Andrzej Koziara
Centrum Informacji Naukowej
i Biblioteka Akademicka – Uniwersytet Śląski

Agnieszka Jezierska
Dział Audytu – Uniwersytet Śląski

BEZPIECZEŃSTWO SYSTEMÓW INFORMACYJNYCH PRACUJĄCYCH W MODELU SAAS

Streszczenie: Rozważania analityczne przedstawione w tym artykule nakierowano na zarządzanie biblioteką, które pozwoli kadrom decyzyjnym, z uwzględnieniem zasad bezpieczeństwa informacji, dokonać oceny oferty w sytuacji konieczności wyboru lub zmiany systemu wspomagającego zarządzanie instytucją. W praktyce decyzje o wyborach takich systemów zapadają bowiem najczęściej w zamkniętych gronach najwyższego kierownictwa, bez udziału specjalistów z zakresu bezpieczeństwa informacji. Analizy takie powinny dotyczyć nie tylko systemów informatycznych, lecz również powiązanych ze sobą zjawisk organizacyjnych, społecznych i technologicznych. Intencją autorów było przedstawienie reguł, które mogłyby stać się jednym z wzorców do podejmowania konkretnych decyzji dotyczących organizacji pracy instytucji i zapewniających realizowanie zaprogramowanych usług. Informacje zawarte w artykule mogą również stać się podstawą do przygotowania założeń do budowy architektury systemu wspomagającego pracę instytucji, a w szczególności zapobiec powielaniu poglądu, iż jednym z najważniejszych zadań bibliotekarza systemowego jest dostosowanie biblioteki do systemu wspomagania zarządzania biblioteką. Pogląd ten w sposób wyraźny wskazuje, że wśród kadry zarządzającej panuje przekonanie, iż priorytetowo należy traktować zakup „renomowanego" systemu bibliotecznego, a dopiero później przychodzi czas na refleksję, czy zapewnia on automatyzację i jej wspomaganie w działaniu biblioteki w zakresie zatwierdzonego systemu organizacyjnego usług i instytucji, w której są one świadczone.

Słowa kluczowe: bezpieczeństwo informacji, model SaaS, usługi świadczone z zagranicy, webservices

Wprowadzenie

Piętnaście lat XXI w. to czas bardzo gwałtownych zmian technologii informatycznych, dostrzeżony zarówno przez specjalistów, jak i „zwykłych użytkowników". Kierunki tych zmian bywają różne. Nie zawsze wydają się one racjonalne, a w sytuacjach wymagających podjęcia decyzji dotyczących systemów, które mają być eksploatowane w poszczególnych instytucjach, zmuszają do ich szczegółowej analizy. Inspirująca do podejmowania takich rozważań może być wypowiedź S. Lema: „Mechanizm poszczególnych technologii, zarówno istniejących, jak i możliwych, nie interesuje mnie i nie musiałbym się nim zajmować, gdyby kreacyjna dzia-

łalność człowieka wolna była, na podobieństwo boskiej, od wszelkich zanieczyszczeń mimowiednością – gdybyśmy, teraz czy kiedykolwiek, potrafili zrealizować nasz zamiar w stanie czystym, dorównując metodologicznej precyzji Genezis, byśmy, mówiąc «niech się stanie światło»[1], otrzymywali w postaci produktu końcowego samą tylko jasność bez niepożądanych domieszek". Zainspirowani taką wypowiedzią przystępujemy więc do analizy systemów informatycznych, pracujących w modelu SaaS (Software-as-a-Service).

Jako model systemów obsługi procesów biznesowych instytucji stał się on popularny około 5 lat temu. W dosłownym tłumaczeniu oznacza on dostęp do korzystania z oprogramowania pod postacią usługi, która jest świadczona z dowolnego miejsca w sieci. Według definicji podanej przez Gartner, Inc. „dostawa tak zorganizowanej usługi powinna być świadczona przez dowolny podmiot mający odpowiedni potencjał do jej realizacji i w żaden sposób nie jest obowiązkowo powiązana z producentem oprogramowania".

Głównym odbiorcą wyników opracowania wydaje się więc szeroko pojęte kierownictwo tych instytucji, których podstawowe procesy biznesowe są wspomagane za pomocą narzędzi informatycznych, a efektem przeprowadzonych przez nich analiz powinny być uporządkowane zalecenia związane z wprowadzeniem i utrzymaniem bezpieczeństwa systemów informacyjnych.

Rozważania na temat zapewnienia bezpieczeństwa informacji są szczególnie ważne, gdy do świadczenia takich usług pretenduje firma, która poprzez własność majątkowych praw autorskich będzie stawała się monopolistą rynkowym. Sytuacja taka następuje, gdy świadczenie usług odbywa się w ramach pojedynczych organizacji lub ich grup, a charakter działalności jest jednostkowy lub niszowy.

1. Wdrożenie systemu bezpieczeństwa

Jako podstawę do wdrożenia systemu bezpieczeństwa należy przyjąć wytyczne wydanego w 2012 r. rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, zwane dalej RRM[2]. Szczegółowo omówione zostaną wszystkie warunki w nim wymienione, a dotyczące zapewnienia bezpieczeństwa systemów informacyjnych. Podstawowy materiał w rozważaniach będą stanowiły aktualnie obowiązujące normy wymienione w RRM, będące następcami norm obowiązujących w chwili, kiedy rozporządzenie było wydawane. Należą do nich:

- PN-ISO/IEC 20000-1:2014-01 *Technika informatyczna – Zarządzanie usługami – Część 1: Wymagania dla systemu zarządzania usługami*, która zastąpiła w grudniu 2014 r. obowiązującą w czasie wydawania rozporządzenia PN-ISO/IEC 20000-1:2007,
- PN-ISO/IEC 27001:2014-12 *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*, która zastąpiła w grudniu 2014 r. obowiązującą w czasie wydawania rozporządzenia PN-ISO/IEC 27001:2007,

[1] Lem S., *Summa technologiae*. Wydawnictwo Literackie, Kraków 1967, s. 14.

[2] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r. poz. 526).

- PN-ISO/IEC 27002:2014-12 *Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji*, która zastąpiła w grudniu 2014 r. obowiązującą w czasie wydawania rozporządzenia PN-ISO/IEC 17799:2007,
- PN-ISO/IEC 27005:2014-01 *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji*, która zastąpiła w styczniu 2014 r. obowiązującą w czasie wydawania rozporządzenia PN-ISO/IEC 27005:2010.

Uzupełniająco w rozważaniach będą uwzględnione normy: PN-ISO/IEC 20000-2:2007 – wersja polska: *Technika informatyczna – Zarządzanie usługami – Część 2: Reguły postępowania*, która w obecnej chwili jest nieobowiązująca (wycofana przez Polski Komitet Normalizacyjny), oraz PN-ISO/IEC 24762:2010 – wersja polska: *Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie*, które w przypadku bibliotek naukowych powinny być elementem budowy odtwarzania systemów całej uczelni.

1.1. Wybór modelu systemu

Przystępując do analiz związanych z wyborem modelu pracy systemu, w pierwszej kolejności należy zidentyfikować wszystkie funkcje systemu wspomagającego prace biblioteki, niezbędne do realizacji usług oferowanych przez instytucję. Szczegółową identyfikację należy rozpocząć od wydzielenia procesów niezbędnych do podejmowania poszczególnych usług informacyjno-bibliotecznych, unikając zbędnych powtórzeń, gdyż wiele z nich może stanowić element pozornie różnych usług świadczonych przez bibliotekę. Wybierając klasyczny system biblioteczny, należy pamiętać o tym, by jego budowa pozwalała na bardzo głęboką parametryzację praktycznie wszystkich jego modułów, w tym tych realizowanych najczęściej, tj. włączanie i wyłączanie funkcji lub zmianę sposobu jego działania poprzez deklarację parametryczną zmiennych. Należy pamiętać również o tym, że już we wstępnej fazie prac powinno się zidentyfikować potrzeby rozwojowe i zawrzeć je jako elementy systemu docelowego. Wskazane jest również takie dobranie systemu, by był on zaprojektowany w sposób umożliwiający dostęp do poszczególnych grup danych, zarówno w opcji odczytu, jak i zapisu, i był on realizowany przez szynę integracyjną lub zespół bramek funkcjonalnych, zwanych bardzo często webservices.

W odniesieniu do biblioteki analizy powinno się prowadzić pod różnymi kątami bezpieczeństwa i użyteczności narzędzia używane do informatycznego wspomagania usług bibliotecznych. W pierwszym etapie przygotowania do wprowadzenia ich na terenie instytucji już pracującej należy przystąpić do inwentaryzacji obszarów, w których obecnie jest wykorzystywany system zarządzania biblioteką, oraz tych, które w niedalekiej przyszłości będą podlegać modernizacji lub zostaną zautomatyzowane (wg oceny autorów dla biblioteki jest to przynajmniej 5 lat). W ogólności specyfikacja powinna być sporządzona w zakresie następujących grup działań:

- zespołu modułów obsługujących czynności związane z gromadzeniem, wymianą i opracowaniem zbiorów;
- zespołu modułów związanych z bezpośrednią obsługą czytelnika w zakresie udostępniania zbiorów papierowych najczęściej reprezentowanych poprzez obsługę magazynu i wypożyczalni przystosowanych co najmniej do znakowania zbiorów za pomocą in-

formacji zapisanych w etykietach RFID lub kodach kreskowych oraz czytelników użytkujących karty biblioteczne wyposażone w interfejsy przewodowe i bezprzewodowe identyczne ze specyfikacją Elektronicznej Legitymacji Studenckiej lub kart czytelnika ze zwykłymi kodami kreskowymi;

- zespołu modułów przygotowanych do współpracy zewnętrznych urządzeń technologii bibliotekarskiej: urządzeń do samodzielnego wypożyczania książek, urządzeń do całodobowego samodzielnego zwrotu książek z opcją wyposażenia ich w systemy sortowania, urządzeń do prowadzenia skontrum, dodatkowych urządzeń informacyjnych (jak np. w CINiBA Bookviewer's) udostępniających informacje o zbiorach podobnych na podstawie zapisów w etykietach RFID oraz specjalnie przygotowanych bramek funkcjonalnych pracujących przy systemach wyszukujących, najczęściej OPAC;
- zespołu modułów zintegrowanych lub samodzielnych systemów wyszukujących (multiwyszukiwarek) umożliwiających wyszukiwanie i linkowanie do zbiorów wyszukanych w lokalnym katalogu, katalogach licencjonowanych (najczęściej w ograniczonym lub płatnym dostępie) źródeł dokumentów elektronicznych indeksowanych za pomocą kwalifikowanych zestawów metadanych, dokumentów elektronicznych ogólnodostępnych indeksowanych pełnotekstowo lub za pomocą metadanych;
- zespołu modułów lub aplikacji mobilnych zastępujących na urządzeniach mobilnych klasyczne multiwyszukiwarki wraz z dodatkowymi funkcjonalnościami (np. dla systemów bibliotecznych Uniwersytetu Śląskiego i Uniwersytetu Ekonomicznego w Katowicach wraz z instytucją konsorcyjną CINiBA to system geonawigacyjny wewnątrz- i zewnątrzbudynkowy).

1.2. Modele pracy systemów zarządzania biblioteką

Oprócz analizy standardowych funkcjonalności, jakie powinien dostarczać system wspomagania pracy biblioteki, należy przeanalizować model, w którym system taki będzie pracował. W najbardziej typowych rozwiązaniach można wyróżnić następujące modele pracy systemów zarządzania biblioteką (SZB):

- dostęp do aplikacji SZB zlokalizowanej na serwerach pracujących w serwerowni instytucji będącej użytkownikiem aplikacji (model użytkowany np. w CINiBA). Właścicielem niewyłącznego prawa do użytkowania jest najczęściej instytucja, w której znajduje się instalacja, rzadko mamy do czynienia z licencją czasową subskrypcyjną;
- dostęp do aplikacji SZB zlokalizowanej na serwerach pracujących w serwerowni akademickiego miejskiego ośrodka obliczeniowego (model wykorzystywany np. w Krakowie, Gdańsku i innych ośrodkach użytkujących np. system Virtua). Właścicielem niewyłącznego prawa do użytkowania są najczęściej instytucje, które są obsługiwane, rzadziej instytucje miejskie, które są promotorem użytkowania oprogramowania lub posiadają licencję czasową subskrypcyjną;
- dostęp do aplikacji SZB zlokalizowanej na serwerach pracujących w serwerowni dostawcy komercyjnego (model wynajmu mocy obliczeniowej w „chmurze" prywatnej polskiej lub światowej). Właścicielem niewyłącznego prawa do użytkowania oprogramowania jest najczęściej instytucja, w której znajduje się instalacja, rzadko mamy do czynienia z licencją czasową subskrypcyjną;

- dostęp do aplikacji SZB zlokalizowanej na serwerach pracujących w serwerowni dostawcy komercyjnego (model wynajmu aplikacji). Właścicielem niewyłącznego prawa do użytkowania oprogramowania jest najczęściej dostawca specjalizujący się w wynajmie oprogramowania do celów komercyjnych. W skrajnych przypadkach niektórzy producenci oprogramowania proponują monopolistyczny model dostępu z własnych źródeł (najczęściej zlokalizowanych w niezidentyfikowanej dla odbiorcy „chmurze" obliczeniowej). Model takiego dostępu określamy jako Software-as-a-Service (Saas), czyli po prostu dostawa oprogramowania jako usługi.

Dostęp do aplikacji SZB, a tak naprawdę do danych gromadzonych i przetwarzanych w systemie wspomagania informatycznego, dla każdego z modeli wymienionych powyżej, można realizować na dwa sposoby:

- aplikacją dostępową specjalnie przygotowaną do tego celu przez producenta oprogramowania,
- przeglądarką internetową; możliwe mutacje takiego dostępu zostaną omówione w dalszej części tekstu.

2. Przechowywanie dokumentu w chmurze

Analizując działania, jakie trzeba podjąć, by wykorzystanie aplikacji dostarczanych w modelu SaaS było w całości zgodne z polskim prawem, można stwierdzić uświadomienie sobie specyficznych cech, które wystąpią w sytuacji, gdy dane w sposób świadomy przechowywać będziemy w „chmurach", a zlokalizowanie fizycznych nośników będzie bliżej nieokreślone. Konieczne jest również uświadomienie rzeczywistej odpowiedzialności usługodawcy w przeciwwadze do ryzyka, jakie musi ponieść usługobiorca.

Pierwszym ważnym elementem dla dalszych analiz jest zrozumienie, czym jest sam dokument oraz fakt przechowywania danych w „chmurze". Pojęcie dokumentu nie zostało zdefiniowane przez ustawodawcę na gruncie prawa cywilnego. Polski ustawodawca nie wyjaśnił również tego pojęcia w innych, analogicznych aktach normatywnych[3]. Na gruncie prawa cywilnego procesowego przeprowadzony został tylko podział dokumentów na urzędowe i prywatne. Pojęcie dokumentu elektronicznego zostało natomiast zdefiniowane w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2005 r. nr 64, poz. 565 ze zm.). Zgodnie z art. 3 pkt 2 tej ustawy dokument elektroniczny to stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych. Informatyczny nośnik danych, zgodnie z art. 3 pkt 1 ustawy, to materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej. Cytowana definicja dokumentu elektronicznego, choć nie znajduje wprost przełożenia na grunt prawa cywilnego, wydaje się cennym krokiem ustawodawcy w kierunku porządkowania terminologicznego aktów prawnych. Propozycja definicji legalnej pojęcia

[3] Wyjątkiem jest Kodeks karny, który w art. 115 § 14 zawiera definicję legalną dokumentu, zasadniczo jednak odnosi się ona do przestępstw związanych z wiarygodnością dokumentów.

dokumentu została natomiast przedstawiona w projekcie Księgi pierwszej Kodeksu cywilnego opracowanym przez Komisję Kodyfikacyjną Prawa Cywilnego działającą przy Ministrze Sprawiedliwości pod kierownictwem prof. Zbigniewa Radwańskiego. Zgodnie z art. 105 tego projektu: „Dokumentem jest informacja obejmująca treść oświadczenia woli lub innego oświadczenia, utrwalona w sposób umożliwiający jej zachowanie i odtworzenie". Należy odnotować, że projekt nowelizacji Kodeksu cywilnego wyraźnie przewiduje wprowadzenie formy elektronicznej dokumentu, która będzie równoważna formie pisemnej dokumentu[4].

Zgodnie z wyżej przytoczonymi projektowanymi zmianami Kodeksu cywilnego w zakresie dokumentu elektronicznego, traktując dane w „chmurze" w sposób analogiczny do nich, można powiedzieć, że dane gromadzone w niej są „nośnikiem informacji umożliwiającym jej odtworzenie". Takie ujęcie elektronicznego przechowywania i przetwarzania danych zmienia podejście do usług, w szczególności tych w modelu SaaS, świadczonych przez firmy zewnętrzne.

Na bazie tak zdefiniowanego kontekstu prawnego można ogólnie stwierdzić, że przetwarzanie i przechowywanie danych w „chmurze" obarczone jest następującymi niebezpieczeństwami prawno-organizacyjnymi:

- utratą fizycznej kontroli nad nośnikami;
- ryzykiem związanym z ograniczeniem przez usługodawcę dostępu do danych (awaria, upadłość, zmiany własnościowe czy działania podmiotów trzecich);
- brakiem wpływu na lokalizację nośników, na których zapisane są dane;
- problemem uzależnienia się od jednego dostawcy, w tym problemem:
  - „zwrotu danych",
  - dyslokacji i przeniesienia danych,
  - skasowania danych,
  - interoperacyjności danych z usługami dostawcy „chmury";
- ryzykiem w przypadku przechowywania danych w państwie trzecim, dotyczącym wymagań prawnych (obniżone bezpieczeństwo lub zakaz prawny, jak np. względem danych osobowych);
- ryzykiem uzależnienia działalności instytucji (dostępu do danych) od podmiotu trzeciego;
- ryzykiem zmieniania się ról uczestników procesów w „chmurze" w zależności od warunków;
- ryzykiem wystąpienia podpowierzania;
- nierówną pozycją stron umowy o usługi chmurowe – dominacja świadczącego usługi;
- problemem mapowania i alokacji zasobów (w skrajnych przypadkach ze względu na jeden podmiot z występującym incydentem brak dostępu do całej infrastruktury „chmury" dla innych usługobiorców)[5].

---

[4] Dyląg Ł., *Dokument a dokument elektroniczny w prawie cywilnym – pojęcie oraz istota desygnatu (w kontekście projektu nowelizacji Kodeksu cywilnego i Kodeksu postępowania cywilnego)*, „Kwartalnik Naukowy Prawo Mediów Elektronicznych" 2011, nr 1, s. 8.

[5] Ten fragment tekstu opracowano na podstawie referatu wygłoszonego przez dr. hab. prof. UO, Dariusza Szostka na konferencji „Bezpieczeństwo i niezawodność systemów informatycznych" w Katowicach, w dniu 28 maja 2015 r.

3. Użytkowanie modelu Saas

Analizując powyższe zagrożenia, można stwierdzić, że podjęcie decyzji o użytkowaniu oprogramowania dostarczanego w modelu SaaS to poważne działanie organizacyjne, które musi zostać poprzedzone nie tylko analizami merytorycznymi, lecz również pozyskaniem odpowiedniej kadry zarządzającej, posiadającej umiejętności zapewniające bezpieczeństwo działania instytucji. W powyższym obszarze rozważania skupią się na następujących zagadnieniach:

- kwestie prawne, w tym:
  - warunki umowy, na jakich się ją podpisuje – wybór właściwego prawa w przypadku usługodawcy zagranicznego przy zaleceniu, żeby to było prawo polskie;
  - konstrukcja kontraktu umożliwiająca odpowiedzialność usługodawcy na podstawie europejskich norm dotyczących:
    - odpowiedzialności kontraktowej, tj. za wyrządzone szkody,
    - odpowiedzialności deliktowej, tj. wykonania czynności niedozwolonych,
    - odpowiedzialności świadczącego usługi drogą elektroniczną, w szczególności w zakresie regulacji opisanym w prawie polskim;
  - zagwarantowanie w umowie prawa do audytów i weryfikacji bezpieczeństwa, w tym odpowiedni sposób weryfikacji certyfikatów, którymi legitymuje się usługodawca;
- kwestie organizacyjne, w tym:
  - poziom wypełnienia funkcjonalnego modułów – możliwość i sposób realizacji usług biblioteki za pomocą oferowanego systemu informatycznego,
  - ewidencja uzupełnień systemowych wraz ze sposobem ich realizacji,
  - zgodność systemu organizacyjnego aplikacji z organizacją pracy instytucji i ewentualna konieczność dokonania takich zmian w powiązaniu z obowiązującymi regulacjami prawnymi na poziomie Unii Europejskiej, prawa polskiego oraz prawa lokalnego, np. dla CINiBA, regulacja Uniwersytetu Śląskiego i Uniwersytetu Ekonomicznego w Katowicach oraz wynikających z nich regulaminów wewnętrznych;
- kwestie technologiczne, w tym:
  - sprawy zewnętrzne – warunki dotyczące systemu, do jakiego będzie pozyskiwany dostęp,
  - sprawy wewnętrzne – działania technologiczne, jakie trzeba będzie podjąć w instytucji w celu wdrożenia wykorzystania systemu zewnętrznego.

Przed przystąpieniem do szczegółowego opisu działań niezbędnych przy wprowadzaniu do eksploatacji systemu SaaS należy zewidencjonować przynajmniej część warunków, jakie powinna spełniać korzystnie sformułowana dla nas umowa.

Należą do nich:

- zapewnienie interoperacyjności i przenaszalności danych;
- minimalizacja niebezpieczeństwa „przywiązania" do pojedynczego dostarczyciela usług – dopuszczenie użytkowania danych zapisywanych w formatach;
- pisemne zagwarantowane dostępu do dokumentacji dotyczącej zasad bezpieczeństwa oraz środków technicznych przyjmowanych w poszczególnych centrach przetwarzania danych, nawet jeśli w standardowym układzie takie informacje stanowią tajemnicę usługodawcy;

- pisemne zagwarantowanie w umowie prawa do informacji o fizycznej lokalizacji serwerów oraz macierzy dyskowych, na których są lub mogą być przetwarzane dane (zmiana lokalizacji powinna podlegać zatwierdzeniu przez usługobiorcę);
- pełna, wystarczająca na mocy prawa polskiego, informacja dotycząca podwykonawców i innych instytucji uczestniczących w realizacji usługi chmurowej dostawy oprogramowania wraz z zagwarantowaniem, że każdy z nich spełnia takie same wymagania, jak główny dostawca usługi;
- pisemne zagwarantowanie w umowie raportowania usługobiorcy o wszelkich incydentach dotyczących bezpieczeństwa danych wraz z usuwaniem skutków takich incydentów;
- pisemne zobowiązanie, że usługobiorca pozostaje wyłącznym administratorem danych przekazanych do „chmury", co implikuje, że usługodawca nie ma prawa do decydowania o celach i sposobach przetwarzania danych;
- zagwarantowanie w umowie raportowania usługobiorcy o wszelkich incydentach dotyczących bezpieczeństwa danych wraz z usuwaniem skutków takich incydentów;
- pisemne zagwarantowanie informacji o zobowiązaniach usługodawcy względem organów państwa: policji, prokuratury, służb specjalnych, organów ścigania w powiązaniu z informowaniem usługobiorcy o wszelkich wnioskach dotyczących udostępnienia danych, a także o samym udostępnieniu;
- dokładne ustalenie w umowie zasad przeszukiwania, retencji i usuwania danych dostarczanych przez usługodawcę;
- na mocy ustawy o świadczeniu usług drogą elektroniczną pisemne zagwarantowanie, że usługodawca zapewni usługobiorcy dostęp do aktualnej informacji o szczególnych zagrożeniach związanych z korzystaniem z usługi świadczonej drogą elektroniczną oraz funkcjach i celu oprogramowania lub danych niebędących składnikiem treści usługi, wprowadzanych przez usługodawcę do systemu teleinformatycznego, którym posługuje się usługobiorca, co przekłada się na specyficzny dostęp do dokumentacji, która może stanowić tajemnicę firmy[6].

Biorąc pod uwagę wszystkie wyspecyfikowane powyżej zapisy umowy, można przystąpić do budowy systemu bezpieczeństwa, do którego utworzenia zobowiązują nas krajowe przepisy związane z bezpieczeństwem systemów informacyjnych. Uzupełniając wymienione uprzednio normy i rozporządzenia, nie możemy zapomnieć o przepisach prawnych dotyczących ochrony danych osobowych. Należą do nich:

- ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z późniejszymi zmianami; tekst jednolity na dzień 26 czerwca 2014 r. opublikowany w Dz.U.2014.1182;
- rozporządzenie 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, opublikowane w dniu

[6] Ten fragment tekstu opracowano na podstawie referatu wygłoszonego przez dr. hab. prof. UO Dariusza Szostka na konferencji „Bezpieczeństwo i niezawodność systemów informatycznych" w Katowicach, w dniu 28 maja 2015 r.

1 maja 2004 r. w Dz.U.2004.100.1024 (uwaga: powszechnym błędem wskazywanym przez GIODO jest błędne stosowanie nieobowiązującego rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. ze zmianą z dnia 1 października 2001 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych);

- rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (wzór zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych), opublikowane w dniu 1 maja 2004 r. w Dz.U.2004.100.1025, zmienione obecnie przez rozporządzenie z dnia 11 grudnia 2008 r., opublikowane w Dz.U.2008.229.1536.

4. Polityka bezpieczeństwa

Bazując na tych przepisach, w szczególności na rozporządzeniu dotyczącym systemów teleinformatycznych, można przystąpić do przygotowania podstawowego dokumentu, jakim jest Polityka Bezpieczeństwa Informacji (PBI). Decydując się na korzystanie z usług dostarczanych w modelu SaaS – w PBI konieczne jest nie tylko zdefiniowanie wszystkich sfer informacji, które będą podlegały ochronie, lecz także odniesienie się do zasad związanych z postępowaniem z podmiotami, które będą dla nas świadczyły usługi z wykorzystaniem danych, które są własnością instytucji. W szczególności w polityce tej konieczne są odpowiednie deklaracje dotyczące tych danych, które objęte są na mocy odrębnych ustaw, a które wcześniej nie były uwzględnione, np. dotyczących tajemnicy służbowej lub państwowej. W polityce bezpieczeństwa w szczególny sposób należy opisać zakładane podziały obowiązków pomiędzy biblioteki i firmy, które będą świadczyć usługi dostawy oprogramowania w modelu SaaS, wynikających z wdrożonych procedur ochrony informacji. W polityce bezpieczeństwa informacji oraz w powiązanym z nią systemie zarządzania bezpieczeństwem informacji w szczególności trzeba zwrócić uwagę na elementy opisujące procedury działania systemu wspomagającego instytucji.

W zakresie organizacyjnym będą one dotyczyć:

- utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację – zadanie usługodawcy po stronie serwerowej oraz po stronie klienta usługobiorcy;
- podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji (zadanie leżące głównie po stronie usługobiorcy); należy dążyć do tego, by usługodawca nie miał możliwości bezpośredniego dostępu do danych;
- zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami – zadanie leżące w równej mierze po obydwu stronach, struktura użytkowanego oprogramowania decyduje o tym, w jakim zakresie niezbędne jest wdrażanie adekwatnych środków przez partnerów do określe-

nia w załącznikach do umowy.

W zakresie technicznym będzie to:

- dbałość o aktualizację oprogramowania – zadanie usługodawcy po stronie serwerowej oraz po stronie klienta usługobiorcy;
- minimalizowanie ryzyka utraty informacji w wyniku awarii – konieczne jest ustalenie sposobu robienia kopii bezpieczeństwa oraz miejsca ich przechowywania, w szczególności gdy dane zawierają elementy chronione na mocy odrębnych ustaw, zadanie wspólne obydwu partnerów do określenia w załącznikach do umowy;
- ochrona przed błędami, utratą, nieuprawnioną modyfikacją – w szczególności jest to zadanie usługodawcy;
- stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa – zadanie usługodawcy w zakresie możliwości stosowania, natomiast usługobiorcy w zakresie rzeczywistego wykorzystania;
- zapewnienie bezpieczeństwa plików systemowych – zadanie usługodawcy po stronie serwerowej oraz po stronie klienta usługobiorcy;
- redukcja ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych – zadanie wspólne obydwu partnerów do określenia w załącznikach do umowy;
- zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie oraz niezwłoczne podejmowanie działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa – zadanie wspólne obydwu partnerów;
- zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych – zadanie wspólne obydwu partnerów do określenia w załącznikach do umowy.

5. Szkolenia

Ważnym zadaniem organizacyjnym jest przygotowanie i realizowanie systemu szkoleń personelu. Szkolenia personelu to zadanie, które powinno być realizowane przez usługodawcę, a usługobiorca powinien mieć realny wpływ na program szkoleń. Ma to szczególne znaczenie, gdy powierzane dane są cenne, a musimy zachować pełną kontrolę nad ich kompletnością i integralnością. W przypadku szkolenia personelu własnego trzeba pamiętać, że zgodnie z wymaganiami norm musi być ono prowadzone zgodnie z wcześniej ustalonym harmonogramem i nie tylko zawierać wiedzę i elementy nowe, ale także przypominać o wszystkich elementarnych czynnikach związanych z zagrożeniami bezpieczeństwa informacji, skutkami naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialnością prawną za jej złamanie oraz stosowanie środków zapewniających bezpieczeństwo informacji. W szkoleniach w szczególności należy poruszać tematykę wykorzystywania wszystkich elementów technologicznych, które będą minimalizować ryzyko błędów ludzkich. Wydaje się celowe zobowiązanie usługodawcy do zapoznawania personelu z podstawowymi elementami programu szkoleń prowadzonych wśród pracowników usługobiorcy. Jest to szczególnie ważne w zakresie działania pomocy technicznej, z którą będą kontaktować się pracownicy wykonujący poszczególne operacje związane np. z udostępnianiem księgozbioru.

6. Audyt wewnętrzny

W celu realizacji obowiązku zapisanego w rozporządzeniu Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych należy ustalić model audytu wewnętrznego w zakresie bezpieczeństwa informacji. Jest to szczególnie istotne, gdyż ze względu na sam charakter usługi świadczonej w modelu SaaS systemy takie mogą prowadzić do „wyprowadzenia" informacji z siedziby instytucji. Kwestie te można rozwiązać, zastrzegając sobie w umowie konieczność poddania się usługodawcy audytowi wewnętrznemu usługobiorcy, poprzez zobowiązanie się do poddania audytowi prowadzonemu przez osoby posiadające stosowne uprawnienia. Równocześnie w umowie należy doprecyzować zakres audytu oraz częstotliwość jego prowadzenia. Wskazane jest też, by przed przekazaniem danych do usługodawcy został przeprowadzony audyt otwarcia, którego pozytywny wynik byłby podstawą do przekazania danych i rozpoczęcia świadczenia usług przez usługodawcę. Jednym z elementów kończących okres świadczenia usługi powinien być audyt zamknięcia, którego pozytywny wynik warunkowałby zamknięcie realizacji umowy z potwierdzeniem braku roszczeń pomiędzy stronami umowy o dostawę oprogramowania w modelu SaaS.

7. Zarządzanie ryzykiem

Jednym z najważniejszych elementów, który powinien być opracowywany na każdym etapie przygotowania, zawierania umów, a później realizacji i zakończenia korzystania z dostawy oprogramowania w modelu SaaS jest zarządzanie ryzykiem w bezpieczeństwie informacji. Zarządzanie to powinno odbywać się na podstawie normy PN-ISO/IEC 27005:2014-01. Do najważniejszych elementów niezbędnych do wykonania w analizie ryzyka należą:

- zidentyfikowanie ryzyka, oszacowanie ryzyka z punktu następstw dla działalności instytucji wraz z określeniem prawdopodobieństwa wystąpienia,
- przygotowanie systemu informowania o ryzykach umożliwiającego zrozumienie tych informacji,
- ustanowienie priorytetów postępowania z ryzykiem wraz z działaniami, jakie zostają podjęte w celu jego zredukowania,
- wdrożenie systemu skutecznego monitorowania ryzyk wraz z wprowadzeniem ich przeglądów na etapie zarządzania ryzykiem,
- szkolenie kierownictwa i personelu w zakresie zarówno samego ryzyka, jak i podejmowanych działań zmierzających do jego ograniczenia.

Realizując zadania związane z analizą ryzyka, należy je rozszerzyć na potencjalnego lub realnego dostawcę usług świadczonych w modelu SaaS. Już na etapie negocjowania wstępnych warunków umowy należy ją przygotować w taki sposób, by mieć realny wpływ na różnego typu parametry systemów informatycznych, jak również na procedury zarządzania tymi systemami w zakresie, który leży po stronie usługodawcy. W szczególności wpływ na

procedury usługodawcy w zakresie oceny ryzyka, kryteriów skutków zniszczenia lub braku dostępu do informacji oraz kryteriów akceptowalnych poziomów ryzyka. Jeszcze przed podpisaniem umowy należy w sposób precyzyjny opisać zakres i granice stosowania zarządzania ryzykiem leżące po stronie usługodawcy. Konieczne jest również uzgodnienie z nim sposobów identyfikowania ryzyka, identyfikowania aktywów i powiązanych z nimi zagrożeń wraz z identyfikacją istniejących zabezpieczeń. Na tym etapie nie można także zapomnieć o identyfikacji podatności przez usługodawcę. Na podstawie dostarczonej dokumentacji, przy udziale specjalistycznego zespołu posiadającego realną wiedzę o systemach teleinformatycznych, powinna zostać dokonana analiza kompletności ich wykazu. Już podczas przygotowania do zawarcia umowy o świadczenie usług należy ustalić w stosunku do wszystkich zidentyfikowanych podatności, jaką metodę będziemy stosować w odniesieniu do każdej z nich. Wśród dostępnych opcji jest możliwość wykorzystania modyfikacji ryzyka, zachowania ryzyka, unikania go lub dzielenia się nim. Wykonywana w sposób ciągły analiza ryzyka pozwala na zwiększenie prawdopodobieństwa bezawaryjnej pracy systemów teleinformatycznych wspomagających działanie naszej instytucji.

Podsumowanie

Analizując opisane działania, które powinny być podjęte w celu zorganizowania, zgodnie z obowiązującymi zasadami prawa, użytkowania aplikacji dostarczanych w modelu SaaS, dostrzegamy, że wiele z nich nie występuje, gdy aplikacje pracują na serwerach zarządzanych bezpośrednio przez instytucję. Niemalże identyczna sytuacja występuje również, gdy aplikacje rozmieszczone są na serwerach zarządzanych przez konsorcjantów lub mamy do czynienia z centrami komputerowymi powstałymi jako jednostki przeznaczone do użytku tylko i wyłącznie przez państwowe uczelnie wyższe. Przygotowując się do wyboru modelu systemu, poprzez zbadanie kosztów jego eksploatacji, należy uwzględnić wszystkie miejsca i czynniki, które wpływają na ich powstanie. Optymalny i zbliżony do rzeczywistych wydatków osobowo-rzeczowych jest model ich liczenia nazwany Total Cost of Ownership – TCO. Stosując się ściśle do jego założeń, należy uwzględnić wszystko, co ma jakikolwiek związek z informatycznym systemem wspomagania działalności biblioteki, a prowadzona w ten sposób ocena może wykazać, iż eksploatacja systemu dostarczanego z „chmury" jako SaaS jest znacznie droższa od innych rozwiązań.

Bibliografia

Chmielarz W., *Zarządzanie projektami @ rozwój systemów informatycznych zarządzania*. Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego, Warszawa 2013.

Dyląg Ł., *Dokument a dokument elektroniczny w prawie cywilnym – pojęcie oraz istota desygnatu (w kontekście projektu nowelizacji Kodeksu cywilnego i Kodeksu postępowania cywilnego)*, „Kwartalnik Naukowy Prawo Mediów Elektronicznych" 2011, nr 1, http://www.bibliotekacyfrowa.pl/Content/38782/004.pdf [2.10.2001].

Kodeks karny; dostęp poprzez system Lex Intranet: 2.10.2015 r.

Lem S., *Summa technologiae*. Wydawnictwo Literackie, Kraków 1967, s. 14.

Palonka J., *Zarządzanie umowami z wykonawcami systemów IT*, [w:] *Wyzwania w rozwoju podstaw metodycznych projektowania systemów informatycznych zarządzania*, „Studia Ekonomiczne" nr 128 „Zeszyty Naukowe Wydziałowe Akademia Ekonomiczna w Katowicach", Katowice 2013, s. 63–80.

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r. poz. 526).

Stanek S., *Analiza wybranych koncepcji w obszarze projektowania wymagań*, [w:] *Wyzwania w rozwoju podstaw metodycznych projektowania systemów informatycznych zarządzania*, „Studia Ekonomiczne, Zeszyty Naukowe Wydziałowe" nr 129, Akademia Ekonomiczna w Katowicach, Katowice 2013, s. 137–162.

Szostek D., *Jak bezpiecznie zawrzeć umowę o przechowywanie danych?* Prezentacja z konferencji „Bezpieczeństwo i niezawodność systemów informatycznych" w Katowicach, 28 maja 2015 r. [niepublikowany].