Elżbieta Czerwińska
e.czerwinska@po.opole.pl

Anna Jańdziak
a.jandziak@po.opole.pl
Biblioteka Główna Politechniki Opolskiej

OCHRONA ZASOBÓW INFORMACYJNYCH W BIBLIOTECE

Abstract: The emergence of new sources of information (e-sources) forced libraries to a different approach to the protection of library resources. This paper presents the issues of information resources protection. Particular attention was paid to issues related to protection of electronic resources, while seeking to make available collections as the largest range of users.

Słowa kluczowe: ochrona zbiorów bibliotecznych, elektroniczne źródła informacji, bezpieczeństwo informacji, ochrona danych osobowych w bibliotece

Ochrona zbiorów bibliotecznych jest jednym z podstawowych zadań biblioteki, regulowanym ustawowo[1]. Jest ona realizowana poprzez zabezpieczenia techniczne oraz środki wynikające z obowiązujących regulacji organizacyjno-prawnych. Do pierwszej grupy należą zarówno urządzenia chroniące przed kradzieżą, jak i wszelkie środki i metody służące zapobieganiu niszczeniu się zbiorów. Można tu zaliczyć różnego typu bramki przeciwkradzieżowe reagujące na paski magnetyczne lub chipy wklejone do zbiorów, systemy alarmowe reagujące na dym czy ogień, systemy telewizji przemysłowej monitorujące pomieszczenia biblioteczne (magazyny, czytelnie itp.), a także specjalne systemy oświetleniowe, np. zaopatrzone w fotokomórki chroniące zbiory przed nadmiernym działaniem światła słonecznego, specjalne filtry przeciw promieniowaniu UV montowane na okna czy szyby gablot wystawowych itp. Obowiązujące regulacje organizacyjno-prawne zawarte są w aktach prawnych ustanowionych przez urzędy centralne, przepisach i zarządzeniach jednostek zwierzchnich bibliotek oraz regulaminach, instrukcjach opracowanych przez same biblioteki.

O ile urządzenia stosowane do ochrony zbiorów tradycyjnych skutecznie je zabezpieczają, największym problemem dla bibliotek pozostają niezmiennie od lat:

– użytkownicy, którzy nie zwracają wypożyczonych zbiorów. Powodują oni największe straty w księgozbiorach, dlatego coraz częściej biblioteki podejmują kroki prawne celem odzyskania przynajmniej równowartości pieniężnej zagubionych pozycji,

[1] Ustawa o bibliotekach z dnia 27 czerwca 1997 r. (Dz.U.97.85.539).

– zła jakość wydawanych książek. Co roku kilka procent nowo zakupionych pozycji musi być poddawane ponownej oprawie,

– nieprzestrzeganie przez bibliotekarzy procedur (regulaminów). Zdarzają się przypadki wypożyczeń znajomym bez wypełnienia rewersów, wypożyczeń, mimo że czytelnik zalega ze zwrotem książek, wypożyczanie zbiorów poza obręb czytelni bez stosownego zabezpieczenia w postaci kaucji, dokumentu tożsamości,

– kradzieże zbiorów dokonywane przez bibliotekarzy[2],

– zła jakość papieru, na którym zostały wydane książki, czasopisma – tzw. „kwaśny papier",

– zła jakość nośników fizycznych (dyskietek, CD-ROM-ów, DVD). Znane są przypadki, że nośnik po roku przechowywania nie nadaje się do odtworzenia,

– brak odpowiedniego sprzętu odtwarzającego. W każdej bibliotece naukowej znajdują się książki z dołączonymi do nich dyskietkami 5,25", które są dzisiaj martwym zbiorem.

W ciągu ostatnich piętnastu lat w bibliotekach równoprawnymi zbiorami z papierowymi stały się zbiory elektroniczne zarówno te na nośnikach fizycznych, jak i dostępne *on-line*. Poruszając problem ochrony zbiorów elektronicznych należy zwrócić uwagę, że ochronie podlegają zarówno zgromadzone zasoby informacji jak i infrastruktura w postaci systemów informatycznych. Aby prawidłowo chronić zasoby informacyjne należy określić model bezpieczeństwa, mechanizmy kontroli dostępu, poziomy uprawnień dla użytkowników (czytelników i bibliotekarzy), mechanizmy identyfikacji oraz zapewnić możliwość śledzenia zdarzeń w systemie[3].

Podstawowa baza danych w bibliotece jest zawarta w systemie bibliotecznym. Przechowuje ona informacje o gromadzonych, opracowanych i udostępnionych zbiorach, inwentarzach, statystykach oraz dane osobowe zarejestrowanych czytelników. Najczęściej system biblioteczny posiada odpowiednie mechanizmy bezpieczeństwa. Można do nich zaliczyć m. in.:

– identyfikację użytkowników, realizowaną np. przez zabezpieczone indywidualnym hasłem wejście do poszczególnych modułów systemu,

– autoryzację stanowisk i terminali do wykonywania tylko określonych zadań, operacji i usług (np. modyfikacja inwentarzy, realizacja wypożyczeń),

– możliwość analizy operacji wykonywanych w systemie, np. śledzenia zmian zachodzących na kontach czytelniczych i blokowania ich w przypadku naruszenia zasad korzystania, czy to z powodu nieterminowego zwrotu lub zniszczenia wypożyczonych pozycji, czy też utraty ważności karty bibliotecznej czytelnika. Część bibliotek wykorzystuje w swej działalności elektroniczne

---

[2] P. S a r z y ń s k i, *Sępy na kruki*, „Polityka" 2006, nr 8, s. 62–64.

[3] M. E n g e l m a n n, *Bezpieczeństwo informacji – bezpieczeństwo fizyczne*, [dostęp: 27.03.2009], http://www.centrum.bezpieczenstwa.pl/artykuly/BITSR_3_bezpieczenstwo_fizyczne.pdf.

systemy zabezpieczające, np. typu HAN, które dają możliwość monitorowania wszystkich procesów wejścia/wyjścia, a jednocześnie umożliwiają korzystanie z większości źródeł elektronicznych w dowolnym czasie i miejscu, po wykonaniu logowania (zazwyczaj identyfikator użytkownika jest połączony z numerem PESEL jako hasłem),

– automatyczne wykonywanie kopii bezpieczeństwa (np. co godzinę, co dzień itp.) Kopie te powinny być przechowywane w bibliotece i poza nią[4].

Aby chronić informację w bibliotece należy bezwzględnie przestrzegać obowiązujących przepisów prawa, w tym m. in.:

– ustawy o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 r. z późniejszymi zmianami (Dz.U. 00.80.904),

– ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. z późniejszymi zmianami (Dz.U. 02.101.926),

– ustawy o ochronie informacji niejawnych z dnia 22 stycznia 1999 r. (Dz.U. 99.11.95),

– ustawy o ochronie baz danych z dnia 27 lipca 2001 r. (Dz.U. 01.128.1402),

– ustawy o dostępie do informacji publicznej z dnia 6 września 2001 r. (Dz.U. 01.112.1198),

– ustawy o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002 r. (Dz.U. 02.144.1204),

– rozporządzenia Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. 05.171.1433),

– rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 04.100.1024).

Przepisy prawa zezwalają na wykorzystywanie istotnej części baz danych systemów bibliotecznych (własnych i zakupionych) dla użytku osobistego, celów naukowo-dydaktycznych i badawczych. W przypadku naruszenia przez użytkownika (czytelnika, bibliotekarza) zasad korzystania producentowi bazy przysługuje prawo do roszczeń.

Kwestie dostępu do kupowanych przez bibliotekę baz danych regulują licencje zawierane z wydawcą danej bazy. Najczęściej dane z baz udostępnianie są na podstawie numerów IP, które obejmują stanowiska komputerowe sieci uczelnianej. W przypadku funkcjonowania na terenie biblioteki czy uczelni bezprzewodowej sieci WiFi, często wprowadza się obowiązek jednorazowej

[4] *Strategie i modele gospodarki elektronicznej*, red. C. Olszak, E. Ziemba, Warszawa 2007, s. 409–415.

rejestracji komputera przenośnego, aby umożliwić identyfikację jego właściciela. Część dostawców umożliwia korzystanie z baz danych ze stanowisk spoza sieci, w oparciu o pisemne zobowiązanie i po nadaniu indywidualnych haseł dostępu. Wszyscy użytkownicy baz muszą przestrzegać wewnętrznych regulaminów zawierających m. in. następujące zasady:

– z baz mogą korzystać wyłącznie pracownicy i studenci danej jednostki wykorzystując ją wyłącznie do celów naukowych i dydaktycznych,

– zabrania się udostępniania baz osobom postronnym,

– każdy korzystający z baz zobowiązany jest do przestrzegania obowiązującego w tym zakresie ustawodawstwa,

– można wykonywać wydruki materiałów poprzez druk on-line, off-line, czy przesyłać je pocztę elektroniczną,

– kopiowanie wydruków uzyskanych z baz, jak również wszelkie ściąganie i przechowywanie kopii elektronicznych uzyskanych z baz powinno służyć tylko do użytku osobistego lub wewnętrznego,

– zabrania się użytkownikom ściągania całości lub części baz w celu stworzenia lokalnej kopii zbioru materiałów, bez względu na to, czy zbiór taki ma postać elektroniczną, czy też drukowaną oraz używania skryptów i programów automatyzujących proces pobierania danych z baz.

Ważnym zagadnieniem jest przestrzeganie polityki prywatności. Biblioteki mogą tworzyć bazę danych osobowych tylko z elementów niezbędnych do identyfikacji użytkownika oraz dających możliwość kontaktowania się z nim, przy jednoczesnym uzyskaniu jego zgody na przetwarzanie danych osobowych. Dostęp do bazy danych osobowych powinien być ograniczony do określonej grupy pracowników (np. oddziału udostępniania), którzy podpisują stosowne zobowiązanie do ochrony tychże danych. Stanowiska z dostępem do bazy powinny być zabezpieczone zgodnie z zasadą „czystego ekranu" oraz „czystego biurka". Pierwsza z nich odnosi się do stanowisk z dostępem do bazy danych o użytkownikach i wymaga zablokowania klawiatury oraz włączenia wygaszacza ekranu zabezpieczonego hasłem przy każdorazowym odejściu od komputera. Zasada druga nakazuje nie pozostawiać na wierzchu żadnych dokumentów zawierających dane poufne i bezwzględnie chować je w zamkniętych szafach[5].

Należy również pamiętać, że funkcje systemowe usuwające dane z nośników (twardych dysków, dyskietek, CD-ROM-ów,) nie gwarantują 100% pewności, że danych tych nie da się ponownie odczytać. W tej sytuacji konieczne jest fizyczne niszczenie urządzeń lub nośników przechowujących ważne dane. Jeśli nośniki te służą do przechowywania danych osobowych to istnieje ustawowy wymóg usunięcia z nich danych w sposób uniemożliwiający ich odzyskanie[6].

---

[5] M. E n g e l m a n n, *op. cit*.

[6] *Ibidem*.

Pomimo ciągłego rozwoju zabezpieczeń bardzo ważnym ogniwem w systemie nadal pozostaje człowiek. To do bibliotekarza należy bowiem nadzór nad bezpieczeństwem gromadzonych zbiorów i przestrzeganie zasad polityki bezpieczeństwa, bez których nawet najbardziej skomplikowane systemy zabezpieczeń i wejść do biblioteki nie uchronią zasobów bibliotecznych przed zniszczeniem lub utratą. Do najczęściej spotykanych nieprawidłowości w tym zakresie można zaliczyć:

– zbyt krótkie i łatwe do rozszyfrowania hasła dostępu do informatycznego systemu bibliotecznego,

– łatwy dostęp do nich osób postronnych (hasło umieszczone na monitorze, biurku),

– używanie niezmienionych haseł dostępu,

– serwery przechowujące dane nie posiadają macierzy dyskowych pozwalających na równoległy zapis danych,

– pozostawianie kluczy w drzwiach pomieszczeń bibliotecznych, które bibliotekarz w danym momencie opuścił,

– likwidacja sprzętu komputerowego bez fizycznego zniszczenia dysków twardych,

– wykorzystywanie za zgodą bibliotekarzy sprzętu służbowego przez osoby trzecie,

– usuwanie dokumentów zawierających dane osobowe bez użycia niszczarek (deklaracje, kartoteki czytelników),

– nietworzenie przynajmniej codziennych kopii bezpieczeństwa,

– nieprzestrzeganie przez bibliotekarzy przepisów, zarządzeń, regulaminów i instrukcji.

Zarówno ustawowe zasady bezpieczeństwa, jak i zidentyfikowane nieprawidłowości wymagają odpowiednich zapisów w wewnętrznych regulaminach bibliotecznych oraz stworzenia odpowiednich procedur bezpieczeństwa, które będą przestrzegane przez wszystkich pracowników biblioteki i jej użytkowników. W związku z gwałtownym rozwojem technologii informacyjnych będą się zapewne pojawiały nowe rodzaje zagrożeń dla zasobów informacyjnych zgromadzonych w bibliotekach i dlatego trzeba je na bieżąco monitorować i utrzymywać odpowiedni poziom bezpieczeństwa systemów bibliotecznych. Słusznym wydaje się stwierdzenie, że wraz z dalszym rozwojem źródeł elektronicznych nastąpi przeniesienie zasobów bibliotecznych z fizycznej strefy biblioteki do świata wirtualnego, a ochronie podlegać będzie przede wszystkim informacja sieciowa.

Bibliografia

E n g e l m a n n M., *Bezpieczeństwo informacji – Bezpieczeństwo fizyczne*, [dostęp: 27.03.2009], http://www.centrum.bezpieczenstwa.pl/artykuly/BITSR_3_bezpieczenstwo_fizyczne.pdf.
M o c y d l a r z M., *Udostępnianie informacji naukowej na nośnikach elektronicznych*, [dostęp: 27.03.2009], http://www.pfsl.poznan.pl/horyzonty/nosniki/5rozdzial.html.
S a r z y ń s k i P., *Sępy na kruki*, „Polityka" 2006, nr 8, s. 62–64.
Strategie i modele gospodarki elektronicznej, red. C. Olszak, E. Ziemba, Warszawa 2007.
Ustawa o bibliotekach z dnia 27 czerwca 1997 r. (Dz.U. 97.85.539).