А. Ю., Ходов, С. И. 2014).

Инвентаризация как путь к порядку

Прежде чем заняться сохранением чего-либо, надо понять, что сохранять. Для этого нужно провести полную инвентаризацию используемых в работе данных и их классификацию, решить вопросы безопасности и секретности.

Следует определиться с уровнем допуска пользователей к различным данным и соответственно структурировать доступ к электронным ресурсам согласно установленным регламентам.

Важно учесть использование антивирусного программного обеспечения и

свежие антивирусные базы. Потеря данных в результате вирусной атаки – одно из наиболее распространенных явлений в нашей практике. Уберечься от данной угрозы можно только при наличии надежного антивирусного программного обеспечения и свежих, актуальных антивирусных баз, использовании на компьютерах только необходимого для работы и проверенного программного обеспечения, постоянное обновление и установка новых версий программ, в которых постоянно решаются вопросы устранения уязвимости.

Обратить внимание на общие данные основных рабочих программ, меняются они ежеминутно, архивироваться должны каждодневно минимум, а лучше и не по разу. Это как правило серверные задачи, т.е. построенные по распределённой архитектуре «клиент-сервер», где данные хранятся на сервере, а клиентские части приложения осуществляют только запросы-транзакции к ним.

Определить пользовательские критичные данные. К пользовательским документам относятся переписка и текущий документооборот. Данные, которые почти не меняется, такие как: информационные материалы, сопутствующие документы, лицензии, учебная литература, должностные инструкции и тому подобное. Как правило, это общедоступная информация, и архивируется изредка, по мере обновления. Хранится на сервере в отдельной папке, фильмы и музыка занимают большие объёмы информации. Учитывая среднюю загруженность пользовательского ПК рабочими данными примерно в 5-10 Гб, и среднюю ёмкость диска современного офисного ПК в 80-120 Гб, можно на каждой машине создать некое пространство на 50-100 Гб для хранения фильмов, музыки и резервных копий. Это может быть, как скрытая от пользователя партиция, так и просто папка с ограниченным доступом. Конечно, не у каждого сотрудника можно заводить такие ресурсы. Централизованно управлять ими не обязательно, надо просто продумать права доступа в первую очередь и не забывать об их каталогизации. На этапе инвентаризации определяемся, кто и что будет копировать, исходя из секретности и важности данных. То есть, что совсем секретно, должен оберегать именно тот, кто не может доверить эту задачу администратору сети. А то, что не имеет значения для организации, должен копировать тот, для кого это имеет значение, то есть пользователь. Результатом инвентаризации должна стать агрегация на сервере всей важной информации, подлежащей защите.

Защита основного места размещения информации

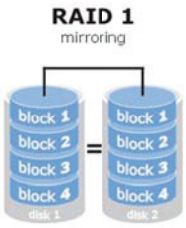
Есть простые, не очень дорогие и эффективные средства минимизации вероятности сбоев ПК, ведущих к разрушению информации. Самые важные – защита по питанию и резервирование жёстких дисков.

Применение ИБП (Источник бесперебойного питания) способно предотвратить возможное разрушение файловой системы или даже физическое повреждение жёсткого диска при пропадании напряжения в питающей сети и частично при нарушении параметров питания. Чем мощнее и дороже решение, тем больше вероятность, что оно справится со своей задачей. Благодаря использованию технологии AVR Bypass, энергоэффективность новых ИБП увеличивается до 97%. При нормальных параметрах электрического сигнала на входе в источник, питание к подключенному оборудованию подается в обход трансформатора ИБП, который задействуется только в случае возникновения нештатных ситуаций. Модели SMT2200 и 3000 могут быть опционально оборудованы настраиваемой системой аварийного выключения EPO, позволяющей экстренно обесточить оборудование, подключенное к ИБП. Напряжение питания порта – 24 В, что соответствует требованиям безопасности.

Жесткие диски выходят из строя достаточно часто, поэтому достаточно давно придумано простое средство борьбы с их отказами. Называется оно

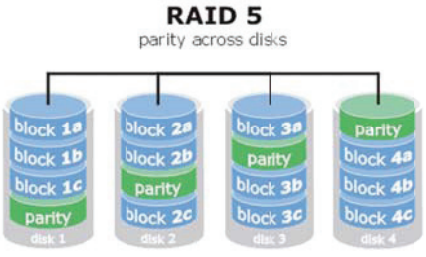
RAID, и в простом случае может быть реализовано просто добавлением ещё одного диска к уже имеющемуся. Затраты на это при современном уровне цен на комплектующие не настолько малы, чтобы рекомендовать использовать во всех машинах, тем более что места на диске много не бывает. Но и не настолько велики, чтобы не использовать зеркалирование там, где цена простоя в работе с восстановлением из вчерашней архивной копии за один сбой составит хотя бы половину стоимости решения. По возрастающей степени сложности и затратности это выглядит так:

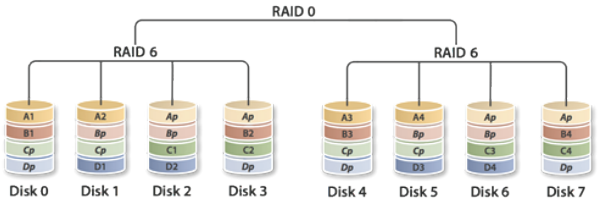
• Два диска в RAID 1 средствами ОС или с использованием встроенного RAID контроллера.



• Минимум четыре (лучше пять-семь по соображениям минимизации потерь дискового пространства и увеличения скорости работы) диска в RAID 5 с обязательным выделением одного в горячий резерв (Hot Spare) для немедленного пересчёта массива в случае отказа, на качественном контроллере со своей памятью и обязательного использования бесперебойного источника питания для корректного завершения работы при пропадании питания, что делает возможным включение к эширования записи.

• Выделенное сетевое хранилище со своей системой обработки данных и высокой надёжностью вплоть до RAID 60 с несколькими резервными дисками.





В нашем случае целесообразно рассматривать два первых варианта. Почему не стоит использовать RAID 5 без «правильного» контроллера? Да потому, что в RAID 1, «зеркале», каждый из двух дисков несёт на себе в явном виде всю необходимую информацию, которую можно снять с него на большом количестве других машин. А вот снять информацию с дисков RAID 5 при сбое к примеру контроллера – задача нетривиальная и не очень дешёвая (Фролов, Александр; Фролов, Григорий 2001).

Сетевые хранилища целесообразно использовать для большей надежности хранения информации.

NAS (Network Attached Storage) – отдельно стоящая интегрированная дисковая система. NAS-сервер обладает специализированной ОС с набором полезных функций быстрого запуска системы и обеспечения доступа к файлам. Система подключается к обычной компьютерной сети (ЛВС) и является быстрым решением проблемы нехватки свободного дискового пространства, доступного для пользователей данной сети. NAS – это хранилище, подключаемое к сети, и как любое сетевое устройство, обеспечивает файловый доступ к данным. NAS-устройства представляют из себя комбинацию Сетевого Хранилища Данных и сервера, к которому она подключена. В простейшем варианте устройством NAS является обычный сетевой сервер, предоставляющий файловые ресурсы.

Второй подход – выделение специального хранилища, к которому пользователи не обращаются, а информация собирается на нём по его запросу через специальную программу, к примеру производства EMC, и её агентов на станциях, где находятся архивируемые данные (Уваров, Сергей 2018).

Облачные хранилища – это общедоступный метод хранения информации широкого использования. Их первое преимущество в том, что к ним можно обращаться с любой точки доступа, это очень удобно для пользователей. В таких хранилищах целесообразно размещать информацию для текущей работы. Существуют 3 модели облачных хранилищ – частное, публичное и гибридное. Конечно наиболее доступное это публичное облачное хранилище. Наиболее известные и популярные: DropBox, Google Диск, Яндекс Диск, MEGA, Облако Mail.ru, 4shared, Files.fm, OneDrive. По функциональным возможностям и предоставляемым объемом бесплатного пространства эти хранилища разные (Васильков, Андрей 2016).

Работа Dropbox построена на синхронизации файлов с папкой приложения, установленной на устройствах. Сервис можно использовать не только как облачное хранилище, но и как файлообменник – выкладывать файлы в папку с общим доступом «Public».

Google Диск, Яндекс.Диск и облака Mail.ru – это облачные хранилища данных, очень похожие по своему функционалу. Они хранят файлы своих пользователей в «облаке», позволяют организовать совместных доступ к ним, редактировать в браузере, благодаря наборам офисных приложений.

MEGA в первую очередь является облачным файлообменником. Его основные функции – хранение и передача файлов другим пользователям. Важной особенностью сервиса является шифрование загружаемых данных на стороне клиента, а ключи доступа к файлам распространяются исключительно между доверенными пользователями.

4shared также является облачным файлообменным хостингом с возможностью поиска по категориям и публикации файлов для общего пользования.

Files.fm – это облачное хранилище файлов для компаний и частных пользователей. Сервисом можно воспользоваться без регистрации для обмена – пользователь копирует файлы с компьютера или телефона на сервер и получает на них ссылки.

OneDrive – облачное хранилище данных компании Microsoft. Сервис полностью интегрирован с ОС Windows, папка хранилища доступна сразу после установки системы.

Проектирование системы хранения данных – ключевая задача обеспечения сохранности.

Процесс проектирования системы хранения данных, обеспечивающей резервное копирование, архивирование, структурированное хранение и восстановление данных в требуемые сроки должен опираться на пофайловый анализ подлежащих хранению данных, рекомендуемый проводить на основе следующей информации о файлах:

- даты создания, модификации, последнего обращения;
- расширение;
- расположение в каталогах файловой системы.

Процесс проектирования системы хранения сетевых данных рекомендуется начинать со сбора и анализа информации о хранящихся в сети данных. По всем серверам и рабочим станциям с критически важными данными необходимо выяснить:

- время работы и требования ко времени восстановления в случае сбоя;
- общий объём установленной дисковой памяти, в т. ч. занятый и свободный объёмы;
- данные о файлах (даты создания, модификации, последнего обращения к ним).

Нужно постараться упорядочить хранящиеся данные, поместив файлы, подлежащие резервному копированию, архивированию и другим видам хранения, в отдельные каталоги. Оценив

реальную скорость копирования/восстановления информации, можно уточнить необходимое число накопителей в устройствах хранения данных.

При очень больших объёмах информации, подлежащей резервному копированию, архивированию и структурированному хранению, становится неудобно осуществлять мониторинг и администрирование этих процессов непосредственно из ПО. В этом случае его интегрируют со средствами сетевого управления. Конечно же при наличии возможности лучше полностью дублировать все пользовательские файлы (кроме медийных) на сервере, или просто их там и хранить, включая профайлы. Заодно такой подход сильно упрощает администрирование домена. Но это не дешёвое решение, такой сервер должен быть весьма мощным и содержать большой объём дисковой памяти с быстрым доступом. Кроме того, пропускная способность сети, и прежде всего концентратора, должна быть достаточной для обеспечения доступа к документам и профайлам без ущерба для скорости работы в основной серверной базе (базах) данных. Если пойти немного дальше от уровня пользователя, то в серверной возможны две реализации такого подхода. Возможно полное дублирование критичной машины, когда на полностью настроенную, но не обслуживающую запросы пользователей её копию периодически сбрасывается вся важная информация с рабочего сервера. Если он не должен работать круглосуточно, то ночью полная копия (при остановленном как правило рабочем процессе и серверной программе) и, возможно, в обеденный перерыв – частичная. В это же время выполняются другие регламентные работы. При полном отказе основного сервера поднять вчерашнюю копию при правильной организации процесса займёт не более часа. Если же обращения к нему идут круглосуточно, то решение проблемы сложнее и дороже, и в данную тему не укладывается. Кстати даже Microsoft позволяет при наличии одной лицензии на серверную ОС устанавливать ещё одну её копию на сервер резерва, правда «холодного», т. е. который постоянно выключен. А то, что мы рассмотрели ранее – это «горячий резерв» с функциями сетевого хранилища.

В вопросе сохранности информации нет понятия «дорогое решение», есть понятие соответствия цены решения уровню предоставляемой надёжности и сервиса. Раньше для резервного копирования и архивного хранения чаще всего использовались ленточные накопители, с кассетами с магнитной лентой и автоподатчиками. Используются и сейчас из-за большой ёмкости кассет, но всё реже и реже, в связи с удешевлением решений на базе жёстких дисков. Библиотеки на основе оптических носителей всегда были скорее экзотикой, чем массовым товаром. Итак, сейчас в основном применяются просто серверы с большим дисковым пространством. Надёжные комплектующие, мощные блоки питания, хороший SATA/SAS контроллер на пять – десять каналов, те самые пять – десять дисков в RAID 5, не быстрые, но ёмкие. В принципе, количество дисков на один сервер может быть достаточно большим, но это уже дорого за счёт специализированных корпусов и блоков питания, да и контроллеры с большим количеством каналов не дёшевы (вот SCSI поддерживает до 14 устройств, а на SATA портов меньше обычно). А десяток дисков можно разместить в стандартном корпусе 2-3U, и остальные комплектующие использовать массовые, если такой термин применим к рынку серверных комплектующих.

А вот самое главное это подходящая под задачу и правильно настроенная программа для реализации этой задачи. Диапазон здесь очень широк, от встроенных средств операционной системы (слабо), через самописные скрипты до мощных специализированных пакетов, предоставляющих максимально гибкие и удобные инструменты. Но на каком уровне реализации системы «близкого копирования» остановиться в аппарат-

ном и программном обеспечении, решать надо исходя из оценочной стоимости информации и простоя в работе в данном конкретном случае

Следует обратить внимание на методы архивного хранения. Информация в оперативных хранилищах переписывается ежедневно, а зачастую хочется посмотреть данные годовой давности, а то и глубже. Поэтому архив является не заменой, а дополнением к текущему резервированию. Возможно полное архивирование данных. Точнее невозможно, поскольку ВСЕ изменения в течении дня отследить затруднительно, и слепок делается в лучшем случае один-два раза в сутки.

Резервное копирование делится на: ***полное, инкрементальное* и *дифференциальное.***

При *полном резервном копировании* создаётся копия всех данных, подлежащих резервному копированию. Недостаток процедуры – необходимость значительного времени на её осуществление и значительного числа и (или) объёма резервных носителей; достоинство – быстрое восстановление информации.

При *дифференциальном копировании* дублируются только файлы, созданные или измененные со времени проведения последнего полного копирования. Чем больше это время, тем дольше будет осуществляться дифференциальное копирование. В случае краха системы для восстановления данных приходится задействовать последние полную и дифференциальную копии.

При *инкрементальном копировании* дублируются только те файлы, которые были созданы или изменены после последнего полного, дифференциального или инкрементального копирования. Время выполнения такого копирования относительно мало, но в случае утраты информации её придётся восстанавливать, используя последнюю полную и все последующие инкрементальные копии – самая длительная процедура восстановления.

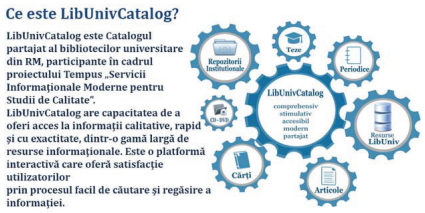
Наиболее приемлемая схема, минимизирующая время резервного копирования данных и их восстановления – еженедельное полное и ежедневное инкрементальное копирование.

Информация раз в сутки копируется, сжимается архиватором. В идеале это второй сервер, настроенный так, что в случае сбоя основного он сможет быстро и легко принять на себя все его функции. Там хранится ежедневный архив за неделю. Всё это по достижении объёма сменного носителя или чаще копируется на два таких носителя. И происходит это всё с максимально возможной степенью автоматизации. Вот тогда системный администратор может особо не переживать за сохранность данных и непрерывность рабочего процесса.

Внедрение методов сохранности информации в Научной Библиотеке Бэлцького Государственного Университета имени А. Руссо

На текущий момент Научная Библиотека оснащена компьютерным парком из 116 рабочих станций, подклеенных в локальную сеть с выходом в интернет, 6-ю серверами на которых размещены веб-сайт библиотеки, файл сервер SAMBA с внутренними документами, сервер базы данных MoldLex, институционный репозиторий DSPACE, Прокси сервер с программой SQUID и сервер базы данных TinLib, TinRead с библиографическим описанием документа и локальным хранилищем полнотекстовых документов.

В рамках участия в проекте MISISQ в научной библиотеке USARB внедрена новая система базы данных ALEPH-EXLIBRUS PRIMO. Это облачная база данных, находящаяся на удалённом сервере в научной библиотеке кишиневского мед университета. В научной библиотеке USARB проинсталлировано 29 лицензий рабочих модулей CIRCULATIE, ACHIZITIE, CATALOGARE. Доступ для пользователей осуществляется через веб-интерфейс PRIMO-мощный поисковый инструмент, который позволяет включать результаты с разных баз данных.

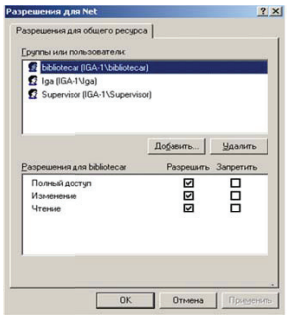


Настройка локальных компьютеров пользователей

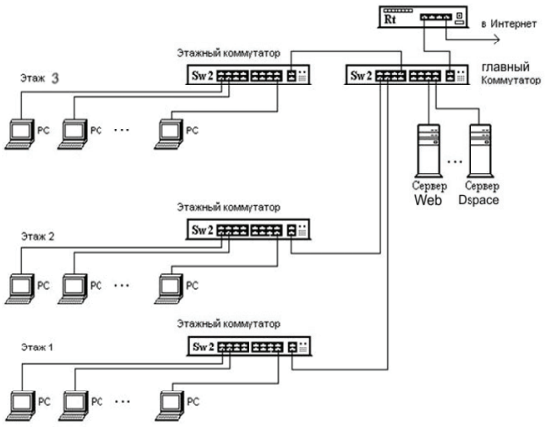
Настройка локальных компьютеров пользователей

На пользовательских компьютерах установлен только перечень необходимых для работы пакетов программного обеспечения. Используются последние версии операционной системы с доступными обновлениями. Настроена система безопасности Firewall, оптимизированы службы для быстрого доступа при помощи программы утилиты Auslogics BoostSpeed. Установлено и обновлено бесплатное антивирусное программное обеспечение Avast Antivirus. В браузерах системы установлено антирекламное и антивирусное расширение. Использование обновленного компьютерного парка обеспечивает возможность установки новых пакетов программ и оперативного доступа к информации.

Политика безопасности информации в Научной Библиотеке USARB состоит из следующих аспектов: безопасность информации на локальных компьютерах, включающее в себя ограничение доступа к ресурсам компьютера на уровне пользователей, безопасность информации в локальной сети, которая определяется ограничением доступа пользователей к сетевым ресурсам сети. Для этого в BŞ USARB существуют 3 категории пользователей: UTILIZATOR – с ограниченными правами, BIBLIOTECAR – с расширенными правами и SUPERVISOR – пользователь, имеющий доступ ко всем сетевым локальным ресурсам.



Настройка инфраструктуры локальной компьютерной сети

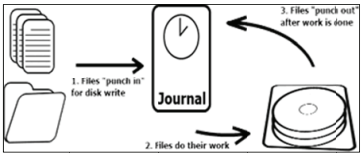


Локальная сеть построена по следующему принципу: все сервера и коммуникационное оборудование рабочих станций подключены к главному коммутатору с большой производительностью 1000 мб/сек., что обеспечивает быстрый доступ и минимизирует количество коллизий в локальной сети, обеспечивает равномерное распределение нагрузки на коммуникационное оборудование локальных станций.

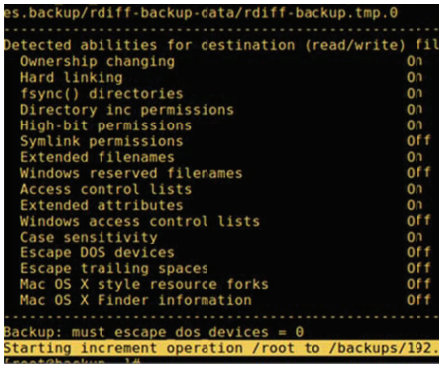
В свою очередь это обеспечивает надежность передачи данных по локальной компьютерной сети.

Осуществляется программное разграничение уровня приоритета пользователей по скорости доступа и привилегиям в доступе. Выполняется это при помощи настройки коммутаторов через веб-интерфейс. Выход в интрасеть осуществляется через прокси сервер по определенным установленным портам, что повышает уровень безопасности доступа.

Настройка архивирования серверов

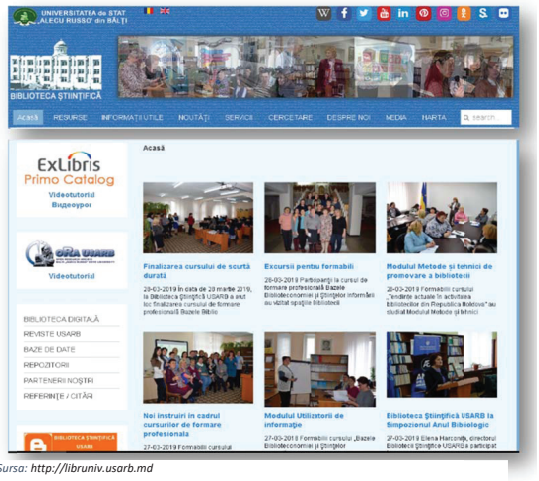


И главный аспект – это безопасность информации, содержащейся на серверах. Политика безопасности информации, содержащейся на серверах определяется постоянным обновлением серверных программ, что решает проблему уязвимости, а также использование новых типов файловых систем, оснащенных новыми методами журнализации и обеспечивающие лучшую систему защиты от сбоев, более быстрый доступ к дисковому пространству. На серверах с открытым доступом в интернет, наряду с установленными программами аутентификации и firewall, использовать программы защиты от хакерских атак. Мы используем программу denyhosts которая позволяет блокировать несанкционированный доступ к серверу.



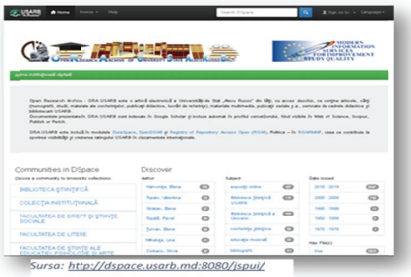
Для формирования архивов информации, разработаны скрипты, которые в установленное время осуществляют копирование и сжатие информации, архивные дубликаты переписываются на другие 2 сервера. Для экономии времени и трафика при копировании используется утилита RDIFF, которая только освежает архивные дубликаты.

Веб-сайт библиотеки libruniv.usarb.md построен на движке Joomla, поэтому его сохранность включает в себя ежедневное создание backup таблиц базы данных сайта и архивирование файлов самого сайта. Осуществляется хранение четырех хронологических копий архива и делаются дубликаты архивов на двух других серверах для надежности.



Sursa: http://libruniv.usarb.md

Репозиторий ORA USARB также использует базу данных. Сохранность включает в себя ежедневное архивирование данных при помощи встроенной в Dspace функции AIP-EXPORT, которая сохраняет как сами статьи, так и структуру коллекций и данные о пользователях. Периодически делается полное дублирование файлов и базы данных репозитория и дубликаты переносятся на другой сервер.



Sursa: http://dspace.usarb.md:8080/jspui/

Сервер TinRead ежедневно делает update базы данных из сервера TINLIB с актуальными данными дублируется в архив на сервер JURIST Файл сервер Jurist включает в себя общую директорию Mapa Generala, базу данных MoldLex и таблицы CuprinsScanat. На дополнительном диске хранятся копии

архивов, которые постоянно обновляются по графику, а MoldLex

обновляется с FTP сервера компании MolData.

Заключение

Надо продолжать постоянно совершенствовать систему сохранности информации используя новые прогрессивные технологии, создавать специальные сервера для резервирования данных и использовать новые технологии для резервирования данных. В последнее время развитие получили стримеры, устройства для создания архивов долговременного хранения (Ланц, Марк 2018).

Перспективой развития является установка сервера виртуализации с мощными ресурсами, позволяющими клонировать и создавать копии виртуальных машин. Виртуальный выделенный сервер характеризуется стабильной и надежной работой. Виртуальные выделенные сервера, расположенные на одной хост-машине, работают независимо друг от друга. Таким образом, неисправности функционирования одного сервера не повлияют на работу другого. Кроме этого, виртуальные выделенные сервера гарантируют высокую степень безопасности и конфиденциальности для размещаемых данных.

В рамках проекта LNSS в научную библиотеку USARB были приобретены новые компьютеры и сервер Dell PowerEdge R740 и в настоящее время осуществляется работа над созданием виртуального кластера, который позволит более гибко управлять и администрировать серверы, создавать копии всего сервера для надежности и оперативности в восстановлении (Уткина, Л. И., 2017).

Очень перспективное направление – развёртывание терминального сервера. Внедрение использования терминалов – тонких клиентов (компьютеров без жёсткого диска, загружающихся по локальной сети), данные которых хранятся сразу на сервере терминалов. Такой метод позволяет более полно и точно сохранять данные всех рабочих станций.

Терминальный сервер – это единое информационное пространство и глубоко интегрированная корпоративная среда для максимально эффективной организации работы, экономии ресурсов, контроля прав доступа и безопасности хранения данных. Терминальный сервер обеспечивает централизацию и контроль прав доступа, перевод пользователей с ПК на тонкие клиенты. Вместо компьютера с данными пользователю устанавливается миниатюрное устройство, которое позволяет подключаться к терминальной сессии. Тонкий клиент не требует обслуживания, не шумит, не греется, потребляет мало электричества. Позволяет свести к минимуму техническую поддержку на рабочих местах.

В заключении хочу отметить, что развитие информационных технологий, стремительный процесс информатизации всех сфер современного общества радикально повлияли на привычные библиотечные технологии: изменили методы сбора информации, ее визуального отображения и обеспечения доступа к ней; преобразовали традиционные формы и методы библиотечного и библиографического обслуживания; трансформировали процессы комплектования, обработки, сохранности фондов. Внедрение передовых интернет-технологий позволяет использовать инновационные библиотечные услуги и сервисы, направленные на удовлетворение потребностей пользователей с учетом особенностей информационного взаимодействия в обществе.

Библиографические ссылки:

1. Lege cu privire la biblioteci Nr. 160 din 20.07.2017. In: *Monitorul Oficial al R. Moldova.* 2017, nr. 301-315, pp. 141-147.
2. БАРАБАНОВ, Алексей, 2006. Современный Linux-сервер : виртуализируем сетевые устройства. Ч. 2. В: Системный администратор, nr. 8, pp. 18-25. ISSN 1813-5579.
3. ВАСИЛЬКОВ, Андрей, 2016. Облачная азбука, или о пользе «непубличных» облаков [online] [citat 25 martie 2018]. Disponibil: https://www.computerra.ru/132947/cloud_abc-and-benefits-of-non-public-clouds/
4. ЛАНЦ, Марк, 2018. Почему будущее хранения данных всё ещё за магнитной плёнкой [online] [citat 18 martie 2018]. Disponibil: https://habr.com/ru/post/422851/
5. ИБП APC Smart-UPS серии SMT для защиты серверов. В: Журнал Сетевых Решений/ LAN [online] 2012, nr. 4 [citat 23 martie 2018]. Disponibil: https://www.osp.ru/lan/2012/04/13014739/
6. Обзор 10+ облачных хранилищ данных [online] [citat 25 martie 2018]. Disponibil: http://www.topobzor.com/obzor-10-oblachnyx-xranilishh-dannyx/.html
7. ПИЛИЧЕВ, Алексей, 2010. О сетях хранения данных [online] [citat 25 martie 2018]. Disponibil: https://habr.com/ru/post/80971/
8. ПОЛЯК-БРАГИНСКИЙ, А. В., 2011. Локальная сеть. Самое необходимое : практическое руководство. Санкт-Петербург : БХВ-Петербург. 576 p. ISBN 978-5-9775-0636-6.
9. ПРИКАЗ Nr. 94 от 17.09.2009 об утверждении некоторых технических регламентов. В: *Monitorul Oficial al R. Moldova.* 2010, nr. 58-60, pp. 35-107.
10. ПРОСКУРЯКОВ, Н. Е., АНУФРИЕВА, А. Ю., ХОДОВ, С. И., 2014. Альтернативные методы хранения цифровой информации на основе гибридных технологий. В: Известия ТулГУ. Технические науки [online], вып. 11, ч. 2, pp. 418-424 [citat 23 martie 2018]. Disponibil: https://cyberleninka.ru/article/n/alternativnye-metody-hraneniya-tsifrovoy-informatsii-na-osnove-gibridnyh-tehnologiy
11. Разработка стратегии резервного копирования [online] [citat 18 martie 2018]. Disponibil: https://system-admins.ru/strategii-rezervnogo-kopirovaniya/
12. Резервирование данных средствами ОС Windows. В: КомпьютерПресс. 2013, nr. 5, pp. 22-24. ISSN 0868-6157.
13. Сетевые устройства хранения (Network Attached Storage, NAS) [online] [citat 20 martie 2018]. Disponibil:
14. http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D1%8B%D0%B5_%D1%83%D1%81%D1%82%D1%80%D0%BE%D0%B9%D1%81%D1%82%D0%B2%D0%B0_%D1%85%D1%80%D0%B0%D0%BD%D0%B5%D0%BD%D0%B8%D1%8F_(Network_Attached_Storage,_NAS)
15. Способы оптимизации работы Хранилищ данных. В: Журнал BPM *World* [online] [citat 12 martie 2018]. Disponibil: http://iso.ru/ru/press-center/journal/2112.phtml
16. Техническая коллекция *Schneider Electric* [online]. 2011, вып. 36: Защита систем от кибер-атак. 110 p. [citat 23 martie 2018]. Disponibil: https://profsector.com/media/catalogs/566dd744e79dd.pdf
17. УВАРОВ, Сергей, 2018. Конференция EMC & Microsoft:Совместные интегрированные решения для крупного бизнеса [online] [citat 25 martie 2018]. Disponibil: https://www.ixbt.com/cm/microsoft-emc2007.shtml
18. УТКИНА, Л. И., 2017. Возможности виртуального выделенного сервера в поддержке сайта компании. В: Огарёв-*Online* [online], nr. 2(91) [citat 18 martie 2018]. Disponibil: https://cyberleninka.ru/article/n/vozmozhnosti-virtualnogo-vydelennogo-servera-v-podderzhke-sayta-kompanii
19. ФРОЛОВ, Александр, ФРОЛОВ, Григорий, 2001. Сохранность и восстановление компьютерных данных: теория и практика. В: *BYTE* [online], nr. 1(30), pp. 67-78 [citat 23 martie 2018]. Disponibil: https://www.bytemag.ru/articles/detail.php?ID=9020
20. ШЛЯХТИНА, Светлана, 2013. Как ограничить доступ к домашнему компьютеру. В: КомпьютерПресс, nr. 8, pp. 13-17. ISSN 0868-6157
21. ЯРЕМЧУК, Сергей, 2006. FreeNAS: строим надежную систему хранения данных. В: Системный администратор, nr. 7, pp. 48-52. ISSN 1813-5579.