PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
Technika, Informatyka, Inżynieria Bezpieczeństwa 2014, t. II, s. 69–80

http://dx.doi.org/10.16926/tiib.2014.02.05

Alina Gil, Karolina Nowotna
Akademia im. Jana Długosza w Częstochowie
al. Armii Krajowej 13/15, 42-200 Częstochowa
e-mail: a.gil@ajd.czest.pl

OCHRONA DANYCH OSOBOWYCH NA PRZYKŁADZIE WYBRANEGO URZĘDU MIASTA

Streszczenie. W czasach szybkiego rozwoju informatycznego następuje zastępowanie tradycyjnych metod gromadzenia i utrwalania informacji nowoczesnymi skomputeryzowanymi metodami. Gromadzone w sposób elektroniczny dane są łatwiejsze w przetwarzaniu i udostępnianiu. Wzrasta więc ryzyko naruszenia praw osób, których dane są gromadzone w różnych bazach danych, dlatego wymagamy, aby nasze dane były odpowiednio chronione. Pozostawienie skomputeryzowanych baz danych poza prawną regulacją sprzyjałoby ingerowaniu w wolność osobistą jednostki i jej prywatność.
Celem pracy jest przedstawienie tematu ochrony danych osobowych w instytucji administracyjnej, jaką jest urząd miasta. Po zaprezentowaniu terminologii zagadnienia, polityki bezpieczeństwa urzędu, przedstawione zostaną badania, które zostały przeprowadzone za pomocą ankiety weryfikującej stan i poziom bezpieczeństwa danych osobowych, oraz analiza przeprowadzonych badań.
Słowa kluczowe: dane osobowe, ochrona danych osobowych, polityka haseł.

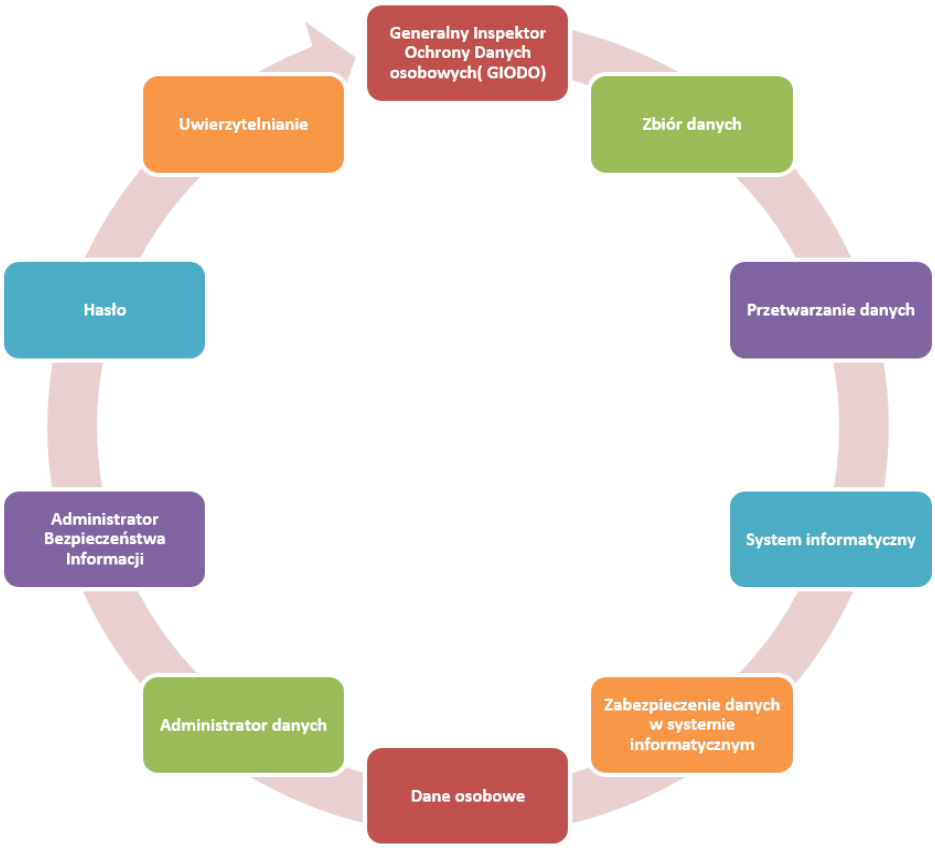
PROTECTION OF PERSONAL DATA ON THE EXAMPLE OF SELECTED MUNICIPALITY OFFICE

Abstract. In times of rapid development in information technology, the modern computerized methods replace traditional methods of collecting and fusing of information. Collected the electronic data are easier to process and make available. Thus increases the risk of infringement of the rights of persons whose data are stored in different databases, so we require that our data are adequately protected. Leaving computerized databases outside legal regulation would facilitate interference with personal liberty of the individual and their privacy.
The aim of this article is to present the subject of protection of personal data in administrative institutions such as the office of the city. After introducing terminology, office

security policy, we present studies conducted using a survey verifying the status and security of personal data, and analysis of the study.
Keywords: personal data, data protection, password policy.

Terminologia

Terminologię związaną z ochroną danych osobowych przedstawia poniższy schemat.



Zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
Przetwarzanie danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie,

opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
System informatyczny – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
Zabezpieczenie danych w systemie informatycznym – to wdrożenie i eksploatacja środków technicznych zapewniających ochronę danych.
Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (np. imię i nazwisko, PESEL, adres zamieszkana… itp.).
Dane osobowe sensytywne (wrażliwe) – szczególna kategoria danych osobowych, co do których istnieje generalny zakaz przetwarzania – z wyjątkiem sytuacji, gdy zezwalają na to przepisy prawne. Dane „wrażliwe" to np.: dane rasowe lub etniczne, stan zdrowia, kod genetyczny, mandaty, kary…
Administrator danych – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych.
Administrator Bezpieczeństwa Informacji – wyznaczony przez Administratora Danych pracownik odpowiedzialny za bezpieczeństwo danych osobowych.
Hasło – tajny parametr znany wyłącznie użytkownikowi, stosowany w kryptografii oraz uwierzytelnianiu.
Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
Generalny Inspektor Ochrony Danych osobowych (GIODO) – główny organ do spraw ochrony danych osobowych działający na podstawie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Przepisy prawa w zakresie ochrony danych osobowych

Najstarszym aktem prawnym o zasięgu międzynarodowym, kompleksowo regulującym zagadnienia związane z ochroną danych osobowych jest Konwencja Rady Europy Nr 108 z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[1].

[1] http://www.giodo.gov.pl/593/id_art/1596/j/pl z dnia 10.02.2014

Gwarancje ochrony danych osobowych w Polsce zapewnia Konstytucja z 1997 r. Jej art. 47 gwarantuje obywatelom prawo do prywatności, a art. 51 – każdej osobie – prawo do ochrony informacji z nią związanych[2].

W momencie przyłączenia Polski do Unii Europejskiej w 2004 roku wyniknęła konieczność zapewnienia ochrony danym osobowych, jaką na swoim terytorium zapewniają państwa Unii. Wszystkie obowiązujące ustawy europejskie wzorowane były lub dostosowano je do Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady. Zasady ochrony danych ustanowione Dyrektywą 95/46/EC wprowadzone zostały do polskiego porządku prawnego ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[3].

„Ustawa o ochronie danych osobowych (UODO) określiła prawne ramy obrotu danymi osobowymi, a także zasady, jakie należy stosować przy przetwarzaniu danych osobowych, sprecyzowała też prawa i obowiązki organów, instytucji i osób prowadzących zbiory danych osobowych oraz prawa osób, których dane dotyczą, w taki sposób, aby zagwarantować maksymalną ochronę praw i wolności każdej osobie fizycznej oraz poszanowania jej życia prywatnego”[4].

Aktami wykonawczymi do wspomnianej wcześniej ustawy są rozporządzenia MSWiA:

1. 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. Nr 100, poz.1024);
2. z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Danych Osobowych (Dz.U. Nr 94, poz. 923);

[2] Konstytucja RP z 1997 r.:
Art. 47. Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.
Art. 51. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.
1. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
2. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
3. Każdy ma prawo pożądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
4. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

[3] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.).

[4] http://www.giodo.gov.pl/593/id_art/1596/j/pl z dnia 10.02.2014.

3. z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. Nr 229, poz. 1536).

Polityka haseł – zabezpieczenia systemów zawierających dane osobowe

W instytucji podstawą bezpieczeństwa jest odpowiednia polityka haseł. „Wystawienie" systemu teleinformatycznego na atak może prowadzić do ogromnych konsekwencji. Podstawowym zadaniem hasła w systemach teleinformatycznych jest zapewnienie bezpieczeństwa systemów wraz z przechowywanymi w nich informacjami oraz potwierdzanie tożsamości „obiektu" posiadającego uprawnienia do korzystania z danego zbioru informacji.

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010[5], czyli dokument przygotowywany co roku przez Rządowy Zespół Reagowania na Incydenty Komputerowe (CERT.GOV.PL), wykazał, że nieostrożne działania administratorów, skanowanie, nieuprawniona zmiana informacji znajdują się w pierwszej piątce występujących incydentów bezpieczeństwa. Zatem nie ulega wątpliwości, że odpowiednia polityka haseł stanowi jeden z najważniejszych aspektów bezpieczeństwa.

Dla systemów szczególnie zagrożonych atakami oraz przetwarzających ważne dane stosuje się różne metody uwierzytelnienia. Zwiększenie bezpieczeństwa systemu można uzyskać, łącząc hasło z kartą mikroprocesorową. Zastosowanie samego hasła i identyfikatora użytkownika (*one-factor*) jest dość proste do złamania, ale zastosowanie dwóch metod znacząco poprawia poziom ochrony. Zastosowanie rozwiązania *two-factor authentication* lub *three-factor authentication* (łączenie od jednej do trzech opisanych metod) powoduje, że system nie będzie podatny na proste ataki zmierzające do jego kompromitacji.

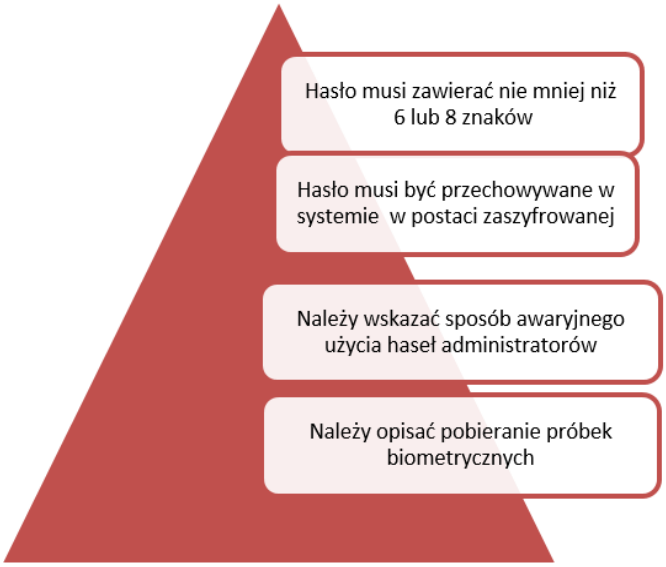
[5] http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi z dnia 10.02.2014.

Metody potwierdzania tożsamości użytkownika przedstawia poniższy schemat.

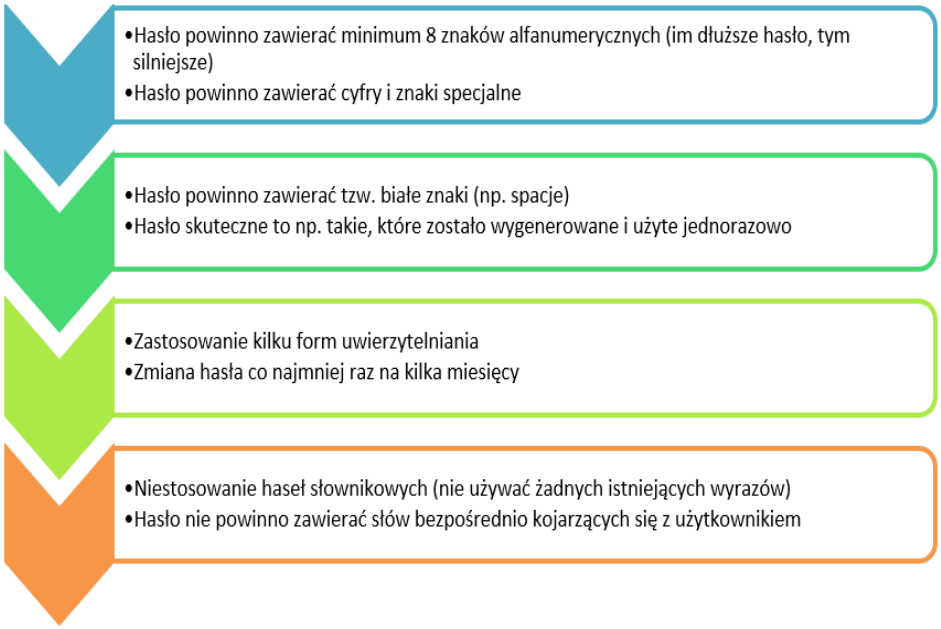
Administrator Danych Osobowych w instytucji ma obowiązek wprowadzenia regulacji dotyczących polityki haseł i ich implementacji w systemach teleinformatycznych. Reguluje to ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[6] oraz rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych[7], jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Użytkownik zobowiązany jest do zmiany hasła z częstotliwością co 30 dni, a samo hasło powinno składać się z 6 lub 8 znaków w zależności od tego, czy w systemie przetwarzane są dane wrażliwe zgodne z art. 27 cytowanej ustawy.

[6] Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.
[7] Dz. U. z 2004 r. Nr 100, poz. 1024.

Przykładowe wymagania dotyczące haseł wg UODO przedstawia poniższy schemat.



Budowanie bezpiecznego hasła:



Niezależnie od obowiązującej polityki, częstotliwość zmiany haseł i liberalności polityki wszystkie zastosowania techniczne powinny być poparte analizą ryzyka. Możliwością pośrednią jest użycie kilku metod uwierzytelniania użytkowników. Zastosowanie liberalnej polityki haseł z elementami biometrii lub elementami technologicznymi (np. karty mikroprocesorowe) może zwiększyć nasz poziom bezpieczeństwa, eliminując zapisywanie haseł czystym tekstem przez użytkowników. Na podstawie analizy ryzyka i możliwych zagrożeń organizacja powinna zastosować odpowiednie rozwiązanie dla każdego użytkownika. Polityka haseł, jak i same hasła powinny podlegać cyklicznym audytom bezpieczeństwa.

Badania

Celem badań było sprawdzenie wiedzy pracowników Wydziału Zarządzania Kryzysowego i Ochrony Ludności w jednym ze śląskich urzędów miasta[8], na temat ochrony danych osobowych, jak również sprawdzenie skuteczności stosowanych zabezpieczeń, m.in. haseł dostępowych, w celu ochrony danych osobowych.

Podjęto również próbę oceny, jaką postawę i jakie zachowania prezentują respondenci w celu skutecznego zabezpieczania przetwarzanych danych osobowych na zajmowanym stanowisku pracy.

W niniejszej pracy posłużono się metodą ankietową. Ankieta pozwala na badanie zjawisk masowych na podstawie odpowiednio opracowanego kwestionariusza. Jest metodą zdobywania informacji poprzez zapytanie wybranych osób za pośrednictwem drukowanej listy pytań, zwanej kwestionariuszem[9]. Ze względu na kategorie pytań wyróżniamy dwa rodzaje kwestionariuszy: kwestionariusz pytań otwartych i kwestionariusz pytań zamkniętych. Kwestionariusz jest jednym z najpopularniejszych narzędzi, używanych do zbierania informacji źródłowych, zawiera starannie dobrany zestaw pytań, na które respondent ankiety udziela informacji.

W przeprowadzonym badaniu wykorzystano pytania zamknięte, które mają określone wszystkie możliwości odpowiedzi. Ankieta zawiera 10 pytań dla badanej grupy respondentów. W części wstępnej kwestionariusza ankiety umieszczono informację o tym, jaki jest cel przeprowadzonego badania i czemu mają służyć uzyskane wyniki. Ponadto w ankiecie zapewnia się o całkowitej anonimowości, co w znaczący sposób zwiększa prawdopodobieństwo udzielania szczerych odpowiedzi.

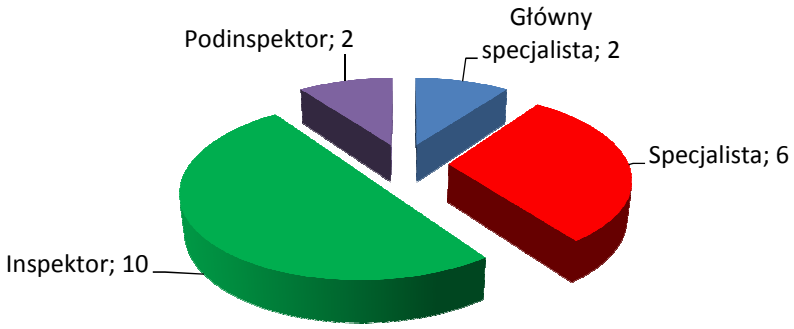
[8] Ze względu na prośbę o anonimowość, nie podajemy pełnej nazwy urzędu.

[9] Gruszczyński L. A., Elementy metod i technik badań socjologicznych, Śląskie Wydawnictwa Naukowe, Tychy 2002.

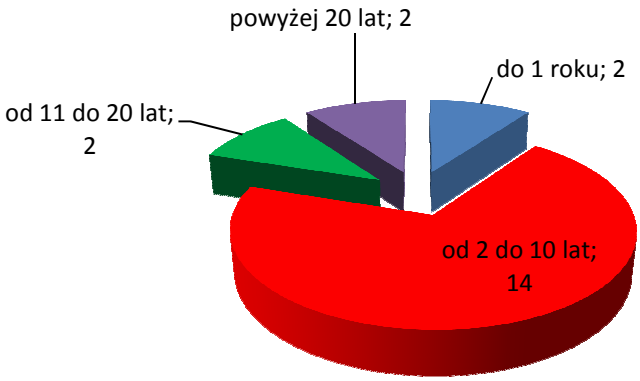
Wyniki badań

Badania przeprowadzono na 20 osobach Wydziału Zarządzania Kryzysowego i Ochrony Ludności Urzędu Miejskiego, o zróżnicowanym stażu pracy. Pozyskane informacje pozwoliły odpowiedzieć na pytania:

- Jaka jest wiedza respondentów w zakresie ochrony danych osobowych?
- Jaka jest skuteczność stosowanych zabezpieczeń w ochronie danych osobowych?



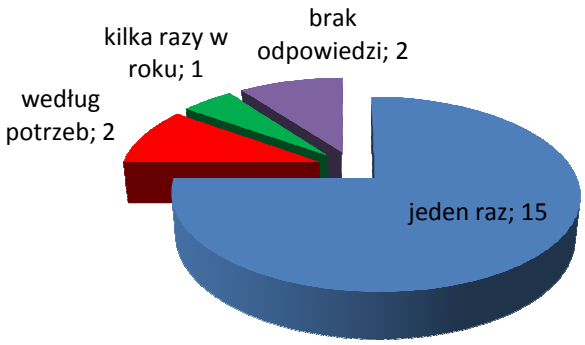
Rys. 1 . Charakterystyka badanej populacji ze względu na zajmowane stanowisko



Rys. 2. Charakterystyka badanej populacji ze względu na staż pracy

Na pytanie: „Czy był Pan/Pani przeszkolony w zakresie ochrony danych osobowych?" wszyscy respondenci odpowiedzieli, że posiadają przeszkolenie w zakresie ochrony danych osobowych.

Na pytanie: „Czy szkolenia odbywają się cyklicznie?" prawie wszyscy respondenci, tj. 17 osób, stwierdzili, że „Nie", jedynie 3 osoby uważają, że „Tak".



Rys. 3. Informacja od respondentów na temat częstotliwości odbywania szkoleń na zajmowanym stanowisku

Z zebranych informacji wynika, że tylko 2 osoby nie pamiętają o wszystkich zabezpieczeniach na swoim stanowisku pracy w zakresie ochrony danych osobowych. 18 osób wskazało natomiast, że pamięta wszystkie stosowane zabezpieczenia na swoim stanowisku pracy w zakresie ochrony danych osobowych.

Na pytanie: „Czy zmienia Pan/Pani hasła regularnie?" wszyscy ankietowani – 20 osób – wskazali odpowiedź, że „Tak". Świadczy to o wysokiej świadomości związanej z ochroną danych osobowych, jak również wskazuje na stosowanie odpowiednich systemów (oprogramowania), które wymuszają dokonywanie czynności zmiany hasła.

Na pytanie: „Czy hasła związane są z życiem prywatnym?" większość respondentów, tj. 16 osób, twierdzi, że „Nie", jedynie 4 osoby uważają, że „Tak".

Na pytanie: „Czy uważa Pan/Pani, że częsta zmiana haseł jest potrzebna?" 14 respondentów wskazało, że „Tak", 6 osób wskazało natomiast odpowiedź „Nie".

Na ostatnie pytanie: „Czy odkąd Pan/Pani pracuje, zdarzyły się przypadki złamania zabezpieczeń w systemie ochrony danych osobowych?" respondenci jednogłośnie wskazali odpowiedź „Nie", co daje rzeczywiste odzwierciedlenie jakości stosowanych zabezpieczeń w ochronie danych osobowych.

Wnioski

Z przeprowadzanych badań wynika, że:

- Respondenci skutecznie realizują prowadzoną politykę bezpieczeństwa urzędu miejskiego w zakresie ochrony danych osobowych.
- Ankietowani wskazują w większości przypadków na brak cykliczności szkoleń w zakresie ochrony danych osobowych. Przeważająca ilość podaje,

że szkolenie w zakresie ochrony danych osobowych zostało przeprowadzone tylko jeden raz i miało to miejsce na początku zatrudnienia w ankietowanym wydziale. Brak cyklicznych szkoleń może prowadzić do pogorszenia wysokiego stopnia świadomości pracowników wydziału w zakresie ochrony danych osobowych przetwarzanych w niniejszym wydziale.

- Staż pracy respondentów nie ma znaczenia dla zapewnienia wysokiego poziomu zabezpieczeń w zakresie ochrony danych osobowych. Świadomość respondentów jest bardzo wysoka.
- Badani jednogłośnie wskazali, że w ankietowanym wydziale urzędu miejskiego nie doszło do złamania stosowanych zabezpieczeń w zakresie ochrony danych osobowych, co jednoznacznie może określić wysoki poziom stosowanych zabezpieczeń w tym zakresie.
- Do głównych czynników wpływających na skuteczną ochronę danych osobowych należy zaliczyć regularną zmianę haseł stosowaną przez respondentów.
- Należy przyjąć, że wiedza pracowników na temat ochrony danych osobowych jest wysoka, gdyż nie odnotowano przypadków złamania stosowanych dotychczasowych zabezpieczeń. Brak szkoleń może jednak prowadzić do pogorszenia tej wiedzy.

Podsumowanie

Każda instytucja publiczna, w tym urzędy miasta, gminy, w ramach wykonywania swoich czynności gromadzą ogromne zasoby danych osobowych. Dlatego szczególnie istotne jest właściwe ich zabezpieczenie. System regulacji prawnych nadaje charakter organom wyspecjalizowanym w zakresie ochrony danych, niemniej należy również pamiętać o odpowiednich szkoleniach, celem przypomnienia i utrwalenia obowiązujących przepisów z zakresu ochrony danych osobowych. Właściwa kontrola i skuteczność zastosowanych środków w przypadku wykrytych nieprawidłowości zapewniają prawidłowy i bezpieczny proces tworzenia i przetwarzania danych, co w konsekwencji gwarantuje bezpieczeństwo jednostki. Dobrym podsumowaniem będzie zdanie wypowiedziane przez Bruce'a Schneiera[10]: „bezpieczeństwo nie jest produktem, lecz procesem, tylko ciągłe udoskonalanie naszej ochrony może zabezpieczyć nasze dane".

[10] Amerykański kryptograf i specjalista z zakresu bezpieczeństwa teleinformatycznego. Autor książek opisujących zagadnienia bezpieczeństwa teleinformatycznego oraz kryptografii.

Literatura

[1] Gruszczyński L. A., Elementy metod i technik badań socjologicznych, Śląskie Wydawnictwa Naukowe, Tychy 2002
[2] Konstytucja RP z 1997 r., Dz.U. 1997 nr 78 poz. 483
[3] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.
[4] Rozporządzenie MSWiA 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. Nr 100, poz.1024).
[5] Rozporządzenie MSWiA z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Danych Osobowych (Dz.U. Nr 94, poz. 923).
[6] Rozporządzenie MSWiA z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. Nr 229, poz. 1536)
[7] http://www.giodo.gov.pl/593/id_art/1596/j/pl z dnia 10.02.2014
[8] http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi z dnia 10.02.2014