Zuzanna Korońska1, Marek Krzywonos2

BANKOWE SYSTEMY INFORMATYCZNE – BEZPIECZEŃSTWO DANYCH

Streszczenie: Celem niniejszego opracowania jest omówienie wybranych zagadnień odnośnie bankowych systemów informatycznych oraz bezpieczeństwa danych w nich zawartych. Przedstawione są wymagania odnośnie systemów informatycznych, poziomy bezpieczeństwa dla poszczególnych danych, zadania administratora danych. Omówiono stosowaną w bankach politykę bezpieczeństwa oraz metody oceny ryzyka i sposoby przeprowadzania audytu bezpieczeństwa w bankowych systemach informatycznych.
Słowa kluczowe: bank, bankowe systemy informatyczne, bezpieczeństwo danych.

Wstęp

Banki należą do instytucji zaufania publicznego dlatego powinny niezwykle skrupulatnie dbać o powierzone im dane. Klienci przekazując swoje oszczędności oraz wrażliwe informacje oczekują zapewnienia im całkowitego bezpieczeństwa. Stosowanie skutecznych metod ochrony danych jest wiec kluczowym elementem pozwalającym stabilnie funkcjonować każdej instytucji finansowej. Dotyczy to przede wszystkim zapewnienia bezpieczeństwa powierzonych środków tak ważnego ze względu na wizerunek marketingowy instytucji, ale również realne straty które może ponieść bank. Korporacje w oparciu o akty prawne przez lata budowały procedury zapewniające bezpieczeństwo. Elementem wspólnym

[1] mgr Zuzanna Korońska, doktorantka, Instytut Nauk Ekonomicznych PAN w Warszawie.

[2] mgr Marek Krzywonos, Zakład Zarządzania, Instytut Politechniczny, Państwowa Wyższa Szkoła Zawodowa im. Stanisława Pigonia w Krośnie.

tych wszystkich dokumentów jest zabezpieczenie właściwych, z punktu widzenia ustawodawcy lub uprawnionego podmiotu, danych i informacji przed ich nieuprawnionym ujawnieniem. Ich celem jest wskazanie oczekiwań nadzorczych co do zarządzania środowiskiem informatycznym oraz bezpieczeństwem danych pozostawiając jednak duży margines pozwalający uwzględnić różnorakie skale działalności, profile ryzyka czy technologię która zostanie zastosowana.

Systemy informatyczne stosowane w bankach

Instytucje finansowe, a w szczególności banki szczególną wagę przywiązują do bezpieczeństwa informacji. Banki posiadają najbardziej precyzyjne i sztywne reguły funkcjonowania systemów informatycznych. Dzięki tym systemom bank ma możliwość sprawnej obsługi osób fizycznych, przedsiębiorstw oraz instytucji. Ma to wpływ na efektywność obrotu gospodarczego oraz bezpieczeństwo finansowe klientów.

Modele bankowych systemów informatycznych zależą od wielu czynników:

- zasięgu terytorialnego, obszaru na jakim bank prowadzi działalność (bank lokalny, regionalny, krajowy, międzynarodowy);
- liczby oraz wielkości poszczególnych oddziałów;
- segmentu rynku (banki uniwersalne i wyspecjalizowane);
- skali działania (liczby prowadzonych rachunków bankowych, liczby klientów, średniej liczby realizowanych transakcji);
- zakresu świadczonych usług.

Należy przykładać szczególną wagę do poziomu bezpieczeństwa gromadzonych i przetwarzanych informacji. W banku musi być przygotowany system kwalifikacyjny, który umożliwi posortowanie informacji i przyporządkowanie do nich odpowiedniego poziomu zabezpieczeń. Kwalifikacja ta musi byś adekwatna do zewnętrznych i wewnętrznych uwarunkowań funkcjonowania banku.

W rekomendacji D przedstawiono otwarty katalog informacji, jakie powinny być klasyfikowane na odpowiednich poziomach bezpieczeństwa. Są to m.in.:

- znaczenie tych informacji dla banku i realizowanych w nim procesów;
- znaczenie tych informacji z perspektywy zarządzania rodzajami ryzyka, które zostały zidentyfikowane jako istotne w prowadzonej przez bank działalności;
- skutki utraty lub nieuprawnionej zmiany danej informacji;

– skutki nieuprawnionego ujawnienia danej informacji;
– szczególne wymagania regulacyjnych i prawnych dotyczących danego rodzaju informacji[3].

Ważne, aby zaszeregowanie do danego poziomu bezpieczeństwa było określane na każdym etapie gromadzenia, przechowywania i przetwarzania danych, aż do ich archiwizacji a potem usunięcia.

Oprócz bezpieczeństwa systemu informatycznego ważnym czynnikiem są też ludzie. Osoby, które posiadają dostęp do danych poufnych, należy szczegółowo sprawdzać. Dodatkowo każda osoba posiadająca dostęp powinna podpisać oświadczenia o zobligowaniu do zachowania poufności. Oświadczenie powinno zawierać klauzulę o zachowaniu poufności, również po ustaniu dostępu albo co najmniej przez jakiś czas po zdarzeniu. Przechowywane informacje muszą być zabezpieczone (np. poprzez szyfrowanie, mechanizmy kontroli dostępu, mechanizmy zapewniające możliwość odzyskiwania danych)[4].

Komisja Nadzoru Finansowego wskazuje konieczność stosowania rozwiązań, które w sposób automatyczny będą wykonywały działania kontrolne, np. poprzez „rozwiązania ograniczające użytkownikom systemów informatycznych możliwość zapisu informacji na przenośnych nośnikach danych, umożliwiające sprawowanie kontroli nad informacjami przesyłanymi za pośrednictwem poczty elektronicznej oraz ograniczające dostęp do innych, niż przyjęte w banku, systemów poczty”[5].

Administrator danych

Z punktu widzenia bezpieczeństwa systemu informatycznego jednym z najbardziej ważnych stanowisk jest administrator danych. Wzrost zagrożenia bezpie-

---

[3] Komisja Nadzoru Finansowego *Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach*, https://www.knf.gov.pl/Images/Rekomendacja_D_8_01_13_uchwala_7_tcm75-33016.pdf [dostęp: 06.06.2016].

[4] J. Madej *Klasyfikacja zagrożeń bezpieczeństwa systemu informatycznego* Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie nr 814, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie 2010, s. 77.

[5] Komisja Nadzoru Finansowego *Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach*, https://www.knf.gov.pl/Images/Rekomendacja_D_8_01_13_uchwala_7_tcm75-33016.pdf [dostęp: 06.06.2016].

czeństwa informacji nakłada na osobę zatrudnioną na tym stanowisku liczne obowiązki:

- przeprowadzenie analiz ryzyka w obszarze utraty poufności przetwarzanych danych, ich utraty lub zniszczenia bądź też nieuprawnionej modyfikacji;
- ustanawianie adekwatnej do celów i zakresu danych polityki bezpieczeństwa oraz procedur zarządzania tym bezpieczeństwem;
- wdrożenie i stosowanie środków przewidzianych w powołanej przez siebie polityce bezpieczeństwa;
- systematyczne szkolenia pracowników w zakresie zgodnego z prawem przetwarzania danych osobowych, w tym odpowiedzialności za jego naruszenie;
- zapewnienie odpowiednich relacji między administratorem danych i podmiotem, któremu powierzono przetwarzanie danych lub administratorem danych i użytkownikiem będącym jednocześnie podmiotem, którego dane są przetwarzane.

W przypadku ostatniego punktu podmiotem przetwarzającym dane może być wyspecjalizowana firma, której jest zlecane wykonywanie konkretnie określonych czynności przetwarzania danych w ramach tzw. umowy powierzenia przetwarzania, o której mowa w art. 31 ustawy o ochronie danych osobowych[6], jak również osoba fizyczna, której dane dotyczą.

Polityka bezpieczeństwa

Podstawą funkcjonowania dużych instytucji finansowych jest skuteczny i bardzo formalny system do zarządzania bezpieczeństwem środowiska teleinformatycznego. Podstawą jego skuteczności jest fakt, że będzie obejmował całe spektrum działań i procesów związanych z identyfikacją, kontrolą, przeciwdziałaniem, monitorowaniem, ale i raportowaniem ryzyka w tym zakresie. Bardzo istotne jest, aby system podlegał kompleksowej integracji z istniejącym już systemem zarządzania ryzykiem i bezpieczeństwem w banku. Jego działanie wynika wtedy ze strategii instytucji co, w oparciu o sformalizowane procedury i normy we-

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

wnętrzne, wzmacnia jego środowisko a tym samym skuteczność. Podstawowym dokumentem w tym zakresie powinna być polityka bezpieczeństwa informacji, która winna zawierać wszelkie wymagania dotyczące funkcjonowania systemu oraz zasady jego użytkowania. Należy w niej zawrzeć stale i systematyczne przeglądy, ponieważ uwzględnienie wszelakich zmian otoczenia teleinformatycznego oraz zmian, które zachodzą w samym banku pozwoli na uszczelnienie systemu i zapewnienie mu możliwie najskuteczniejszej ochrony, wykorzystując m.in. takie narzędzia jak: wymagania oparte o czynniki otoczenia gospodarczego i kontroli wewnętrznej, samoocena ryzyka operacyjnego, analizy scenariusza ataków czy mapy ryzyka. Celem identyfikacji ryzyka w zakresie bezpieczeństwa systemu informatycznego jest „określenie związanych z nim zagrożeń mogących spowodować stratę (w tym finansową) w danej instytucji oraz określenie gdzie, w jaki sposób i dlaczego te zagrożenia mogą się zmaterializować”[7]. Najistotniejsza sprawa aby zidentyfikować ryzyka jest określenie istniejących podatności środowiska, zagrożeń oraz podmiotów, które mogłyby (potencjalnie) próbować je wykorzystać do swej działalności. Bank poprzez rekomendacje D jest zobowiązany do prowadzenia rejestru zdarzeń operacyjnych, który uwzględnia wszystkie zdarzenia zgodne z przyjętą w banku definicją zdarzenia operacyjnego. KNF rekomenduje także nawiązanie stałej współpracy międzybankowej w zakresie wymiany informacji o zidentyfikowanych już przez poszczególne instytucje zagrożeniach. Jest to o tyle skomplikowane, że sposób oraz zakres wymienianych informacji powinny zapewniać ich poufność, a przede wszystkim zachowanie tajemnicy bankowej. Inną opcją jest minimalizacja ryzyka poprzez zmianę istniejących mechanizmów kontroli lub po prostu transfer istniejącego ryzyka powiązanego z danym zagrożeniem na podmiot zewnętrzny. W przypadku kiedy żadne z powyższych rozwiązań nie może zostać wdrożone, instytucja musi zaakceptować powstałe ryzyko. Wtedy jednak musi liczyć się z zapewnieniem środków na pokrycie ewentualnych strat.

Rekomendacja D jasno określa zasady postępowania w sytuacjach naruszenia bezpieczeństwa. Katalog jest otwarty i uwzględnia m.in.:

---

[7] Komisja Nadzoru Finansowego *Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach*, https://www.knf.gov.pl/Images/Rekomendacja_D_8_01_13_uchwala_7_tcm75-33016.pdf [dostęp: 06.06.2016].

- sposób przeprowadzania analiz wpływu incydentów na środowisko teleinformatyczne, w tym jego bezpieczeństwo;
- zasady kategoryzacji i priorytetyzacji incydentów, informacji i systemów informatycznych związanych z danym incydentem, metody i zakres zbierania informacji o incydentach;
- zakresy odpowiedzialności w obszarze zarządzania incydentami;
- zasady wykrywania zależności pomiędzy incydentami;
- zasady komunikacji, obejmujące zarówno pracowników banku, jak i zewnętrznych dostawców usług oraz – w przypadku istotnego narażenia na skutki danego incydentu – również innych stron trzecich (klientów, kontrahentów itp.), zapewniające odpowiednio szybkie powiadamianie zainteresowanych stron i podejmowanie działań, adekwatnie do poziomu istotności incydentu;
- zasady gromadzenia i zabezpieczania dowodów związanych z incydentami, które będą mogły zostać wykorzystane w ewentualnych postępowaniach sądowych;
- zasady dotyczące podejmowania działań naprawczych i zapobiegawczych, obejmujące w szczególności przypisanie osób odpowiedzialnych za realizację tych działań oraz monitorowanie stanu ich realizacji[8].

Każdorazowo bank powinien przeanalizować proces zarządzania oraz przepływu informacji i na tej podstawie podjąć decyzję w zakresie wykorzystania rozwiązań ułatwiających zarządzanie incydentami naruszenia bezpieczeństwa, m.in. poprzez centralizację analizowania, zbierania czy przechowywania dzienników zdarzeń generowanych przez systemy informatyczne.

Ocena ryzyka

Analiza potencjalnego ryzyka powinna być wykonana każdorazowo tam gdzie ma zostać wdrożony system bezpieczeństwa informacji. Dokonanie takiej weryfikacji ma na celu ograniczenie ryzyka do minimum lub też do poziomu, w którym organizacja będzie w stanie ponieść ciężar konsekwencji wynikających ze złamania schematu bezpieczeństwa. Najważniejszym zadaniem jest więc zidentyfikowanie naturalnych zagrożeń i oszacowanie skutków w razie potencjalnego wystąpienia.

[8] Ibidem.

Typowy proces analizy szczegółowej powstałego ryzyka składa się z kilku podstawowych etapów[9]:

1. Identyfikacja zasobów i ich ocena;
2. Identyfikacja potencjalnych zagrożeń;
3. Identyfikacja istniejących zabezpieczeń;
4. Identyfikacja podatności na wykryte wcześniej zagrożenia;
5. Szacowanie ryzyka i opracowanie rekomendacji.

Oszacowane już ryzyka można zminimalizować, natomiast bank nigdy nie wyeliminuje go całkowicie. Ważne aby w takowej analizie odpowiedzieć na pytanie co może się wydarzyć, jakie byłyby skutki dla organizacji i klientów oraz w jaki sposób można zminimalizować potencjalne straty. Na pewnym poziomie bezpieczeństwa systemu dodawanie nowych zabezpieczeń jest zdecydowanie bardziej kosztowne niż stopień bezpieczeństwa, który można osiągnąć poprzez dodanie komponentu. Pozostałe ryzyko szczątkowe jest w bankowości często nazwane ryzykiem akceptowalnym. System w dużych instytucjach, ze względu na swój globalny charakter oraz poziom skomplikowania, jest bardzo często narażony na rożnej maści niebezpieczeństwa.

Bardzo ogólnie można wyróżnić kilka podstawowych kategorii zagrożeń systemów informatycznych w banku:

- ataki sieciowe (atak DoS, włamania, penetracje);
- zagrożenia transmisji danych (przechwytywanie danych sesji czy połączeń sieciowych);
- zagrożenia aplikacyjne (robaki, wirusy czy konie trojańskie);
- awarie techniczne (sprzętu, oprogramowania);
- zagrożenia kryptograficzne (związane z kluczami do szyfrowania);
- niebezpieczeństwo komunikacyjne (np. przeciążenia sieci);
- zagrożenia fizyczne (np. pożary, kradzieże);
- błędy ludzi (użytkowników wewnętrznych, zewnętrznych czy administratorów)[10].

---

[9] A. Kaczmarek, *ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych* http://www.giodo.gov.pl/487/id_art/3912/j/pl/ [dostęp: 06.06.2016].

[10] J. Syta *Sektor bankowy jako potencjalny cel ataku cyberterrorystycznego* w: *Cyberterroryzm – nowe wyzwania XXI wieku* red. T. Jemioła, J. Kisielnicki i K. Rajchel K. Wydział Wydawnictw i Poligrafii Wyższej Szkoły Policji w Szczytnie, Warszawa 2009, s. 696.

Zapewnienie wysokiego poziomu bezpieczeństwa zasobów strategicznych wymaga regularnego monitorowania oraz systematycznego badania stanu zabezpieczeń. Pomimo jednak posiadania najbardziej zaawansowanego systemu, w trakcie jego wprowadzenia do użytkowania, niezbędna jest stała jego weryfikacja. Jej brak może spowodować, że bardzo szybko starci swoje właściwości oraz stanie się źródłem niestabilności i zagrożeń.

Istnieje konieczność wykonywania testów oprogramowania, dzięki nim możliwa jest wiarygodna ocena poziomu zabezpieczeń. Testy należy przeprowadzać za pomocą dedykowanego do tego oprogramowania. Nie ma możliwości wykonania testów w zakresie całego systemu, pomimo tego że panuje powszechnie taka opinia. Systemy bankowe, które są zaliczane do dużych systemów informatycznych, mogą być testowane ze względów technicznych, finansowych i organizacyjnych tylko w wybranych elementach składowych. Należy skupić się na ocenie odporności zabezpieczeń odporności najbardziej wrażliwych zasobów.

Audyt to przede wszystkim analiza, ale głównie badania praktyczne, w celu ochrony poziomu bezpieczeństwa w konkretnej części systemu. Analiza odbywa się pod kątem szczelności i odporności na nieautoryzowane zewnętrzne oraz wewnętrzne ingerencje. Metodą, która wykorzystywana jest najczęściej jest symulacja włamania. Istnieje bardzo duża liczba potencjalnych metod włamań, przez to taką próbę należy poprzedzić identyfikacją oraz wstępną penetracją systemu. Symulacja powinna obejmować wszystkie dostępne urządzenia sieciowe. Dzięki takiej symulacji określa się możliwość nieupoważnionego dostępu do danych lub usług.

Wykonywana jest także analiza systemowa za pomocą modeli matematycznych, dzięki którym opisywane są własności jakościowe i ilościowe rzeczywistych systemów. W wyniku analizy formalnej możliwe jest zastosowanie praktyczne, ponieważ umożliwia bezproblemową implementację w systemach informatycznych oraz znacznie obniża możliwość popełnienia błędu.

Dzięki audytom bezpieczeństwa opracowywany jest raport, który pomaga zobrazować rzeczywisty stan zabezpieczenia zasobów. W raporcie przedstawia się słabe punkty zabezpieczeń a także prezentuje się procedury ich eliminacji lub redukcji. Dzięki audytowi uaktualniane są procedury oraz polityka bezpieczeństwa. Pozyskanie informacji o narzędziach testów oraz sposobie ich wykorzystania jest pomocne, aby w przyszłości zweryfikować ich skuteczność.

Zagrożenia bankowych systemów informatycznych

Segment bankowości elektronicznej naznaczony jest z bardzo dynamicznym rozwojem. Opieranie się na elektronicznym przetwarzaniu danych powoduje przyrost wielorakich form aktywności przestępczej skierowanej bezpośrednio przeciwko bezpieczeństwu środków klientów zgromadzonych na rachunkach bankowych. Wraz z rosnącym i nieuniknionym rozpowszechnianiem się usług elektronicznych, rodzaj i skala zagrożeń będą systematycznie rosły. Ze względu na atrakcyjność swobodnej dostępności do zgromadzonych na swoich rachunkach środków, poprzez niezależne kanały typu telefon, komputer, również dostępność dla przestępców staje się praktycznie nieograniczona. Przestępcy nie posiadają ograniczeń co do miejscu i czasu, a zagrożenia płynące z nieodpowiedniej polityki bezpieczeństwa potrafią wywołać dotkliwe straty, zarówno dla klientów, jak i wizerunku banku. Bardzo często pojedynczy użytkownicy nie posiadają pełnej świadomości istniejących zagrożeń. Większość z nas słyszała o możliwych konsekwencjach ale bardzo często lekceważy je myśląc, że nas ten problem nie dotknie a cyberprzestępcy są zorientowani na wielkie firmy i duże pieniądze. Tym bardziej jest to widoczne, gdy użytkowanie nowego produktu albo też usługi przez klienta obnaża słabość systemu dopiero w momencie ataku czy zagrożenia bezpośredniego ze strony przestępców. Wtedy gdy potencjalne wcześniej ryzyko staje się zagrożeniem w realnym świecie i dotyczy konkretnych danych konkretnych osób. Dlatego tak istotne jest wstępne definiowanie zagrożeń i ryzyka jeszcze na etapie, zanim staną się realnym zagrożeniem dla klientów.

Wnioski

Funkcjonowanie banku jako dużej korporacji finansowej, nie jest na dzień dzisiejszy możliwe bez wsparcia wszelkich nowoczesnych technologii informatycznych. To właśnie owe technologie są podstawowym warunkiem bezpiecznego funkcjonowania banku. Specyfika branży wymaga stosowania stale unowocześnianych, ale jednocześnie bezpiecznych i sprawdzonych narzędzi. Z jednej strony dynamika rozwoju technologii rozwija przed bankami nowe możliwości, z drugiej zaś rosnące potrzeby związane z bezpieczeństwem informacji powodują rozwój tych technologii. Ta niezwykle ścisła integracja ma charakter bardzo dynamiczny. I to właśnie na menedżerach, jak i kadrze szeregowej, w jednostkach banku spoczywają konkretne obowiązki wynikające z przepisów, zarówno poziomu ustawowego, jak i regulacji wewnętrznych. Wszystkie te działania i procedury mają na celu dostosowanie przepisów do warunków występujących w tej konkretnej

jednostce, których znajomość i skrupulatne przestrzeganie jest jedyną drogą do właściwego i bezpiecznego funkcjonowania instytucji, zwłaszcza takiej jak bank.

Absolutnie niezbędne jest precyzyjne określenie i sumienne przestrzeganie instrukcji dotyczących organizacji ochrony tajemnicy, zwłaszcza wybieranie osób odpowiedzialnych za przedmiotowe zagadnienia, dopuszczania pracowników do informacji chronionych po przeszkoleniu i podpisaniu stosownych dokumentów (umowa, oświadczenie o zachowaniu tajemnicy), ograniczaniu osób mających dostęp do poszczególnych informacji do niezbędnego minimum, odpowiedniej organizacji obiegu dokumentów, sporządzania, klasyfikacji, rejestrowania i ekspedycji korespondencji, wykonywania kopii, odpisów i wyciągów dokumentów oraz ich dystrybucji, archiwizacji i niszczenia. Niezwykle istotną czynnością jest również określenie zasad postępowania w przypadku utraty dokumentów lub ujawnienia informacji chronionych, ale przede wszystkim dokonywanie regularnych szkoleń, którym podlegają pracownicy i kontrola wewnętrzna. Podstawą sprawnego i bezpiecznego działania sektora usług finansowych jest jednak zaufanie jego klientów, a w szczególności ich wiara, że środkami, które powierzyli bankowi nie będzie mógł dysponować nikt nieuprawniony. Poczucie bezpieczeństwa wiąże się z koniecznością spełnienia przez banki wymogu zdefiniowania oraz wyeliminowania zagrożeń powstałych wraz z rozwojem i postępem teleinformatycznym. Zastosowanie konkretnych procedur wprowadza w systemie kontrolę dostępu do zasobów, danych i informacji na różnych poziomach organizacyjnych, ale przede wszystkim eliminuje zagrożenia nieupoważnionego dostępu do zawartości systemu.

Bank to są głównie ludzie i technologie informatyczne. Sieci i systemy są bazą dla całego systemu w instytucji, która jest w stanie realizować swoje najważniejsze cele tylko wtedy, gdy droga rozwoju tychże systemów jest spójna z ogólną strategią rozwoju banku. Kompletne i efektywne zarządzanie tym obszarem umożliwia niezawodne funkcjonowanie systemów, ale przede wszystkim wzmacnia bezpieczeństwo banku i jego klientów. Zarządzanie zabezpieczeniami danych gromadzonych i przechowywanych w systemie, kontrola tego procederu to długotrwały i dynamiczny proces. Zbyt szybkie albo nazbyt restrykcyjne wdrażanie systemu zmniejsza jego wartość i rodzi nowe zagrożenia. Przy wprowadzaniu należy wyeliminować przesadę, a w szczególności – przekonanie o możliwości osiągnięcia totalnego bezpieczeństwa. Technologia zastosowana dla przechowalni danych jest bowiem taką dziedziną, która nie zagwarantuje nigdy stuprocentowej ochrony.

Dla banku najważniejsze powinno stać się budowanie przede wszystkim świa-

domości pracowników oraz użytkowników systemu. To najczęściej niewłaściwe, czy po prostu nieświadome ich działanie, jest przyczyną zagrożenia. Ważne, aby nie było to jednorazowy zryw tylko wieloetapowy, długofalowy proces, który będzie w stanie zapewnić kompleksowe zarządzanie danymi i ich bezpieczeństwem w instytucji zaufania publicznego jaką jest bank.

Literatura

1. Kaczmarek A., *ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych* http://www.giodo.gov.pl/487/id_art/3912/j/pl/ [dostęp: 06.06.2016].
2. Komisja Nadzoru Finansowego *Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach*, https://www.knf.gov.pl/Images/Rekomendacja_D_8_01_13_uchwala_7_tcm75-33016.pdf [dostęp: 06.06.2016].
3. Madej J., *Klasyfikacja zagrożeń bezpieczeństwa systemu informatycznego* Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie nr 814, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie 2010, s. 77.
4. Syta J., *Sektor bankowy jako potencjalny cel ataku cyberterrorystycznego* w: *Cyberterroryzm – nowe wyzwania XXI wieku* red. T. Jemioła, J. Kisielnicki i K. Rajchel K. Wydział Wydawnictw i Poligrafii Wyższej Szkoły Policji w Szczytnie, Warszawa 2009, s. 696.
5. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 j.t. z późn. zm.).

BANK INFORMATION SYSTEMS – SECURITY OF THE DATA

Summary: The paper examines selected issues of bank information systems and the security of data contained therein. The work describes the requirements for security levels of information systems with a particular data and the tasks of data controllers. It also discusses security policies used in banks, risk assessment methods and ways of carrying out the security audits in the bank information systems.

Keywords: bank, bank information systems, data security

Translated by Marek Krzywonos