CZU 027.7 (478):004.65

МЕТОДЫ СОХРАННОСТИ ЭЛЕКТРОННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ В НАУЧНОЙ БИБЛИОТЕКЕ

METHODS OF PRESERVATION OF ELECTRONIC INFORMATION RESOURCES IN THE SCIENTIFIC LIBRARY

Igor AFATIN

Всё может сломаться. Всё, что может сломаться,
когда-нибудь ломается.
Причём происходит это именно тогда,
когда этого меньше всего хочется.
Мёрфи

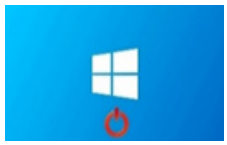
Abstract: *The author reports on USARB's security policy to preserve the information stored on its servers, the types of users who have access to information through the local network, the actions that are performed to ensure data security.*
Keywords: *informational resources, security policy, university library, site, repository*

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

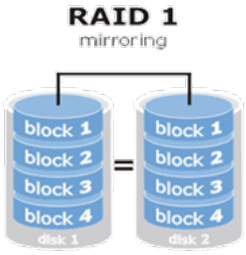
Существует ряд мер, призванных свести к минимуму риск потери информации.

1. Физическое ограничение доступа человека к компьютерам и серверерам. Исключение возможного 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.

2. Ограничение доступа пользователей к файлам, установить пароли на доступ, чтобы посторонний человек не получил доступ к файлам и разделам жесткого диска. Ограничить права доступа к общим папкам в сети.

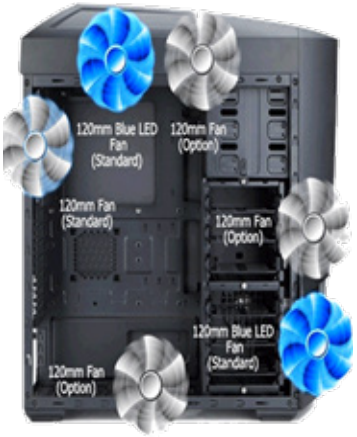


3. Корректно завершать работу операционной системы и приложений. Не допускать аварийного завершения работы.
4. Создание RAID-массива на серверах. Данная мера значительно повышает шансы сохранить информацию в случае физической смерти одного из жестких дисков. Диски выходят из строя достаточно часто и проблема может быть реализована просто добавлением ещё одного диска к уже имеющемуся.

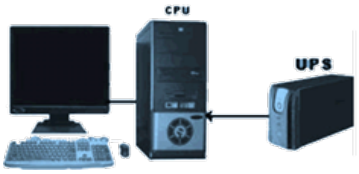


5. Установка программного обеспечения для ежедневного резервного копирования данных в автоматическом режиме. Данная мера спасает от умышленного уничтожения и других случаях потери информации, при автоматически создающихся архивных копиях важных файлов и папок.

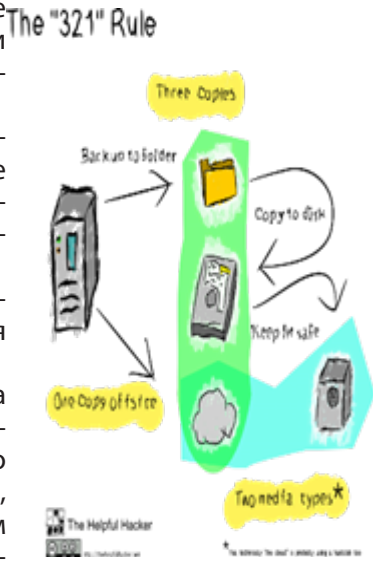
6. Установика дополнительноего охлаждения для жестких дисков на рабочих станциях и серверах. Как известно, электроника не любит жары - перегрев зачастую приводит к некорректной работе оборудования, зависаниям и самопроизвольным перезагрузкам.



7. Использовать источники бесперебойного питания. Тем самым защищая оборудование от перепадов напряжения, которые приводят к некорректному выключению компьютеров. Применение UPS 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.



8. Делать не менее 2-х копий резервных данных на разных носителях. Любая информация, хранящаяся в одном месте, будет потеряна раньше или позже, как бы надёжно это место ни 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.



9. Использование антивирусного программного обеспечения и свежие антивирусные базы. Потеря данных в результате вирусной атаки - одно из наиболее распространенных явлений на практике.

Безопасность электронной информации в научной библиотеке включает в себя ряд аспектов:

1. Политика безопасности информации на локальных компьютерах в подразделениях библиотеки. Первое что необходимо делать, это инвентаризация информации, что является путем к порядку. Прежде чем заняться сохранением чего-либо, надо по-

нять, что сохранять.

Для этого нужно провести полную инвентаризацию используемых в работе данных и классифицировать эти данные по следующему принципу:

а) Определение уровня допуска персонала к различным данным и соответственно структурировать доступ.

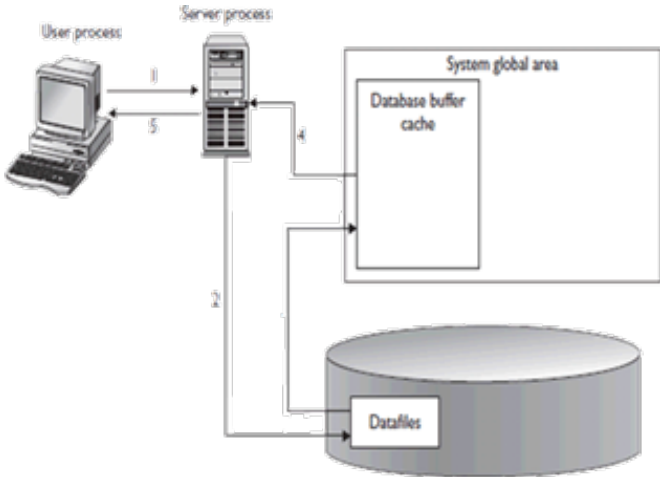
б) Систематизировать работу с Общими данными основных рабочих программ (статистика, базы данных TinLib и TinRead, база данных CuprinsScanat, база данных Aleph-Exlibris, репозиторий ORA USARB, Moldlex), построенных по распределённой архитектуре «клиент-сервер», где данные хранятся на сервере, а клиентские части приложения осуществляют только запросы-транзакции к ним.

в) Выделить пользовательские критичные данные - это переписка и текущий документооборот. В нашей библиотеке вся документация хранится на выделенном файл-сервере с ограниченным доступом только для сотрудников библиотеки. Выделенные данные хранятся в созданных на

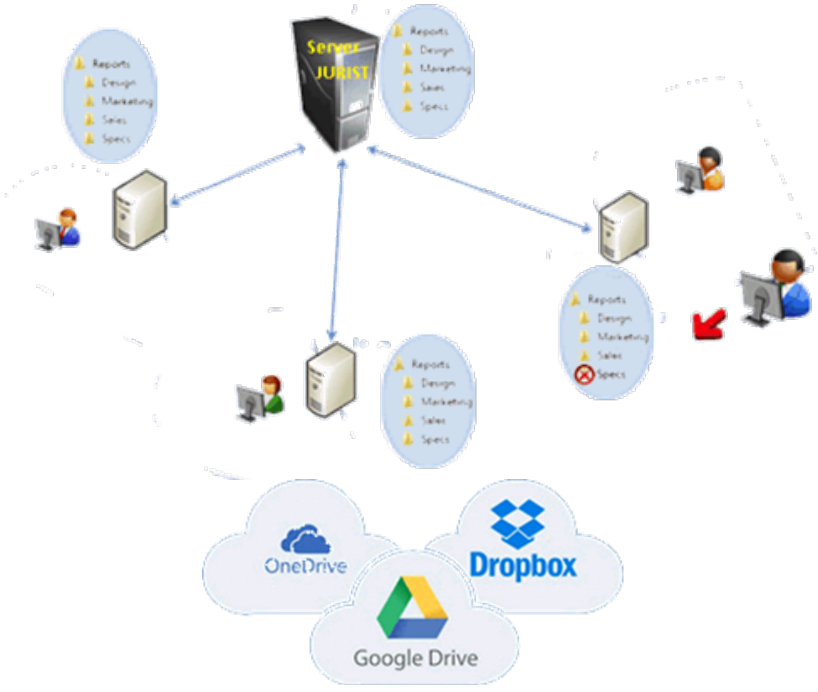
файл-сервере директориях каждого подразделения и в свою очередь эти же данные расположены на рабочих компьютерах подразделений библиотеки.

Есть возможность хранения данных в облачном хранилище.

Для каждого подразделения создана почта@usarb.md которая расположена на сервере Google. В каждой учетной записи есть GoogleDrive облачное хранилище размером в 15 Гигабайт. Также существуют и другие облачные хранилища (Dropbox, OneDrive, Backup, Sync).

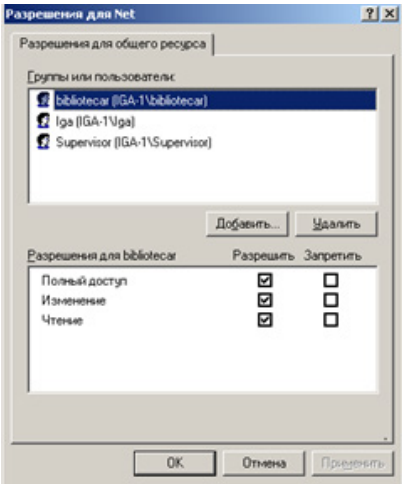


г) Выделить то, что почти не меняется: информационные материалы, сопутствующие документы, лицензии, учебная литература, должностные инструкции и тому подобное. Как правило, это общедоступная информация, и архивируется изредка, по мере обновления. Хранится на файл-сервере в отдельной директории.

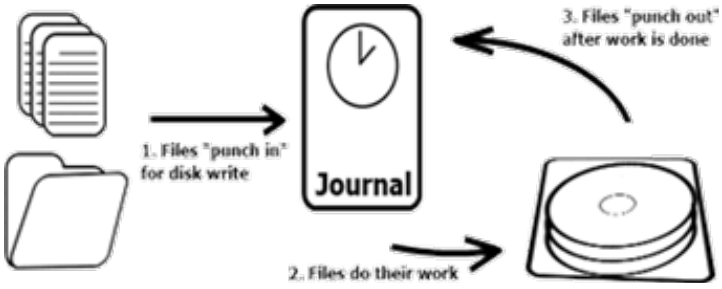


д) фильмы и музыка занимают большие объёмы информации. Поэтому на рабочих компьютерах маркетолога и нотно-музыкального отдела установлены дополнительные диски повышенной надежности для хранения и дублирования мультимедийной информации. Централизованно управлять ими не обязательно, надо устанавливать права доступа, в первую очередь, и не забывать об их каталогизации.

Результатом инвентаризации является агрегация на сервере всей важной информации, подлежащей защите.



2. Политика Безопасности информации в локальной сети определяется ограничением доступа пользователей к ресурсам локальной сети. У нас в этом плане существуют 3 категории пользователей UTILIZATOR - с ограниченными правами, BIBLIOTECAR - с расширенными правами и СУПЕРПОЛЬЗОВАТЕЛЬ, имеющий доступ ко всем сетевым локальным ресурсам.
3. 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. Использовать в полной мере на серверах с открытым доступом в интернет, наряду с установленными программами аутентификации и firewall, программы защиты от хакерских атак, такие как denyhosts и др.



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. Целесообразно хранить 4 хронологические копии архива и делать дубликаты архивов на 2 других серверах для надежности.

Репозиторий ORAUSARB 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.

ORA USARB
OPEN RESEARCH ARCHIVE
OF ALECU RUSSO
BALTI STATE UNIVERSITY

Сервер TinRead ежедневно делает update базы данных из сервера TINLIB с актуальными данными.

Файл сервер Jurist включает в себя общую директорию MapaGenerala, базу данных MoldLex и таблицы CuprinScanat.

На дополнительном диске хранятся копии архивов которые постоянно по графику обновляются, а MoldLex обновляется с FTP сервера компании MolData.

Благодаря выше перечисленным мерам осуществляется безопасность данных в нашей библиотеке. Надо продолжать постоянно совершенствовать систему сохранности информации используя новые прогрессивные технологии, создавать специальные сервера для резервирования данных и использования стримера для создания архивов долговременного хранения.

Внедрение использования терминалов-тонких клиентов (компьютеров без жёсткого диска, загружающихся по локальной сети) данные которых хранятся сразу на сервере терминалов.