Tadeusz DĄBROWSKI, Lesław BĘDKOWSKI
Wojskowa Akademia Techniczna, Wydział Elektroniki, Warszawa
Marcin BEDNAREK
Politechnika Rzeszowska, Wydział Elektrotechniki i Informatyki, Rzeszów

ANALIZA BEZPIECZEŃSTWA OPERACJI KARTAMI BANKOWYMI W ASPEKCIE TECHNICZNYM

Słowa kluczowe

Niezawodność bezpiecznościowa, bezpieczeństwo transakcji kartami, potencjał bezpieczeństwa.

Streszczenie

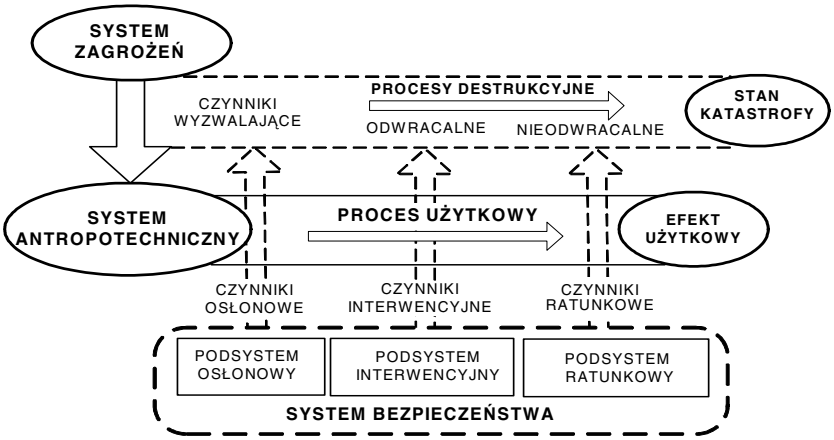
Artykuł poświęcony jest zagadnieniu bezpieczeństwa specyficznego systemu antropotechnicznego, jakim jest system operacji kartami bankowymi. Zawiera definicję systemu bezpiecznościowego i potencjałowego kryterium stanu bezpieczeństwa tego systemu. Omawia wybrane operacje kartami bankowymi, klasyfikuje towarzyszące tym operacjom zagrożenia i stosowane działania ochronne. Charakteryzuje, w aspekcie jakościowym i technicznym, bezpieczeństwo systemu kart bankowych.

Wprowadzenie – dyskusja pojęcia niezawodności bezpiecznościowej

Niezawodność bezpiecznościowa [1] wyraża zaufanie administratora (operatora) systemu eksploatacji do tego, że obiekt (element, urządzenie, system) wykona określone zadanie eksploatacyjne (użytkowe lub obsługowe) bez zagrożenia dla ludzi, samego obiektu i otoczenia. Zaufanie to opiera się – na ogół – na doświadczeniu uzyskanym z obserwacji funkcjonowania obiektów tego samego typu, w takich samych lub zbliżonych warunkach eksploatacyjnych.

Bezpieczność jest pojęciem należącym do zbioru pojęć teorii bezpieczeństwa. Oznacza cechę (właściwość) obiektu (systemu) warunkującą stan bezpiecznego istnienia i funkcjonowania obiektu. Bezpieczne istnienie i funkcjonowanie oznacza, że obiekt nie zagraża życiu i zdrowiu operatora oraz innych ludzi znajdujących się w zasięgu oddziaływania obiektu, nie zagraża sam sobie, a także nie zagraża istnieniu i nie zakłóca prawidłowego funkcjonowania innych obiektów oraz środowiska, które go otacza.

Bezpieczność jest właściwością względną – jej poziom zależy nie tylko od właściwości wewnętrznych obiektu, ale także od jakości oddziaływań otoczenia, a w tym np. od oddziaływań sterujących operatora.



Rys. 1. Struktura systemu bezpiecznościowego na tle podstawowych procesów związanych z użytkowaniem obiektu technicznego

Analiza struktur rzeczywistych systemów eksploatacji wskazuje, że niemal w każdym przypadku daje się wyróżnić pewien – wewnętrzny i/lub zewnętrzny w stosunku do ***systemu antropotechnicznego*** *(SAT) – zestaw środków (urządzeń, reguł, czynników) pozostających względem siebie w określonych relacjach i spełniających funkcje warunkujące stan systemu w aspekcie bezpiecznościowym. Ten zestaw środków i realizowanych przy ich udziale funkcji i procesów podzielić można na dwie przeciwstawne – ze względu na skutki oddziaływań – struktury:* ***system zagrożeń i system bezpieczeństwa****. Systemy te, w połączeniu z systemem antropotechnicznym, tworzą strukturę, którą możemy nazywać* ***systemem bezpiecznościowym*** *(rys. 1).*

Zauważmy, że procesowi użytkowania, w wyniku którego powstaje efekt użytkowy, towarzyszą nieodłącznie procesy destrukcyjne wywoływane przez różne czynniki wyzwalające, generowane przez system zagrożeń. Przykładem takich czynników mogą być niekorzystne warunki klimatyczne lub błędne sterowanie obiektu przez operatora. Brak przeciwdziałania tym czynnikom oraz wy-

wołanym przez nie procesom prowadzi nieuchronnie do stanu niezdatności, który może mieć wymiar awarii lub katastrofy.

Mając to na uwadze, wyposaża się obiekty i systemy eksploatacji w systemy bezpieczeństwa. Zadaniem systemu bezpieczeństwa jest – w najkrótszym ujęciu – zapobieganie pojawianiu się czynników wyzwalających oraz generowanie czynników osłonowych, interwencyjnych i ratunkowych w celu blokowania, przerywania lub przynajmniej spowalniania pojawiających się procesów destrukcyjnych, tak aby system antropotechniczny pozostawał w stanie bezpieczeństwa – a jeśli to niemożliwe, to przynajmniej, by skutki stanu niezdatności nie były zbyt dotkliwe.

Dążenie do stanu bezpieczeństwa, utrzymanie obiektu w tym stanie oraz powracanie do tego stanu ze stanu zagrożenia, a także ograniczanie negatywnych skutków stanu niebezpieczeństwa, wymaga nakładów w postaci metod i urządzeń tworzących system bezpieczeństwa. System taki może posiadać następujące moduły zadaniowe: podsystem osłonowy (PO), podsystem interwencyjny (PI), podsystem ratunkowy (PR).

Podsystem osłonowy (PO) jest to zespół działań i środków wytwarzających czynniki osłonowe, których zadaniem jest zapobieganie uaktywnianiu się czynników wyzwalających w obiekcie (w systemie antropotechnicznym) procesy destrukcyjne, zwłaszcza te, które mogą prowadzić do katastrofy.

Podsystem interwencyjny (PI) jest to zespół działań i środków aktywizujących czynniki interwencyjne, przerywające lub hamujące procesy destrukcyjne, zwłaszcza te, które mogą prowadzić do katastrofy.

Podsystem ratunkowy (PR) jest to zespół działań i środków aktywizujących czynniki przeciwawaryjne i ratunkowe ograniczające skutki katastrofy.

Przyjmijmy, że zasób energii, informacji i substancji systemu bezpieczeństwa, który **może być** użyty w celu zlikwidowania – lub przynajmniej zmniejszenia – negatywnych skutków oddziaływania systemu zagrożeń na system antropotechniczny, nazywać będziemy **potencjałem bezpieczeństwa** F_{PB} systemu bezpiecznościowego.

Podobnie przyjmijmy, że zasób energii, informacji i substancji systemu zagrożeń, który stanowi zagrożenie dla systemu antropotechnicznego, nazywać będziemy **potencjałem niebezpieczeństwa** F_{PN} systemu bezpiecznościowego.

Warunkiem koniecznym zachowania stanu bezpieczeństwa (w tym także powrotu do tego stanu ze stanu zagrożenia) jest istnienie potencjału bezpieczeństwa niemniejszego od potencjału niebezpieczeństwa, czyli:

$$F_{PB} \geq F_{PN} \tag{1}$$

Minimalny, wystarczający potencjał bezpieczeństwa nazywać można **wymaganym potencjałem** $F_{Pb\text{-}wym}$ systemu bezpiecznościowego, zaś istniejący

potencjał bezpieczeństwa nazywać można **potencjałem dysponowanym** $F_{Pb\text{-}dys}$ systemu bezpiecznościowego. W konsekwencji **warunek konieczny zdatności bezpiecznościowej** systemu antropotechnicznego zapisać można następująco:

$$F_{Pb-dys} \geq F_{Pb-wym} \tag{2}$$

Zauważmy, że na potencjał dysponowany składają się potencjały podsystemów zadaniowych systemu bezpieczeństwa, tj. podsystemów: osłonowego, interwencyjnego i ratunkowego.

Można zatem – w tym aspekcie – mówić o trzech poziomach bezpieczeństwa SAT:

- pierwszy poziom bezpieczeństwa (bezpieczeństwo bezwzględne); miarą tego bezpieczeństwa jest akceptowalna wartość prawdopodobieństwa skutecznej deaktywacji, przez podsystem osłonowy, czynników wyzwalających proces destrukcyjny;
- drugi poziom bezpieczeństwa (bezpieczeństwo względne); miarą tego bezpieczeństwa jest akceptowalna wartość prawdopodobieństwa skutecznego działania podsystemu interwencyjnego (tj. działania polegającego na przerwaniu procesu destrukcyjnego);
- trzeci poziom bezpieczeństwa (bezpieczeństwo ograniczone); miarą tego bezpieczeństwa jest akceptowalna wartość prawdopodobieństwa skutecznego działania podsystemu ratunkowego (tj. działania polegającego na ograniczeniu skutków awarii lub katastrofy do akceptowalnego rozmiaru).

Niezawodność bezpieczeństwa systemu antropotechnicznego można – jak łatwo zauważyć – oceniać ogólnie jako wypadkowy rezultat działania wszystkich podsystemów bezpieczeństwa lub szczegółowo – z rozbiciem na poszczególne poziomy bezpieczeństwa i poszczególne podsystemy bezpieczeństwa.

Rozpatrzmy zagadnienie niezawodności bezpieczeństwa na przykładzie operacji wykonywanych kartami bankowymi za pośrednictwem stosowanych aktualnie metod i środków technicznych.

1. Charakterystyka operacji kartami bankowymi

Przeanalizujmy niepożądane oddziaływania, którym poddawani są użytkownicy kart bankowych podczas realizacji operacji bezgotówkowych. Liczni autorzy podają wiele kryteriów klasyfikacji kart bankowych [2, 4]. Są tu wymieniane m.in. kryteria podziału uwzględniające rodzaj:

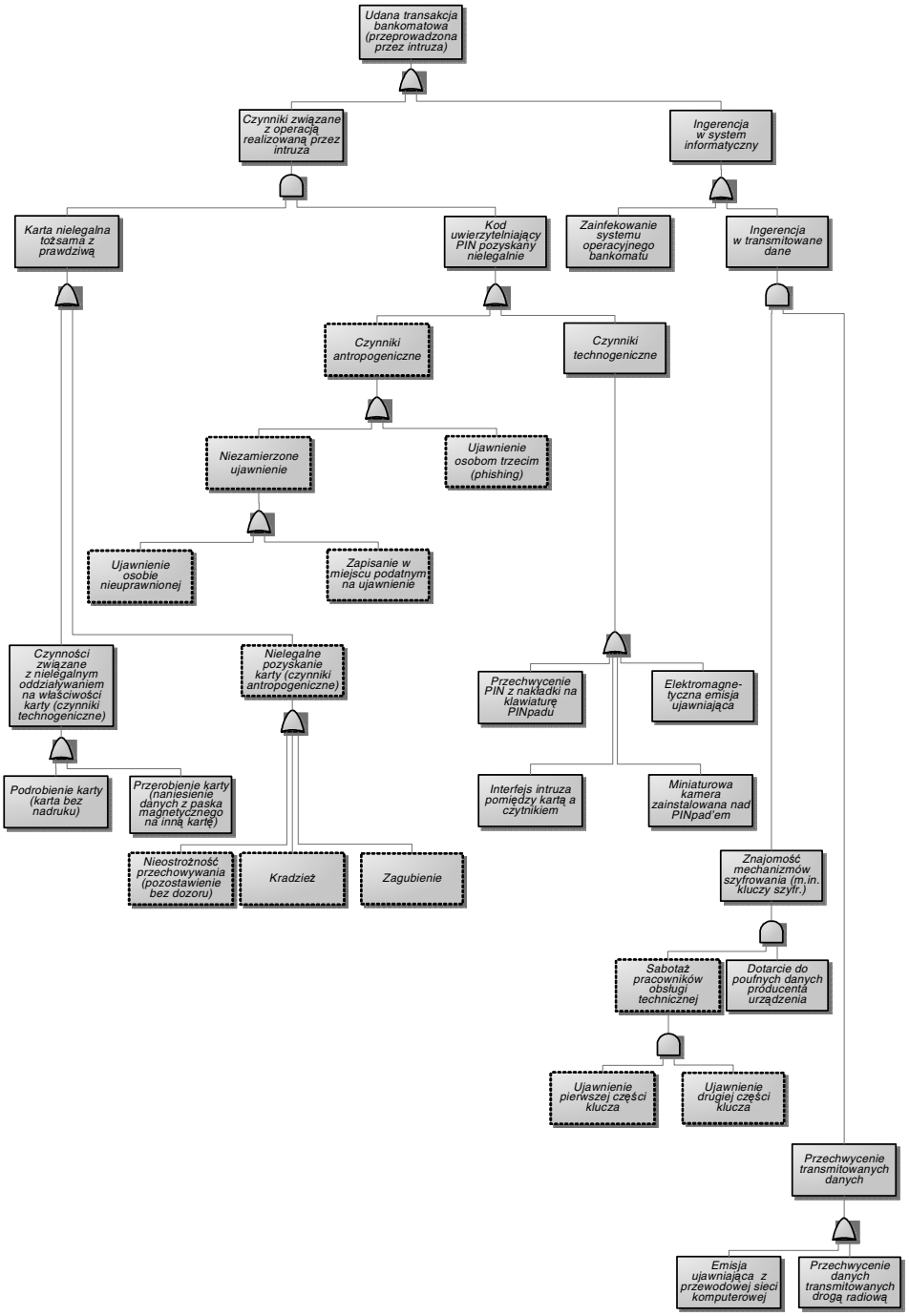
- nośnika informacji, na którym przechowywane są dane na karcie,
- funkcjonalności,
- operacji rozliczeniowych,
- prestiżu klienta i zasięgu działania karty i inne.

W przedstawionej dalej charakterystyce działań niepożądanych związanych z działalnością intruza zagrażającą bezpieczeństwu środków pieniężnych użytkownika karty bankowej (tzn. działań ukierunkowanych na kradzież tych środków) skupiono się na dwóch, spośród trzech możliwych do zrealizowania kategorii operacji kartami, tj.:
– operacji bankomatowej,
– transakcji za pomocą terminala POS (ang. *Point of Sale*),

Pominięto tu aspekty bezpiecznościowe związane z operacjami realizowanymi przez Internet (ang. *IO – Internet Order*), gdyż według dostępnych danych, stanowią one zaledwie około 0,33% liczby wszystkich transakcji wykonywanych kartami w Polsce [6].

Wszystkie wymienione operacje można przedstawić w formie graficznej – w postaci tzw. drzewa zdarzeń (błędów), w którym skutkiem rozpoczynającym drzewo (wierzchołek) jest udana próba intruza, polegająca na przeprowadzeniu nieuprawnionej transakcji kartowej. Są to więc przypadki, w których nie jest spełniony warunek konieczny bezpieczeństwa systemu (1), czyli takie, gdy działania systemu bezpieczeństwa nie są w stanie „zneutralizować" wszystkich czynników destrukcyjnych. Drzewa rozwijają się w kierunku zdarzeń poprzedzających [5]. Przedstawiają one kombinacje zdarzeń niepożądanych prowadzących do utraty stanu bezpieczeństwa (zmniejszenia niezawodności bezpieczeństwa) pary antropotechnicznej „człowiek – karta bankowa". Zdarzenia niepożądane, na które wpływ mają czynniki antropogeniczne wyróżniono przerywaną linią (rys. 2).

Dokonując jakościowej analizy zdarzenia „udana transakcja bankomatowa (przeprowadzona przez intruza)" (rys. 2), należy zwrócić uwagę na dwa wątki prowadzące do zdarzenia głównego. Pierwszy z nich jest ilustracją udanej próby transakcji bankomatowej za pomocą ingerencji w system informatyczny obsługujący bankomat. Ważnymi, z punktu widzenia bezpieczeństwa systemu człowiek–karta bankowa, są w tej gałęzi drzewa czynniki antropogeniczne (m.in. przechwycenie i wykorzystanie przez osoby trzecie kluczy szyfrujących transmisję bankomat – centrum autoryzacji). Pozostałe zdarzenia niepożądane (w tej gałęzi) są mało prawdopodobne ze względu na zastosowanie w wielu miejscach szyfrowania. Dotyczy to samej transmisji danych poprzez sieć komputerową, jak również urządzeń (klawiatur) do wprowadzania kodów PIN automatycznie szyfrujących dane. Większa część zagrożeń drugiego wątku (stosując tu tylko ich jakościową ocenę, nie wartościując poszczególnych prawdopodobieństw wystąpienia zagrożenia) wywołana jest działaniami intruza bezpośrednio przed lub na pulpicie bankomatu (czynniki technogeniczne: interfejsy pomiędzy kartą a czytnikiem, skanery, nakładki na klawiatury PIN-padów, minikamery) oraz niefrasobliwością użytkownika karty (czynniki antropogeniczne wynikające z nieodpowiedniego przechowywania PIN-u i karty: zapisania PIN-u w miejscu dostępnym osobom trzecim, zagubienia karty).



Rys. 2. Transakcja bankomatowa realizowana przez intruza – zdarzenia niepożądane

Drugą z wymienionych kategorii operacji kartowych jest transakcja z wykorzystaniem terminala POS, realizowana zazwyczaj w punkcie usługowym, handlowym, gastronomicznym itp. Schemat zagrożeń w tym przypadku jest dość podobny do drzewa przedstawionego (rys. 2) dla transakcji bankomatowej. Skutkiem rozpoczynającym takie drzewo jest „udana transakcja w terminalu POS" (przeprowadzona przez intruza). Warto tu zwrócić uwagę na nowe elementy drzewa związane z procesem uwierzytelniania karty i użytkownika (antropogeniczne), instalacją terminala (podatność na kradzież i odczytanie danych z urządzenia) oraz transmisją danych z terminala do systemu informatycznego firmy z wykorzystaniem wewnętrznej sieci komputerowej. Do tej ostatniej wykorzystywane są, na rozległych obszarach, często technologie bezprzewodowe. Od skuteczności działania sytemu bezpieczeństwa wewnętrznej sieci radiowej uzależnione jest działanie przeciwdestrukcyjne zapobiegające przechwyceniu i wykorzystaniu transmitowanych danych.

Niezależnie od różnic między drzewem zdarzeń przedstawionym dla operacji bankomatowych a drzewem zdarzeń dla operacji POS, należy wskazać kluczową rolę osłonową czynników antropogenicznych dotyczących procesu uwierzytelniania nie tylko użytkownika, ale też i oryginalności karty. Ważną rolę spełnia tu operator terminala funkcjonujący tu w roli bezpiecznościowego systemu osłonowego (sprzedawca, kelner). Skimming karty oraz naniesienie danych na inny „plastik" jest przecież łatwo wykrywalny. Wystarczy sprawdzenie 2 cech:

– numeru karty – numer karty wydrukowany na paragonie oraz ten, wytłoczony na kracie – w przypadku kart podrobionych z naniesionymi danymi na inną kartę – numery te różnią się;
– wyglądu karty – za podejrzaną należy uznać np. kartę bez nadruku.

Pozostaje tu jeszcze aspekt weryfikacji podpisu posiadacza karty umieszczonego na rewersie karty i złożonego na wydruku z terminalu. Jest to najprostsza (niestety pomijana i zawodna) metoda uwierzytelnienia posiadacza karty. Naganną praktyką stosowaną przez antropogeniczną część osłonowego podsystemu bezpieczeństwa jest brak zaangażowania w porównanie wzorów podpisu lub oddawanie do rąk płacącego karty, a dopiero potem żądanie potwierdzenia transakcji podpisem.

2. Przegląd zbioru zagrożeń dla operacji bankomatowych

Analizując szeroki wachlarz zagrożeń operacji bankomatowych, można go w pewien sposób usystematyzować. Jedną z możliwości jest skategoryzowanie zagrożeń i przyporządkowanie ich do grup związanych z intensywnością oddziaływania zagrożenia (tab. 1). Część z wymienionych w tabeli zagrożeń ma odzwierciedlenie w elementach (zdarzeniach niepożądanych) przedstawionego drzewa błędów sporządzonego dla przypadku dokonywania operacji bankomatowej (rys. 2).

Tabela 1. Zestawienie zagrożeń operacji bankomatowych

Lp.	Nazwa zagrożenia	Kategoria zagrożenia		
		Czynnik wyzwalający	Destrukcja odwracalna	Destrukcja nieodwracalna
1	Standaryzacja systemu operacyjnego bankomatu	X		
2	Kradzież nowej karty w trakcie przesyłania z banku do klienta		X	
3	Instore carding (uwierzytelnianie transakcji podpisem, bez PIN)	X	X	
4	Skimming (skanowanie i kopiowanie paska magnet. – nakładka na szczelinę czytnika)	X	X	
5	Rejestracja za pomocą kamery operacji na klawiaturze (wprowadzanie PIN)	X	X	
6	Rejestracja za pomocą skanującej nakładki na klawiaturę wprowadzany PIN	X	X	
7	Blokowanie zwrotu karty przez bankomat (w celu jej późniejszej kradzieży)		X	
8	Blokowanie śluzy wydajnika banknotów (w celu ich późniejszej kradzieży)		X	
9	Kradzież bankomatu			X
10	Wyłudzenia odszkodowań za rzekomo niezrealizowane transakcje	X	X	

3. Przegląd zbioru czynników bezpiecznościowych dla operacji bankomatowych

Wśród zbioru zagrożeń przyporządkowanych do kategorii antagonistycznych (tab. 2) względem odpowiednich kategorii zagrożeń bezpieczeństwa można znaleźć czynniki wpływające bezpośrednio na bezpieczeństwo wykonywanej operacji i eliminację zdarzeń niepożądanych oraz dodatkowe, pośrednio wpływające na bezpieczeństwo (pozycje 6–7, 9–10, 12–15).

Tabela 2. Zestawienie zabezpieczeń operacji bankomatowych

Lp.	Nazwa zabezpieczenia	Kategoria zabezpieczenia		
		Czynnik osłonowy	Czynnik interwencyjny	Czynnik ratunkowy
1	Kod PIN	X		
2	Autoryzacja online transakcji	X		
3	Szyfrowanie PIN przez PIN-pad	X		
4	Ochrona oprogramowania bankomatu przed szkodliwym oprogramowaniem	X		
5	Separacja sieci bankomatowej od sieci internet	X		
6	Ograniczenie wysokości transakcji		X	X
7	Blokada transakcji i zatrzymanie karty uznanej za skradzioną		X	
8	Kasowanie kluczy szyfrowych (w przypadku ingerencji intruza w strukturę PIN-padu)		X	

9	Zatrzymanie karty po 3-krotnym wprowadzeniu błędnego PIN	X	X	
10	Archiwizacja niepodjętych w określonym czasie banknotów (z powodu błędu klienta)		X	
11	Identyfikacja karty pod względem formalnym (w trakcie wprowadzania jej do czytnika)	X		
12	Zatrzymanie karty nieodebranej przez użytkownika po zakończeniu transakcji	X		
13	Alarmowanie za pomocą czujek (nieuprawnione otwarcie sejfu, mechaniczny lub termiczny atak na strukturę sejfu)		X	
14	Rejestracja za pomocą kamer użytkowników bankomatu	X		
15	Ubezpieczenie stanu konta			X

Podsumowanie

Przytoczone w opracowaniu rozważania, dotyczące bezpieczeństwa transakcji kartowych, można i należy analizować nie tylko w ujęciu jakościowym, ale także ilościowym. Ujęcie ilościowe wymaga informacji odnośnie do prawdopodobieństw poszczególnych zdarzeń wymienionych w drzewie (rys. 2) prowadzących do jego wierzchołka (czyli do niepożądanego skutku łańcucha zdarzeń elementarnych). Wskaźnikiem potencjału niebezpieczeństwa systemu kart bankowych może być prawdopodobieństwo zaistnienia nielegalnej transakcji kartowej. Posługując się tym wskaźnikiem, stosunkowo łatwo można ocenić potencjał bezpieczeństwa systemu oraz przypisać mu określony poziom bezpieczeństwa (np. bezpieczeństwo bezwzględne, względne, ograniczone).

Oszacowania wartości prawdopodobieństw zajścia zdarzeń niepożądanych można dokonać na podstawie danych statystycznych dotyczących liczby przestępstw danej kategorii. Uzyskanie wiarygodnych danych dotyczących oszustw przeprowadzanych za pomocą kart bankowych nie jest łatwym zadaniem, jak można się domyślać, tego typu statystyki nie są powodem do dumy dla żadnego z banków. Są one często cząstkowe i różnią się w zależności od źródła. Najczęściej występującymi przestępstwami z użyciem kart w Polsce (2004, jak podaje [7]) są transakcje kartami skradzionymi (około 50% liczby przestępstw), sfałszowanymi (18,2 %) i zagubionymi (17,6%).

Bibliografia

1. Będkowski L., Dąbrowski T.: Podstawy eksploatacji, cz. 2. Podstawy niezawodności eksploatacyjnej. Wyd. WAT, 2006.
2. Kubas M., Molski M.: Karta elektroniczna. Bezpieczny nośnik informacji. Wyd. Mikom, Warszawa 2002.

3. Markowski P.: Techniki zabezpieczenia wartości pieniężnych i dedykowanych dla nich urządzeń technicznych. Praca dyplomowa inżynierska, WAT, Warszawa 2010.
4. http://mfiles.pl/pl/index.php/Karta_bankowa.
5. Borysiewicz M., Furtek A., Potempski S.: Poradnik metod ocen ryzyka związanego z niebezpiecznymi instalacjami procesowymi. Instytut Energii Atomowej, Otwock – Świerk 2000.
6. www.nbp.pl/systemplatniczy/karty/q_01_2010.pdf, Informator o kartach płatniczych, 1 kw. 2010. NBP, Departament Systemu Płatniczego.
7. http://kartyonline.pl, Wiruk K.: Statystyki dotyczące przestępstw kartowych w okresie świąt Bożego Narodzenia. 2005.

Recenzent:
Wojciech ZAMOJSKI

The technical aspect of the safety analysis of the bankcard operations

Key words

Reliability of safety, card transaction safety, safety potential.

Summary

The question related to the safety of a specific human engineering system, such as the system of bankcard operations, is presented in the paper. The concept of the security system and the potential criterion of the safety state of the system are defined. Selected operations using bankcards and the classification of both the hazards and the protective actions are discussed. The security of bankcard systems in qualitative and technical aspects are characterised.