УДК 026.06

К. А. Колосов, И. И. Михайленко
ГПНТБ России

Решения для авторизации пользователей ИРБИС на веб-порталах и в локальной сети с использованием программных пакетов OpenLDAP, SQUID-proxy и FreeRadius

Представлены программные решения, разработанные для аутентификации пользователей Системы автоматизации библиотек ИРБИС с использованием протокола LDAP и сервера OpenLDAP, а также варианты аутентификации для доступа к сетевым ресурсам на основе использования прокси-сервера Squid и сервера Radius. Рассмотренные решения могут быть использованы для аутентификации локальных и удалённых пользователей сетевых информационных ресурсов библиотеки, а также авторизации пользователей сети Wi-Fi в помещениях библиотеки.

Ключевые слова: Система автоматизации библиотек ИРБИС, LDAP, OpenLDAP, прокси-сервер Squid, сервер Radius, аутентификация пользователей.

UDC 026.06

Kirill Kolosov and Ilya Mihaylenko
Russian National Public Library for Science and Technology, Moscow, Russia

Solutions for IRBIS users authorization via Internet-portals and local networks with OpenLDAP, SQUID-proxy and FreeRadius software packages

Software solutions for IRBIS user authentification using LDAP protocol and OpenLDAP server, as well as IRBIS user authentification options for Internet resources through Squid proxy-server and Radius www-server are discussed. These solutions can be used for authentification of local and remote users of libraries' networked information resources, and Wi-Fi user authentification within the library physical space.

Keywords: IRBIS Library Automation System, LDAP, OpenLDAP server, Squid proxy server, Radius server, user authentification.

One of the common solutions for authorizing or authenticating users of network resources is the LDAP(Lightweight Directory Access Protocol) protocol. It is an application layer protocol for accessing the X.500 directory service. LDAP is a relatively simple protocol that uses TCP / IP and allows operations such as bind, search and compare, modification or deletion of records. It is of interest to use LDAP to authorize the database of IRBIS readers. One of the approaches to this task is the adaptation of the OpénLDAP software package for data exchange with the IRBIS server. Alternatively, you can adapt the LDAP authorization module, where you can access the built-in LDAP user database and check the combination "user name / password" on the IRBIS server in parallel. The username will act as a conditional group of "LDAP server users", and the input password will have the form of the combination "IRBIS user / IRBIS password". In the module result.c one line is changed, which certifies the authorization of the user. Another line with the same purpose was changed in the module bind.c. Authorization of the squid proxy user using LDAP. This option is provided by the squid settings and provides for the addition of the following lines to the configuration file squid.conf: Authorization of Radius server user using LDAP is provided by FreeRadius settings and requires adding lines to the configuration file: An alternative option for authorizing users of network resources is to call a script that accesses the IRBIS server and returns a response confirming the correctness of the IRBIS / IRBIS user combination. This solution is integrated with the Z64 server running HTTP (SRU / SRW), which then accesses the IRBIS server. The presented authorization options for the IRBIS ILS users can be used to solve a wide range of tasks, including authentication: the library reader with the goal of providing remote access to electronic resources (squid proxy server), the user of the Wi-Fi network library (FreeRadius server); a remote user on the library's web portal (OpenLDAP).

Аутентификация пользователей ИРБИС
с использованием сервера OpenLDAP

Одно из распространённых решений авторизации или аутентификации пользователей сетевых ресурсов – это использование протокола LDAP.

LDAP (англ. *Lightweight Directory Access Protocol* — облегчённый протокол доступа к каталогам) — протокол прикладного уровня для доступа к службе каталогов X.500 [**1**]. LDAP — относительно простой протокол, использующий TCP/IP и позволяющий производить операции как аутентификации (*bind*), поиска (*search*) и сравнения (*compare*), так и добавления, изменения или удаления записей.

LDAP может использоваться для авторизации (аутентификации) пользователей в локальной сети и на веб-порталах при наличии программной поддержки этого протокола. Распространённый вариант – использование программных решений на PHP для LDAP-авторизации, в частности, имеются соответствующие модули для *CMS Joomla* [**2**].

Для разработчиков представляет интерес использование LDAP для авторизации базы данных читателей ИРБИС (база данных RDR). Один из подходов к решению этой задачи – адаптация программного пакета OpenLDAP для обмена данными с сервером ИРБИС. Пакет OpenLDAP – открытое ПО, легко собирается из исходных модулей на любой UNIX-системе [**3**]. Однако особенностью OpenLDAP является использование встроенной базы данных. В принципе можно написать собственный провайдер данных OpenLDAP, и есть примеры решений для использования, в частности, базы данных mySQL [**4**].

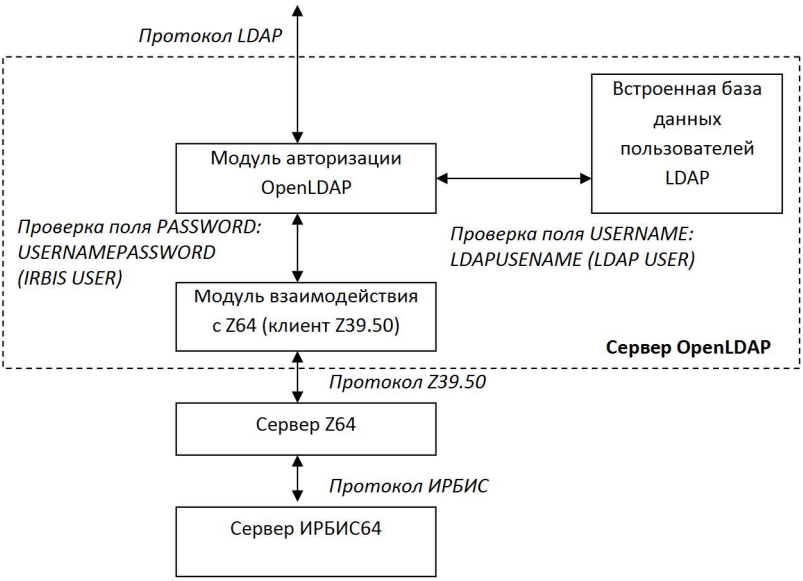
Создание полноценного провайдера данных для взаимодействия OpenLDAP с САБ ИРБИС – задача, требующая значительных усилий. Альтернативным вариантом может быть адаптация модуля авторизации LDAP, при которой сохраняется обращение к встроенной БД пользователей LDAP и параллельно происходит проверка комбинации «имя пользователя/пароль» на сервере ИРБИС. При таком решении имя пользователя будет выполнять функции условной группы «пользователи сервера LDAP», а вводимый пароль будет иметь вид комбинации «*пользователь ИРБИС/пароль ИРБИС*».

Что понимается под паролем читателя САБ ИБРИС? Это может быть любое поле из базы данных RDR, например адрес электронной почты.

На рисунке приведена функциональная схема взаимодействия сервера OpenLDAP с сервером САБ ИРБИС64 через промежуточный сервер Z39.50 (сервер Z64). Для поддержки протокола Z39.50 требуется установка программного пакета YAZ.

Какие модули меняются на сервере OpenLDAP? Изменения затрагивают два модуля – *bind.c* и *result.c*.

В модуле *bind.c* добавлены функции Z39Show (клиент Z39.50), *irbis_check(username,password)* и один вызов функции *irbis_check*, при успешном вызове которой обрабатывается событие «*Пользователь ИРБИС авторизован*» и модулю авторизации сервера LDAP подставляется правильный пароль LDAP пользователя из встроенной базы данных OpenLDAP. В модуле *result.c* изменена одна строка, удостоверяющая авторизацию пользователя. Ещё одна строка с аналогичной целью изменена в модуле *bind.c*. Добавлено ведение журнала авторизации пользователей в отдельном лог-файле.



Функциональная схема аутентификации пользователей САБ ИРБИС с использованием сервера OpenLDAP

Проверка комбинации «*пользователь ИРБИС/пароль ИРБИС*» на сервере Z64 осуществляется с использованием форматного файла *sutrs.pft*, который возвращает пароль пользователя САБ ИРБИС из базы RDR.

Для LDAP-авторизации пользователей САБ ИРБИС можно написать и собственные программные модули, например на языке PHP можно использовать стандартные функции *ldap_connect, ldap_bind* и др.

Авторизация пользователя прокси-сервера Squid с использованием LDAP. Этот вариант авторизации предусмотрен настройками *squid* и предполагает добавление в конфигурационный файл *Squid.conf* строки вида:

auth_param basic program /usr/lib/squid3/squid_ldap_auth -b dc=ru,dc=com -h localhost -D cn=LDAP_user,dc=ru,dc=com -w LDAP_password -f (&(objectClass=person)(cn=%s))

Авторизация пользователя сервера Radius с использованием LDAP. Предусмотрена настройками *FreeRadius* и требует добавления следующих строк в файл конфигурации:

```
ldap {
        server = "127.0.0.1"
        basedn = "cn=%{User-Name},dc=ru,dc=com"
        filter = "(objectClass=person)"
}
```

Использование PHP-скриптов для авторизации пользователей САБ ИРБИС на прокси-сервере *Squid* и сервере *FreeRadius* без использования LDAP

Альтернативным вариантом авторизации пользователей сетевых ресурсов является вызов скрипта, который осуществляет обращение к ИРБИС-серверу и возвращает ответ, подтверждающий правильность сочетания «*пользователь ИРБИС/пароль ИРБИС*». Это решение интегрируется с сервером Z64, работающим по протоколу HTTP (SRU/SRW), который далее обращается к ИРБИС-серверу. Так же просто этот вариант авторизации интегрируется с системой ИРБИС128. При необходимости возможны и другие варианты обращения скрипта авторизации, например через WEB-ИРБИС.

Для прокси-сервера *Squid* авторизация с использованием вызова PHP-скрипта настраивается путём добавления в файл конфигурации *squid.conf* следующих строк:

```
auth_param basic program /usr/bin/php /etc/squid/proxy.php
auth_param basic realm Username and password
```

Файл *proxy.php* при использовании обращения к серверу Z64 по протоколу SRU/SRW имеет следующий вид:

```
        $line = trim(fgets(STDIN));
        $username = rawurldecode($fields[0]);
        $password = rawurldecode($fields[1]);
        $res1="Reject";
        $url='http://192.168.1.3:210/rdr?version=1.1&operation=searchRetrieve&
query=dc.usercheck='.urlencode      ($username).'&maximumRecords=1&record
Schema=user';
        $res=file_get_contents($url);
        $pos=strpos($res,"<zs:numberOfRecords>");
        if ($pos>0)   $res1=substr($res,$pos+20,1);
        if ($res1=="0") $res1="ERR";
        if ($res1=="1") $res1="OK";
        fwrite(STDOUT,$res1."\n");
```

Как следует из приведённого фрагмента кода, сервер САБ ИРБИС возвратит ненулевое значение найденных в базе RDR-записей в случае, если пользователь ввёл верный идентификатор *username* (например, номер читательского билета). Разумеется, здесь можно добавить проверку пароля пользователя, выбрав для него любое значение из списка значимых полей базы данных RDR, например адрес электронной почты.

При работе с САБ ИРБИС128 используется аналогичный скрипт, который обращается к серверу ИРБИС посредством вызова:
$url='http://test.gpntb.ru/?id=WIrbis&action=GPNTB/AuthBasic&kv=PROXY&login='.urlencode($username).'&pw='.urlencode($password);

Разработчики сервера *FreeRadius* тоже предусмотрели режим авторизации пользователей с использованием вызова скрипта. Особенности использования скрипта на PHP и сервера *FreeRadius* описаны в интернете [5].

Для включения данного типа авторизации в файле конфигурации *raddb/site-available/default* требуется добавить следующие строки:

```
update control {
    Auth-Type := `/usr/bin/php5 -f /usr/local/etc/raddb/check.php '%{User-Name}' '%{User-Password}'`
        }
```

Скрипт *check.php* аналогичен скрипту, используемому для авторизации *Squid*, только задействованы другие значения, возвращаемые сервером *Radius*. При успешной авторизации возвращаемое значение – "*Accept*", при ошибке авторизации – "*Reject*".

Таким образом, представленные варианты авторизации пользователей САБ ИРБИС могут использоваться для решения широкого круга задач, включая аутентификацию: читателя библиотеки с целью предоставления удалённого доступа к электронным ресурсам (прокси-сервер *Squid*), пользователя Wi-Fi-сети библиотеки (сервер *FreeRadius*), удалённого пользователя на веб-портале библиотеки (OpenLDAP).

Представленные программные решения, скрипты и примеры их настройки будут выложены на форуме пользователей САБ ИРБИС (http://irbis.gpntb.ru) для свободного использования.

СПИСОК ИСТОЧНИКОВ

1. **Lightweight** Directory Access Protocol. – Режим доступа: https://www.ldap.com

2. **LDAP** Authentication. – Режим доступа: https://docs.joomla.org/LDAP_Authentication

3. **Open** LDAP community developed LDAP software. – Режим доступа: http://www.openldap.org

4. **How** to install OpenLDAP with MySQL as backend data on Debian 6 64-bit. – Режим доступа: http://www.wingfoss.com/content/how-to-install-openldap-with-mysql-on-debian6

5. **Не совсем** стандартный подход к организации доступа к WiFi сети (Cisco WLC -> FreeRadius -> PHP -> страничка в сети). – Режим доступа: https://habrahabr.ru/post/190156/
__Ne sovsem__ standartnyy podhod k organizatsii dostupa k WiFi seti (Cisco WLC -> FreeRadius -> PHP -> stranichka v seti).

Kirill Kolosov, *Cand. Sc. (Engineering), Head, Internet-complex and Digital Libraries Research and Optimization Department, Russian National Public Library for Science and Technology;*
kolosov@gpntb.ru
17, 3rd Khoroshevskaya st., 123298 Moscow, Russia

Ilya Mikhailenko, *senior researcher, Russian National Public Library for Science and Technology; programmer, ELNIT International Association;*
vrmoro@gmail.com
17, 3rd Khoroshevskaya st., 123298 Moscow, Russia