

Krzysztof Doliński  
Krzysztof Moskwa  
Barbara Urbańczyk  
Biblioteka Główna i OINT  
Politechnika Wrocławska, Wrocław

# Zdalny dostęp do elektronicznych źródeł informacji w środowisku akademickim

## STRESZCZENIE

Omówiono rozwiązania umożliwiające uprawnionym użytkownikom dostęp do płatnych serwisów książek i czasopism elektronicznych oraz bibliograficzno-abstraktowych baz danych spoza sieci komputerowej uprawnionej instytucji. Zarysowano tendencje światowe oraz opisano rozwiązania stosowane w polskich ośrodkach akademickich, ze szczególnym uwzględnieniem doświadczeń Biblioteki Głównej i OINT Politechniki Wrocławskiej.

## WSTĘP

Powszechny dostęp do Internetu, coraz szersze oferty bibliotek akademickich w zakresie prenumeraty czasopism i książek elektronicznych oraz baz danych, a także rozwój nauczania na odległość spowodowały duże zainteresowanie wśród bibliotekarzy i użytkowników zdalnym dostępem do elektronicznych źródeł informacji. Zagadnienie to znalazło się także w kręgu zainteresowań wydawców i dostawców zajmujących się tworzeniem i dostarczaniem tych źródeł oraz ustalaniem warunków licencji regulujących korzystanie z nich [1]. Coraz więcej licencji zezwala na szeroki dostęp do prenumerowanych źródeł informacji użytkownikom afiliowanym (*Authorised User*) przy licencjobiorcy, bez względu na fizyczne miejsce ich pobytu (instytucja, dom, podróż służbowa, staż, praktyka).

Zadaniem biblioteki jest umożliwienie takiego dostępu uprawnionym użytkownikom przy pomocy narzędzi informatycznych zapewniających bezpieczną komunikację. Elementami bezpiecznej komunikacji między użytkownikiem a źródłem są procedury uwierzytelniania (*Authentication*) i autoryzacji (*Authorisation*), które zapewniają identyfikację w stopniu wystarczającym do przyznania uprawnionej osobie prawa dostępu.

## DOSTĘP ZDALNY – ROZWIĄZANIA ŚWIATOWE

Zarządzanie dostępem do prenumerowanych elektronicznych źródeł informacji, zarówno w obrębie instytucji jak i zdalnym, jest dużym wyzwaniem dla bibliotekarzy akademickich na całym świecie [2]. Najbardziej rozpowszechnionym sposobem dostępu jest kontrola adresów IP komputerów, która sprawdza się tylko wtedy, gdy użytkownicy znajdują się w obrębie instytucji. Kontrola taka jest wygodna dla użytkowników, którzy nie muszą logować się oraz dla administratora, który podaje producentowi źródła jedynie zakres adresów IP instytucji. Metoda ta nie rozwiązuje problemu autoryzacji użytkowników znajdujących się poza instytucją. Innym sposobem kontroli dostępu do zasobów, także spoza domeny instytucji, są indywidualne hasła. Jest on niewygodny przede wszystkim dla użytkowników, gdyż muszą pamiętać identyfikatory i hasła przypisane licznym źródłom informacji udostępnianym przez bibliotekę.

Na świecie istnieje kilka rozwiązań powszechnie stosowanych w bibliotekach akademickich, które wychodząc naprzeciw wymaganiom użytkowników, umożliwiają bezpieczny i wygodny zdalny dostęp do zasobów. Popularnym rozwiązaniem są serwery proxy [3] posadowione na terenie biblioteki i posiadające numer IP instytucji. Działają one jak pośrednik między użytkownikiem końcowym, a danym źródłem elektronicznym. Z punktu widzenia wydawcy lub właściciela bazy

wszyscy korzystający mają ten sam adres IP – adres serwera proxy. Każda instytucja posiadająca serwer proxy musi utrzymywać jego oprogramowanie i w miarę zwiększania się liczby użytkowników zwiększać także jego moc. Po stronie czynności użytkownika pozostaje jedynie odpowiednie skonfigurowanie przeglądarki. Innym także często wybieranym rozwiązaniem są tzw. serwery EZproxy (*URL rewriters*). Nie wymagają one konfiguracji przeglądarki i pracują na zasadzie dynamicznej zmiany URL.

Popularnym rozwiązaniem stosowanym w bibliotekach niemieckich, realizującym zdalny dostęp do zasobów elektronicznych jest VPN (*Virtual Private Network*) [4]. Używa on istniejącej infrastruktury sieci publicznej, najczęściej Internetu. Transmisja danych jest szyfrowana a użytkownik musi znać hasło do serwera VPN. Protokoły do tworzenia połączeń nazywane są tunelowymi, najpopularniejsze z nich to: PPTP (*Point-to Point Tunneling Protocol*), L2TP (*Laser 2 Tunnelling Protocol*), IPSec (*IP Security Protocol*), SSL (*Secure Socket Layer*). Wybór najodpowiedniejszego z nich zależy od takich czynników jak system operacyjny klienta, wykorzystywane zasoby, wymagany poziom bezpieczeństwa.

Rozwiązaniem stosowanym od 1995 roku w Wielkiej Brytanii jest ATHENS (<http://www.athensams.net>), system autoryzacji dostępu do licencjonowanych źródeł informacji, produkt konsorcjum Eduserv. System ten jest używany w Wielkiej Brytanii przez ponad 2 000 instytucji. Ponad 300 dostawców informacji elektronicznej akceptuje go jako bezpieczny sposób dostępu do własnych zasobów, a liczba zarejestrowanych kont użytkowników przekracza 3 000 000. System ATHENS stanowi centralne repozytorium organizacji, nazw kont i haseł. Daje on każdej organizacji możliwość zarządzania kontami użytkowników, przyznawania odpowiednich uprawnień oraz ich szczegółową kontrolę. Ta metoda autoryzacji wymaga współpracy ze strony wydawców, którzy muszą wprowadzić do swoich produktów protokoły ATHENS. Jeśli jej nie akceptują to trudno zaistnieć im na brytyjskim rynku bibliotekarskim. Stanowi to też dodatkowy problem dla bibliotek, które muszą posiadać alternatywny system autoryzacji do takich zasobów.

Nowym rozwiązaniem, któremu coraz więcej uwagi poświęcają bibliotekarze i wydawcy jest projekt typu *open source* o nazwie Shibboleth realizowany przez konsorcjum Internet2 (<http://shibboleth.internet2.edu>), zrzeszające ponad 200 uniwersytetów współpracujących z gospodarką i przemysłem. Jest to system autoryzacji użytkownika, który przy pomocy przeglądarki z obsługą cookies, przekierowań, SSL, Java Script, może łączyć się z zasobami elektronicznymi, do których jest uprawniony. Obecnie wdrażanych jest wiele projektów z zastosowaniem tego systemu: PAPI w Hiszpanii, SWTCHAAI – *the Swiss Education and Research Network Authentication and Authorization Infrastructure* w Szwajcarii, FEIDE – *Federated Electronic Identity* w Norwegii, PERSEUS – *Portal Enabled Resources via Shibbolized End-User Security* w Anglii. Projekt Shibboleth, w odróżnieniu od ATHENS, jest systemem rozproszonym. Każda z instytucji musi zainstalować oprogramowanie na własnym serwerze. Podobnie jak w przypadku ATHENS ta forma autoryzacji wymaga również akceptacji wydawców. Należy wspomnieć o jeszcze jednym sposobie sprawdzania wiarygodności użytkownika, jakim jest certyfikat cyfrowy X.509. Biblioteki w tym przypadku muszą zarządzać przydziałem certyfikatów dla poszczególnych osób, a wydawcy muszą takie rozwiązanie akceptować.

Coraz częściej w bibliotekach, zarówno polskich jak i zagranicznych, zastosowanie znajdują wyspecjalizowane systemy zarządzania zasobami elektronicznymi zapewniające bezpieczny dostęp do nich również z komputerów spoza instytucji. Dwa z nich to HAN i OneLog.

System HAN (*Hidden Automatic Navigator*) jest komercyjnym narzędziem firmy H + H Software GmbH (<http://www.hh-software.com>) przeznaczonym dla instytucji zdalnie udostępniających swoje zasoby. Jest instalowany lokalnie w domenie instytucji jako moduł serwera Apache i zapewnia jednolity sposób logowania do wszystkich zasobów, niezależnie od metod autoryzacji stosowanych przez wydawców. Uwzględniając potrzeby związane z zarządzaniem specyficznymi zasobami, jakimi są czasopisma elektroniczne, pozwala na logowanie do całych serwisów lub poszczególnych tytułów. Rozwiązanie takie umożliwia kontrolę subskrypcji pojedynczych tytułów, a w przypadku szczególnych zapisów licencyjnych - ograniczenie liczby symultanicznych użytkowników korzystających z danego źródła. HAN zapewnia m.in.

uwierzytelnianie i autoryzację użytkowników w oparciu o identyfikator i hasło, adres i/lub zakres IP, LDAP (*Lightweight Directory Access Protocol*) będący prostym protokołem dostępu do informacji katalogowych, poprzez który możemy odwołać się do innych, istniejących już baz użytkowników i w nich weryfikować ich uprawnienia. System udostępnia jednolite statystyki obejmujące informacje o wykorzystywanych źródłach, czasie i dacie ich użytkowania, użytkownikowi lub ich grupie, pojedynczych komputerach lub zakresach IP. System HAN nie wymaga od użytkownika instalowania żadnego dodatkowego oprogramowania, logowanie do zasobu odbywa się z poziomu przeglądarki internetowej. Jednak warunkiem koniecznym, by HAN mógł realizować dla użytkowników dyskretną automatyczną nawigację po licencjonowanych e-źródłach, jest posiadanie przez instytucję prostej strony internetowej lub platformy prezentującej e-źródła. Dzięki niej możliwa jest wymiana istniejących odsyłaczy na wygenerowane przez system odsyłacze „hanowskie”. Przekierowują one użytkownika na serwer Apache z zainstalowanym HAN-em, jednocześnie weryfikując uprawnienia i logując do systemu.

System OneLog firmy *Info Technology Supply* (<http://www.its.com.pl>) jest profesjonalnym narzędziem służącym do sieciowego zarządzania zasobami elektronicznymi, także tymi, które pierwotnie były na nośnikach CD i DVD. Umożliwia łączenie się przy pomocy osobistego identyfikatora i hasła, z zasobami chronionymi na podstawie adresu IP, także z komputerów spoza wyznaczonego zakresu. Udostępnia interfejs WWW, który może być personalizowany przez użytkowników. Rozwiązanie techniczne oparte jest na systemie operacyjnym Windows oraz serwerze WWW Apache. Wewnętrzną bazą danych jest *MySQL*. Interfejs WWW wykorzystuje technologię *PHP*. Łączenie z zasobami realizowane jest przy pomocy niestandardowego języka skryptowego. System zawiera bazę skryptów, a wszystkie nowe tworzone są przez serwis firmy ITS. Sercem systemu jest *OneLog Web Router*, zintegrowany router WWW systemu OneLog, działający jak serwer proxy (*Rewriteable Proxy Server*), generujący w podobny sposób strony WWW. OneLog rejestruje wszystkie czynności wykonywane przez użytkowników i generuje obszernie statystyki wykorzystania zasobów. Do identyfikacji użytkowników OneLog może używać wewnętrznej bazy systemu lub zewnętrznych baz użytkowników, np. LDAP. Dla prawidłowego łączenia się z zasobami, OneLog wymaga na komputerze-kliencie jednorazowej instalacji przeglądarki *OneLog Scripting Browser*, będącej wtyczką (*plug-in*) do wielu typów przeglądarek. System OneLog jest prosty w obsłudze, zarówno dla użytkownika, jak i osoby administrującej, której przeszkolenie zajmuje zaledwie kilka godzin.

Coraz częściej, sami wydawcy lub twórcy baz danych umożliwiają dostęp do chronionych zasobów spoza sieci komputerowej instytucji. Do takiej grupy zaliczają się m.in.: EBSCO Publishing (<http://www.ebsco.com/>), ProQuest Information and Learning (<http://il.proquest.com/>), Wiley (<http://www.wiley.com/>). Instytucja posiadająca dostęp do pełnotekstowych baz EBSCO i ProQuest otrzymuje również narzędzie administracyjne z funkcją kontroli dostępu do baz. Administrator może dopisać do zbioru zakresów IP uprawnionej instytucji stałe numery IP komputerów domowych użytkowników lub przyznać im identyfikatory i hasła. W takim przypadku wydawcy przenoszą odpowiedzialność za prawidłowe nadawanie uprawnień na licencjobiorcę. Użytkownik platformy InterScience Wiley'a (<http://www.interscience.wiley.com/>) – którym może być również gość odwiedzający instytucję w ramach dostępu publicznego – samodzielnie zakłada osobiste konto w serwisie i pracując na komputerze znajdującym się w domenie instytucji aktywuje usługę *Roaming Access* umożliwiającą 90-dniowy zdalny dostęp do zasobów Wiley'a, który można po upływie tego czasu reaktywować.

### **ZDALNY DOSTĘP W POLSCE**

Jednym z pierwszych rozwiązań umożliwiających w instytucjach akademickich w Polsce zdalny dostęp do chronionych zasobów elektronicznych było uruchomienie usługi RAS (*Remote Access Service*) dla pracowników Uniwersytetu Warszawskiego, zapoczątkowane w lutym 2002 roku. Usługa wykorzystywała łącze telefoniczne i numer dostępowy przyznany Bibliotece UW na podstawie umowy zawartej z operatorem telekomunikacyjnym. Skierowana była wyłącznie do uprawnionych użytkowników inicjujących połączenie z Internetem spoza domeny UW poprzez

modem. System autoryzował użytkowników dzięki przyznanym identyfikatorom i przypisanym im hasłom. Choć usługa była bezpłatna, to jednak użytkownik ponosił koszty połączenia modemowego z Internetem zgodne z cennikiem opłat operatora telekomunikacyjnego. Usługę RAS zlikwidowano w lutym 2006 roku, zastępując ją systemem HAN, który umożliwił użytkownikom UW zdalny dostęp niezależnie od sposobu uzyskiwania przez nich dostępu do Internetu.

Nieco wcześniej, w 2004 roku przeprowadzono testową instalację systemu HAN w Bibliotece Politechniki Wrocławskiej. Funkcjonalność systemu umożliwiającą naukowcom pracę z licencjonowanymi zasobami na komputerach domowych zyskała przychylność użytkowników. Jednak konieczność cyklicznej (2-3 razy w roku) i czasochłonnej aktualizacji wykazu e-czasopism, zawierającego ponad 20 000 odsyłaczy i generowania dla niego odsyłaczy „hanowskich” sprawiła, że w 2005 roku rozpoczęto testy, zaimplementowano i wdrożono system OneLog. W tym samym roku system OneLog wdrożono w Bibliotece Uniwersytetu Śląskiego.

W 2005 roku testy i wdrożenia różnych systemów zdalnego dostępu rozpoczęło kilka ośrodków akademickich. System HAN zaimplementowano w Bibliotece Uniwersytetu Adama Mickiewicza w Poznaniu oraz Bibliotece Głównej Politechniki Warszawskiej. Nowatorskie w skali kraju rozwiązanie zaproponował Uniwersytet Mikołaja Kopernika w Toruniu. Zespół Uczelnianego Centrum Informatycznego wdrożył mechanizm jednokrotnego logowania CAS (*Central Authentication Service*) współpracujący z bazą katalogową LDAP odpowiedzialną za uwierzytelnianie oraz aplikacją autoryzującą użytkowników PAPI (*Point of Access to Providers of Information*), tworząc system jednorodnego dostępu do licencjonowanych zasobów [5].

Od stycznia 2006 roku system HAN funkcjonuje w Bibliotece Głównej Akademii Ekonomicznej w Krakowie. Biblioteki uczelni medycznych wybrały rozwiązania bezkosztowe, wykorzystujące serwery pośredniczące. Od początku roku serwer proxy świadczy usługi dla użytkowników Collegium Medicum Uniwersytetu Jagiellońskiego, w kolejnych miesiącach to rozwiązanie zastosowano w bibliotekach akademii medycznych w Gdańsku, Białymstoku, Lublinie, Poznaniu i Wrocławiu. Od czerwca 2006 r. zdalny dostęp realizowany przez VPN oferuje swoim użytkownikom Politechnika Śląska.

Tab. 1 Zdalny dostęp do licencjonowanych zasobów w uczelniach publicznych (sierpień 2006)

Typ uczelni (liczba)	Zastosowane rozwiązanie					Łącznie
	HAN	OneLog	proxy	VPN	inne	
techniczne (20)	1	1	–	1	–	3
uniwersytety (18)	2	1	–	–	1	4
medyczne (10)	–	–	6	–	–	6
ekonomiczne (5)	1	–	–	–	–	1
artystyczne (18), rolnicze (7), teologiczne (7), pedagogiczne (6), wychowania fizycznego (6), wojskowe i oficerskie (6)	–	–	–	–	–	–
<b>Łącznie (103):</b>	<b>4</b>	<b>2</b>	<b>6</b>	<b>1</b>	<b>1</b>	<b>14</b>

Analiza danych przedstawionych w tabeli obejmuje zdalny dostęp realizowany przez wyższe uczelnie publiczne podległe Ministerstwu Nauki i Szkolnictwa Wyższego (67), ale również uczelnie wyższe o charakterze publicznym podlegające resortom: kultury (18), zdrowia (10), obrony (5), gospodarki morskiej (2), administracji (1), w sumie 103 ośrodki akademickie. Nie uwzględniono uczelni niepublicznych oraz publicznych wyższych szkół zawodowych, które choć nielicznie, to jednak w ostatnich latach zaczynają coraz częściej przystępować do krajowych konsorcjów udostępniających publikacje elektroniczne. Tendencja ta stanowić może podstawę obserwacji w kolejnych latach.

Podział według profili uczelni przejęto, z nielicznymi korektami, z materiałów ministerstw (<http://www.kprm.gov.pl/112.htm>). Do grupy uczelni technicznych zaliczono również akademie morskie w Gdyni i Szczecinie. Jako niezależną placówkę potraktowano Collegium Medicum UJ w Krakowie, posiadające niezależny serwer proxy. Natomiast Collegium Medicum UMK w Bydgoszczy, za względu na wspólny dla całej uczelni sposób dostępu, ujęto w ramach Uniwersytetu Mikołaja Kopernika.

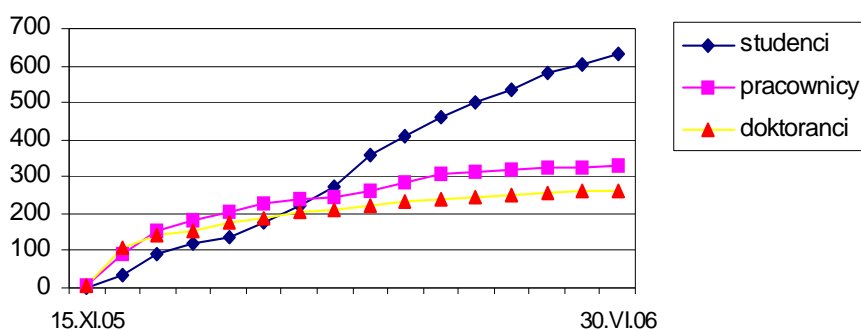
Zestawienie (Tab. 1) wykonano na koniec sierpnia 2006 roku w oparciu o informacje zawarte na stronach internetowych instytucji. Nie obejmuje ono wdrożeń testowych prowadzonych w tym czasie w bibliotekach. Spośród 103 bibliotek uczelnianych, 102 biblioteki (99,0%) posiadają własną stronę internetową lub podstronę informacyjną na stronie uczelni umożliwiającą udostępnianie źródeł elektronicznych. 75 bibliotek (72,8%) udostępnia online publikacje elektroniczne, w tym zasoby licencjonowane, zaś 14 bibliotek (13,6%) umożliwia uprawnionym użytkownikom dostęp zdalny. Większość spośród bibliotek oferujących usługę wybrała rozwiązanie, które nie generuje kosztów związanych z zakupem oprogramowania (proxy, CAS + PAPI, VPN).

Ze względu na typ uczelni możemy zaobserwować dynamiczne działania bibliotek uczelni medycznych, 6 z nich (60,0%) zezwala, aby ich uprawnieni użytkownicy mogli korzystać zdalnie z zasobów chronionych poprzez jednorodne środowisko serwerów proxy. Wpływ na taką dynamikę mogą mieć specyficzne potrzeby użytkowników, jakimi są lekarze, ale również bliska współpraca bibliotek i wymiana doświadczeń poprzez organizację wspólnych szkoleń i seminariów. Cztery biblioteki uniwersyteckie (22,2%) korzystają zarówno z różnych systemów komercyjnych, jak i rozwiązań opartych na licencjach otwartych.

Z grupy bibliotek uczelni technicznych 3 biblioteki (15%) realizują usługę wykorzystując systemy komercyjne i rozwiązania otwarte. Uczelnie o profilu ekonomicznym reprezentuje 1 instytucja (20%) świadcząca usługę w oparciu o system płatny. W przypadku pozostałych typów uczelni wyższych (artystyczne, rolnicze, teologiczne, pedagogiczne, wychowania fizycznego, wojskowe) brak jest informacji o stosowaniu narzędzi umożliwiających zdalny dostęp do zasobów.

### OneLog w POLITECHNICE WROCŁAWSKIEJ

Zakup systemu OneLog poprzedzony był trzymiesięcznym testem, który wykazał, że jest to bardzo przydatne i pozytywnie oceniane przez użytkowników narzędzie, umożliwiające korzystanie z elektronicznych zasobów biblioteki poza siecią uczelni, szczególnie z komputerów domowych. Pierwszej instalacji systemu, wykonanej przez firmę ITS, towarzyszyło szkolenie administratorów, bibliotekarzy i użytkowników. W czasie prób skoncentrowano się głównie na technicznej stronie realizacji połączeń z OneLogiem, a także testowano połączenia z poszczególnymi zasobami udostępnianymi przez system. Zdobyte w ten sposób pierwsze doświadczenia zaowocowały powstaniem „Instrukcji technicznej” dla użytkowników. Opracowano także formularz „Deklaracji użytkownika systemu OneLog”, który od chwili rozpoczęcia właściwej eksploatacji systemu (15 listopada 2005) może być przysyłany także drogą elektroniczną. W teście wzięło udział 200 osób.

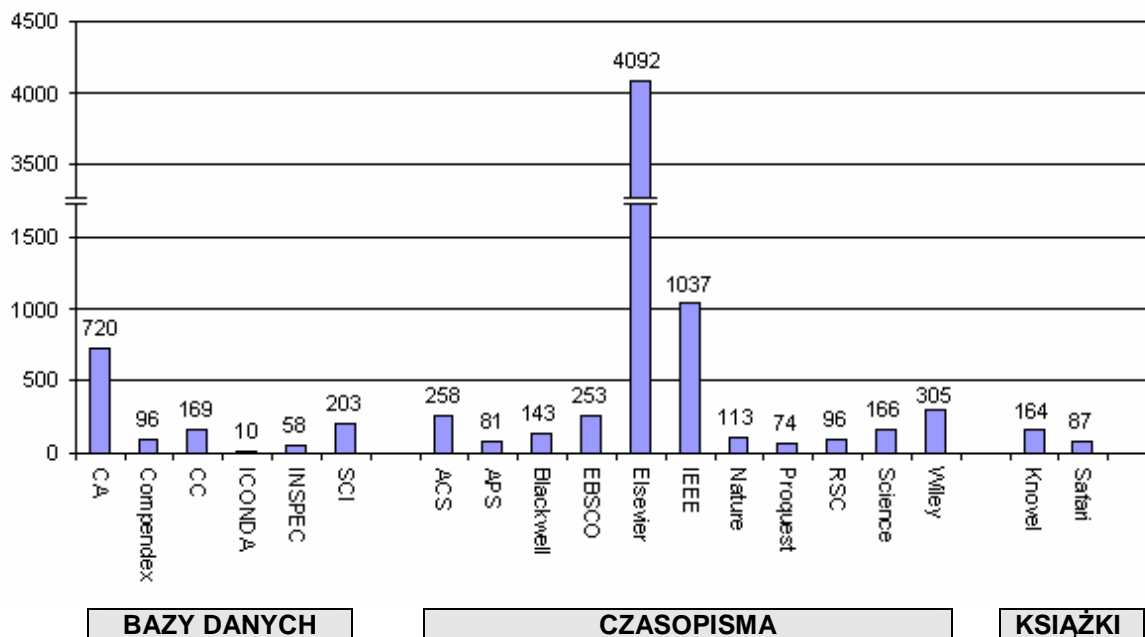


Rys. 1 Użytkownicy systemu OneLog

OneLog został kupiony i wdrożony z myślą przede wszystkim o pracownikach i doktorantach, a także w dalszej kolejności o studentach Politechniki Wrocławskiej. Wg stanu na dzień 30.06.2006, w systemie zarejestrowanych było 1 227 użytkowników, w tym 663 studentów, 331 pracowników i 263 doktorantów. Na rys. 1 przedstawiono dynamikę przyrostu liczby użytkowników. Można zauważyć stały wzrost zainteresowania korzystaniem z OneLoga przez studentów.

Warunkiem korzystania z systemu jest wypełnienie i podpisanie deklaracji, którą można złożyć osobiście, przysłać listownie lub drogą elektroniczną. Trzeci sposób przekazania deklaracji wybrało

507 użytkowników (41%). Po przysłaniu deklaracji, użytkownik jest rejestrowany i wprowadzany do systemu tego samego dnia bądź w dniu następnym i powiadamiany drogą e-mail o aktywacji swojego konta.



Rys. 2 Wykorzystanie licencjonowanych zasobów [w godz.]

Instalacja OneLoga na PWr nie tylko podwyższyła atrakcyjność oferty informacyjnej Biblioteki, ale także zwiększyła wykorzystanie prenumerowanych źródeł elektronicznych (Rys. 2). Największym powodzeniem cieszą się czasopisma elektroniczne, a wśród nich przede wszystkim udostępniane przez Elseviera, IEEE i Wiley'a.

## WNIOSKI

Choć Internet w Polsce jest medium bardzo młodym, w 2006 roku minęło 15 lat jego funkcjonowania, to technologie internetowe bardzo dynamicznie się rozwijają udostępniając nowe usługi. Rozwój kształcenia na odległość, współpraca między uczelniami, staże zagraniczne i wymiana studentów przyczyniają się do wyodrębnienia nowych grup użytkowników z różnymi uprawnieniami i rozproszonymi miejscami pobytu, ale ciągle przynależnych do macierzystej uczelni. Zaspokojenie potrzeb wszystkich grup uprawnionych użytkowników poprzez właściwy dobór elektronicznych źródeł i efektywne udostępnianie ich, także poza domeną instytucji macierzystej, staje się priorytetowym zadaniem każdej nowoczesnej biblioteki akademickiej.

## BIBLIOGRAFIA

- [1] A.Drabek; A.Koziara, „Zasady licencjonowania elektronicznych źródeł informacji naukowej a systemy ochrony sieci komputerowych”, EBIB, Nr 5/2005 (66), <http://ebib.oss.wroc.pl/2005/66/drabek.php> [dostęp: 2006.08.06].
- [2] M.Teets; P.Murray, „Metadata Authentication and Access Management”, D-Lib Magazine, Vol. 12, No 6, 2006, <http://www.dlib.org/dlib/june06/teets/06teets.htm>, [dostęp: 2006.08.06].
- [3] P.Webster, „Remote patron validation: posting a proxy server at the digital doorway”, Computers in Libraries, Vol. 22, No 8, pp. 18-23, 2002.
- [4] R.Gann; R.Janus, „Tunel w Internecie”, PC World Komputer, No 6, pp. 142-144, 2006.
- [5] M.Górecka-Wolniewicz, „Zastosowanie mechanizmów jednokrotnego logowania i systemów autoryzacji użytkowników do obsługi dostępu do baz danych i chronionych zasobów danych”, [W:] Materiały konferencji „Infobazy 2005. Bazy danych dla nauki”, pp. 183-189, Gdańsk 25-27 września, 2005.