**dr hab. inż. Zbigniew Ciekanowski**

Państwowa Szkoła Wyższa im. Papieża Jana Pawła II w Białej Podlaskiej
Państwowa Wyższa Szkoła Techniczno-Ekonomiczna
im. ks. Bronisława Markiewicza w Jarosławiu

**mgr Jarosław Starczewski**

Społeczna Akademia Nauk w Łodzi

# UWARUNKOWANIA BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW TELEINFORMATYCZNYCH

# CONDITIONS FOR THE SECURITY OF INFORMATION AND DATA COMMUNICATION SYSTEMS

## Wstęp

Bezpieczeństwo teleinformatyczne to zbiór zagadnień z dziedziny telekomunikacji i informatyki, związany z szacowaniem i kontrolą ryzyka wynikającego z korzystania z komputerów, sieci komputerowych i przesyłania danych do zdalnych lokalizacji, rozpatrywany z perspektywy poufności, integralności i dostępności[1].

Poufność, integralność i dostępność są atrybutami wspólnymi dla ochrony informacji we wszystkich systemach teleinformatycznych, niezależnie od kategorii informacji w nich przetwarzanych. Poufność to zapewnienie, że informacje są dostępne tylko dla osób uprawnionych. Integralność należy rozpatrywać w dwóch aspektach – jako integralność danych i integralność systemu teleinformatycznego. Integralność danych to właściwość określająca, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony. Integralność systemu teleinformatycznego oznacza zaś, że system wykonuje swoją funkcję w sposób nienaruszony.

[1] Z. Ciekanowski (red.), *Infrastruktura bezpieczeństwa publicznego. Ogólnokrajowe i lokalne wyzwania cywilizacyjne,* Wydawnictwo Wyższej Szkoły Zarządzania i Prawa im. Heleny Chodkowskiej, Warszawa 2010, s. 142.

Przez dostępność rozumie się możliwość wykorzystania zasobu systemu teleinformatycznego na żądanie i w określonym czasie przez wyznaczonych użytkowników.

Wymagania stawiane sieciom i urządzeniom teleinformatycznym zróżnicowane są w zależności od wagi przetwarzanych informacji. Szczególne wymagania muszą spełniać systemy i sieci teleinformatyczne przetwarzające informacje niejawne.

Jednym z wymogów, który musi spełnić każda instytucja przetwarzająca dane osobowe, jest opracowanie i wdrożenie dwóch podstawowych dokumentów: polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Za opracowanie i wdrożenie dokumentacji odpowiada administrator danych, u którego dane są przetwarzane.

Do zadań administratora danych należy:
- wyznaczenie administratora bezpieczeństwa informacji;
- wyznaczanie osób upoważnionych do przetwarzania danych oraz określenie zasad nadawania uprawnień do przetwarzania danych osobowych;
- prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
- kontrola wprowadzania danych osobowych do systemu, tzn. jakie dane osobowe, przez kogo i kiedy zostały wprowadzone oraz komu są przekazywane.

## 1. Instrukcja zarządzania systemem teleinformatycznym

Instrukcja zarządzania systemem teleinformatycznym służącym do przetwarzania danych osobowych jest drugim dokumentem niezbędnym i wymaganym przez prawo w przypadku przetwarzania danych osobowych. Po opracowaniu jest ona zatwierdzana przez administratora danych – kierownika jednostki organizacyjnej lub osobę przez niego upoważnioną, musi być przyjęta do stosowania jako dokument obowiązujący[2].

W instrukcji opisuje się zasady przyznawania użytkownikowi systemu identyfikatora oraz określa procedury nadawania mu uprawnień i ich modyfikacji. Polega to na opisaniu wszystkich czynności z tym związanych, począwszy od utworzenia użytkownikowi konta, przydzielania i modyfikacji jego uprawnień, kończąc na usunięciu konta użytkownika z systemu po wygaśnięciu uprawnień do przetwarzania danych w systemie, np. po zakończeniu pracy przez pracownika w instytucji lub zmianie zakresu jego obowiązków.

Procedura ta powinna także określać zasady postępowania z hasłami administratorów systemów informatycznych, czyli osób odpowiedzialnych za prawidłowe jego funkcjonowanie, oraz administrowanie systemem w sytuacjach awaryjnych, np. podczas nieobecności administratora z powodu choroby lub urlopu.

[2] M. Kałużyńska-Jasak, 2016, *Wskazówki dotyczące sposobu opracowania instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.* Pobrane z: http://www.giodo.gov.pl/163/id_art/1064/j/pl/. (dostęp: 10.11.2018).

Kluczowe jest opisanie stosowanych metod i środków uwierzytelnienia oraz procedur związanych z ich zarządzaniem i użytkowaniem *(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, 2004, par. 5 pkt 2).* Wiąże się to z wypracowaniem trybu przydzielania haseł użytkownikom, określeniem, w jakiej formie są przekazywane, stopnia ich złożoności, np. z ilu znaków muszą się składać oraz ich powtarzalności. Hasła w systemie informatycznym powinny być przechowywane w postaci zaszyfrowanej[3]. Użytkownik po otrzymaniu hasła od administratora systemu powinien być zobowiązany do jego zmiany przy pierwszym logowaniu lub jego zmiana powinna być wymuszana przez konfigurację systemu. Główny Inspektor Ochrony Danych Osobowych zaleca, aby unikać przekazywania haseł przez osoby trzecie lub za pośrednictwem niechronionych wiadomości poczty elektronicznej. Dla bezpieczeństwa przetwarzanych danych w systemie winna być określona częstotliwość zmiany hasła przez użytkownika. Przy czym optymalnym zapewne rozwiązaniem jest wymuszanie tej operacji przez system.

Zapisy w instrukcji dotyczące procesu uwierzytelniania polegają na wskazaniu czynności, jakie musi wykonać użytkownik, aby uruchomić system informatyczny. Dotyczy to w szczególności zasad postępowania podczas logowania się do systemu. Przestrzeganie zasady zachowania poufności hasła przez użytkownika jest jednym ze sposobów uniemożliwienia przetwarzania danych przez osoby nieuprawnione.

Dlatego niezbędne jest określenie metod postępowania w takich przypadkach, jak:

- chwilowe zaprzestanie pracy, w przypadku konieczności opuszczenia stanowiska pracy przez użytkownika;
- podejrzenie naruszenia bezpieczeństwa systemu, wystąpienia incydentu bezpieczeństwa (np. brak możliwości zalogowania).

Tworzenie kopii zapasowych danych oraz kopii zapasowych systemu informatycznego, tzw. kopii bezpieczeństwa, jest szczególnie ważne dla bezpieczeństwa przetwarzanych informacji w systemie. Podstawowym przeznaczeniem kopii bezpieczeństwa jest zachowanie istotnych danych oraz programów. Wówczas w przypadku zniszczenia oryginału można odtworzyć dane lub oprogramowanie. Pozwoli to w maksymalnym stopniu zachować ciągłość działania systemu teleinformatycznego[4]. Dlatego też niezbędne jest wskazanie, które dane wymagają tworzenia kopii zapasowych i na jakich nośnikach oraz przy użyciu jakich programów będą wykonywane, a także, z jaką częstotliwością. Konieczne jest zastosowanie odpowiednich zabezpieczeń (ochrony) elektronicznych nośników informacji zawierających dane osobowe, kopii zapasowych przed nieuprawnionym przejęciem, odczytem, skopiowaniem lub

[3] Ibidem.

[4] K. Liderman, *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012, s. 159.

zniszczeniem. Niezwykle istotne jest opisanie sposobu likwidacji nośników zawierających kopie zapasowe danych w przypadku utraty ich przydatności lub uszkodzenia.

Opisując zabezpieczenia systemu informatycznego przed działalnością wirusów komputerowych oraz wszelkiego rodzaju innych szkodliwych oprogramowań, wskazuje się na możliwe źródła ich przedostania się do systemu oraz działania, jakie należy podejmować, aby minimalizować możliwość samoistnej instalacji takiego oprogramowania. Należy wymieniać dokładnie, jaki program antywirusowy został zainstalowany oraz opisać metody i częstotliwość aktualizacji wirusów. Jeżeli zamiast oprogramowania antywirusowego są stosowane inne metody ochrony przed szkodliwym oprogramowaniem, np. poprzez fizyczne odłączenie urządzeń od sieci, metody te także powinny być opisane.

Niezwykle ważne jest opisanie, w jaki sposób system odnotowuje udostępnianie danych (komu, kiedy i w jakim zakresie) odbiorcom.

Procedura wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych powinna określać cel i zakres oraz częstotliwość ich wykonywania. Powinny być także wymienione podmioty i osoby uprawnione do wykonywania przeglądów i konserwacji systemu informatycznego. Szczególnie dokładnie opisuje się procedurę wykonywania konserwacji systemu w przypadku zlecenia czynności osobom nieposiadającym upoważnień do przetwarzania danych (np. firmom zewnętrznym).

## 2. Ochrona fizyczna

Informacje niejawne stosownie dla danej klauzuli tajności muszą być przetwarzane w profesjonalnie chronionych pomieszczeniach. Informacje niejawne o klauzuli „tajne" i „ściśle tajne" przetwarzane są w kancelariach tajnych. Za zgodą kierownika jednostki organizacyjnej w kancelarii tajnej można także przetwarzać informacje niejawne o klauzuli „poufne" lub „zastrzeżone".

Kancelaria tajna jest wyodrębnioną komórką i stanowi centrum systemu ochrony informacji niejawnych. Podlega pełnomocnikowi ds. ochrony informacji niejawnych. Obsługiwana jest przez pracowników pionu ochrony, którzy odpowiedzialni są za właściwe rejestrowanie, przechowywanie, archiwizowanie, obieg i udostępnianie materiałów niejawnych osobom uprawnionym. Pracami kancelarii tajnej kieruje kierownik wyznaczony na stanowisko przez kierownika jednostki organizacyjnej. Organizacja pracy kancelarii tajnej musi zapewniać ustalenie w dowolnym momencie, gdzie znajduje się każdy dokument pozostający na jej stanie.

Kancelaria tajna winna znajdować się w miejscu ustronnym, ale nie powinna być narażona na możliwość skrytego wtargnięcia. Wybierając lokalizację dla pomieszczeń kancelarii tajnej, należy przewidzieć konieczność jej ewakuacji.

W kancelarii tajnej wydziela się pomieszczenia:

- archiwum, czyli miejsce pracy pracowników kancelarii;
- czytelnia – miejsce zapoznawania się osób upoważnionych z materiałami niejawnymi;

- pomieszczenie do wytwarzania dokumentów niejawnych, dla bezpiecznego stanowiska komputerowego lub sprzętu Tempest.

Pomieszczenie czytelni i rozmieszczenia sprzętu teleinformatycznego powinno znajdować się pod nadzorem wizyjnym pracowników kancelarii.

Przystąpienie Polski do Traktatu Północnoatlantyckiego (NATO) i Unii Europejskiej (UE) oraz podpisanie porozumień z innymi państwami zobowiązuje nasz kraj do zbudowania systemu ochrony informacji niejawnych[5].

Właściwe funkcjonowanie tego sytemu nadzorowane jest przez Szefa Agencji Bezpieczeństwa Wewnętrznego (ABW), który pełni funkcję Krajowej Władzy Bezpieczeństwa.

Umowy i wymiana informacji niejawnych obligują nasz kraj do tworzenia kancelarii tajnych międzynarodowych.

Warunkiem rozpoczęcia funkcjonowania kancelarii tajnej międzynarodowej jest jej wpisanie do ewidencji kancelarii tajnych międzynarodowych. Dla sfery cywilnej Rzeczypospolitej Polskiej wpis dokonywany jest na podstawie decyzji Szefa ABW.

Kancelaria tajna międzynarodowa musi spełniać wymagania bezpieczeństwa tych organizacji. Są one sprawdzane podczas oględzin dokonywanych przez służby ochrony państwa.

Uregulowania prawne NATO – dotyczące bezpieczeństwa – zawarte są w dokumencie C-M(2002) 49 z dnia 17 czerwca 2002 r. z późn. zm. oraz w dyrektywach wykonawczych.

Natomiast przepisy bezpieczeństwa UE uregulowane są w decyzji Rady Unii Europejskiej nr 2011/292/UE z dnia 31 marca 2011 r. oraz w decyzji Komisji Europejskiej nr 2001/844/EC z dnia 29 listopada 2001 r.

Aby systemy ochrony informacji niejawnych funkcjonowały prawidłowo, kancelarie tajne muszą spełniać wszystkie stawiane przed nimi wymagania.

Prawidłowe zabezpieczenie informacji niejawnych, zgodnie z przepisami, wymaga zastosowania właściwych środków bezpieczeństwa fizycznego. To one zapewniają przetwarzanym informacjom niejawnym:

- poufność, tzn. że informacja nie została ujawniona osobom do tego nieuprawnionym;
- integralność, tzn. że informacja nie została zmodyfikowana w sposób nieuprawniony;
- dostępność, tzn. że informacja jest możliwa do wykorzystania na żądanie podmiotu uprawnionego w określonym czasie.

Cele te osiąga się zapewniając właściwe przetwarzanie informacji, różnicując dostęp pracowników do informacji niejawnych, zgodnie z posiadanymi przez nich uprawnieniami, wykrywając i udaremniając działania nieuprawnione. Niezmiernie

[5] Wytyczne w sprawie postępowania z informacjami niejawnymi międzynarodowymi z dnia 31 grudnia 2010 r. szefa ABW file:///C:/Users/Zbigniew/Downloads/Wytyczne_w_sprawie_postepowania_z_informacjami_niejawnymi_miedzynarodowymi%20 (dostęp: 15.11.2018).

istotne jest uniemożliwienie dostępu do pomieszczeń lub wydzielonych obszarów, w których są przetwarzane informacje niejawne osobom, które nie posiadają upoważnienia do dostępu do tych informacji.

W *Rozporządzeniu Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych dla zabezpieczenia informacji niejawnych* (2012, par. 1 ust. 1) zostały wskazane:

- podstawowe kryteria i sposób określania poziomu zagrożeń;
- dobór środków bezpieczeństwa fizycznego odpowiednich do wskazanego poziomu zagrożeń;
- rodzaje zagrożeń, które należy uwzględnić przy określaniu poziomu zagrożeń;
- podstawowe elementy, które powinien zawierać plan ochrony informacji niejawnych;
- zakres stosowania środków bezpieczeństwa fizycznego;
- kryteria tworzenia stref ochronnych.

Dlatego też, bezpieczeństwo fizyczne przetwarzanych informacji niejawnych należy rozpatrywać w dwóch aspektach:

- właściwego określenia kategorii poziomu zagrożeń nieuprawnionym ujawnieniem lub utratą;
- doboru odpowiednich środków bezpieczeństwa w określonej kategorii zagrożeń.

Do czynników mających wpływ na bezpieczeństwo fizyczne przetwarzania informacji zalicza się: klauzule tajności przetwarzanych informacji niejawnych, ilość posiadanych materiałów, liczbę przetwarzanych informacji niejawnych w systemach teleinformatycznych, postać tych informacji, liczbę pracowników jednostki organizacyjnej mających dostęp do informacji niejawnych, zasady dostępu osób do budynku i jego lokalizację. Oceniając poziom zagrożeń, należy uwzględniać także inne czynniki mogące mieć wpływ na ochronę informacji niejawnych. Są nimi: działania obcych służb specjalnych, sabotaż, zamach terrorystyczny, kradzież lub pożar, a także działania sił przyrody.

W przypadku nowo organizowanego systemu ochrony informacji niejawnych przyjmuje się wartości szacunkowe dla takich czynników, jak: „klauzula tajności przetwarzanych informacji niejawnych", „liczba materiałów niejawnych", „postać informacji niejawnych" i „liczba osób"(rozporządzenie w sprawie środków bezpieczeństwa fizycznego, 2012, par. 1 ust. 1).

Określając poziom zagrożeń, przeprowadza się analizę, w której uwzględnia się wszystkie istotne czynniki mogące mieć wpływ na bezpieczeństwo przetwarzanych informacji niejawnych. Czynnikiem najistotniejszym jest klauzula tajności przetwarzanych informacji oraz ilość osób mających do nich dostęp. W wyniku przeprowadzonej analizy poziom zagrożeń można określić w jednej z trzech kategorii, jako: niski, średni lub wysoki.

Ustalony poziom zagrożeń decyduje o tym, w jakiej kombinacji należy zastosować środki bezpieczeństwa fizycznego. Są nimi zarówno rozwiązania organizacyjne

i wyposażenie, jak też urządzenia służące do ochrony informacji niejawnych, w tym także elektroniczne systemy pomocnicze, które wspomagają ich ochronę.

Do środków bezpieczeństwa fizycznego zaliczamy: personel bezpieczeństwa, bariery fizyczne, szafy i zamki, system kontroli dostępu, system sygnalizacji włamania i napadu, system dozoru wizyjnego, system kontroli osób, przedmiotów i pojazdów.

Zgodnie z rozporządzeniem w sprawie środków bezpieczeństwa fizycznego (2012, par. 5), informacje niejawne mogą być przetwarzane w strefach ochronnych: I, II, III lub specjalnej.

Strefą ochronną I określa się pomieszczenia lub obszary, w których są przetwarzane informacje niejawne o klauzuli „poufne" lub wyższej, a dostęp do tej strefy jest równoznaczny z bezpośrednim dostępem do tych informacji.

Pomieszczenie lub obszar, w którym jest zorganizowana strefa ochronna I, musi spełniać wymagania polegające na:

- wskazaniu w planie ochrony najwyższej klauzuli tajności przetwarzanych informacji niejawnych;
- określeniu granic i ich metod zabezpieczenia;
- wprowadzeniu systemu kontroli dostępu zezwalającego na wstęp osób posiadających odpowiednie uprawnienia w zakresie niezbędnym do wykonywania pracy;
- w przypadku konieczności wstępu innych osób przetwarzane informacje niejawne należy zabezpieczyć przed możliwością dostępu do nich przez te osoby. Ponadto zapewnia się nadzór osoby uprawnionej lub stosuje się równoważne mechanizmy kontrolne;
- możliwość wstępu do strefy jest wyłącznie ze strefy ochronnej.

Strefę ochronną II tworzą pomieszczenia lub obszary, w których są przetwarzane informacje niejawne o klauzuli „poufne" lub wyższej, a także gdy dostęp do strefy nie jest równoznaczny z bezpośrednim dostępem do informacji (rozporządzenie w sprawie środków bezpieczeństwa fizycznego, 2012, par. 5 ust. 2).

Wstęp do strefy odbywa się wyłącznie ze strefy ochronnej, przy czym musi ona spełniać dodatkowe wymagania przez:

- wyraźne określanie i zabezpieczenie granic;
- wprowadzenie systemu kontroli dostępu zezwalającego na wstęp osób, które posiadają odpowiednie uprawnienie do dostępu do informacji niejawnych w zakresie niezbędnym do wykonywania pracy.

Strefę ochronną III stanowią pomieszczenia lub obszary z wyraźnym określeniem granic, umożliwiające kontrolowanie osób i pojazdów.

Specjalną strefę ochronną tworzy się w strefie ochronnej I lub II. Strefę specjalną chroni się przed podsłuchem, a także musi ona spełniać dodatkowe niżej wymienione wymagania:

- wyposaża się ją w system sygnalizacji włamania i napadu;
- pozostaje zamknięta, gdy nikogo w niej nie ma;

- w przypadku posiedzenia niejawnego, jest chroniona przed wstępem osób nieupoważnionych;
- podlega inspekcjom przeprowadzanym według zaleceń ABW albo Służby Kontrwywiadu Wojskowego przynajmniej raz w roku, a także po każdym nieuprawnionym wejściu do strefy;
- w strefie tej nie mogą znajdować się linie komunikacyjne, telefony, inne urządzenia komunikacyjne ani sprzęt elektryczny lub elektroniczny, których umieszczenie nie zostało zaakceptowane w sposób określony w opracowanych procedurach bezpieczeństwa.

Ponadto w strefie ochronnej I lub II można utworzyć pomieszczenie wzmocnione. W pomieszczeniu takim dopuszczalne jest przechowywanie informacji niejawnych poza odpowiednimi szafami. Konstrukcja pomieszczenia powinna zapewniać ochronę równoważną ochronie zapewnianej przez szafy przeznaczone do przechowywania informacji niejawnych o tej samej klauzuli tajności.

Tymczasowo w strefie ochronnej III można utworzyć: strefę ochronną I, strefę ochronną II lub specjalną strefę ochronną. Utworzenie tymczasowej strefy może być powodowane koniecznością odbycia np. posiedzenia niejawnego.

Klauzula tajności informacji niejawnych decyduje, w jakiej strefie się je przetwarza i jakie stosuje się zabezpieczenia fizyczne (rozporządzenie w sprawie środków bezpieczeństwa fizycznego, 2012, par. 7).

Informacje niejawne „ściśle tajne" przetwarza się w strefie ochronnej I lub II oraz przechowuje się w szafie metalowej klasy odporności na włamanie S2 lub w pomieszczeniu wzmocnionym. W tym przypadku stosuje się także kombinację środków uzupełniających polegających na:

- stałej ochronie lub kontroli w nieregularnych odstępach czasu;
- wykorzystaniu systemu dozoru wizyjnego, z obowiązkową rejestracją w rozdzielczości nie mniejszej niż 400 linii telewizyjnych; zarejestrowany zapis przechowywany jest przez minimum 30 dni;
- zainstalowaniu systemu sygnalizacji włamania i napadu obsługiwanego przez personel bezpieczeństwa wykorzystującego również system dozoru wizyjnego.

Informacje niejawne o klauzuli „tajne" przetwarza się w strefie ochronnej I lub II i przechowuje się w szafie metalowej spełniającej co najmniej wymagania klasy odporności na włamanie S1 lub w pomieszczeniu wzmocnionym.

Informacje niejawne o klauzuli „poufne" przetwarza się w strefie ochronnej I, II lub III. Przechowuje się je w strefie ochronnej I lub II w szafie metalowej lub w pomieszczeniu wzmocnionym.

Informacje niejawne o klauzuli „zastrzeżone" przetwarza się w pomieszczeniach lub obszarach, które wyposaża się w system kontroli dostępu i przechowuje się w szafach metalowych, zamkniętych na klucz meblach biurowych lub pomieszczeniach wzmocnionych.

Informacje niejawne w systemach teleinformatycznych przetwarza się w strefach ochronnych w zależności od klauzuli tajności, uwzględniając wyniki procesu szacowania ryzyka:

- o klauzuli „poufne" lub wyższej w strefie ochronnej I lub II;
- o klauzuli „zastrzeżone" w pomieszczeniu lub obszarze wyposażonym w system kontroli dostępu.

Serwery, systemy zarządzania siecią, kontrolery sieciowe, a także inne newralgiczne elementy systemów teleinformatycznych rozmieszcza się, uwzględniając wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym. W strefie ochronnej III mogą być przetwarzane informacje niejawne o klauzuli „zastrzeżone". W przypadku przetwarzania informacji niejawnych o klauzuli „poufne" lub wyższej sprzęt teleinformatyczny umieszcza się w strefie ochronnej I lub II.

Informacje niejawne w częściach mobilnych zasobów systemu teleinformatycznego przetwarza się zgodnie z zapisami zawartymi w dokumentacji bezpieczeństwa systemu teleinformatycznego, uwzględniając wyniki procesu szacowania ryzyka.

## Podsumowanie

Wszystkie systemy informatyczne, zarówno w sektorze publicznym, jak i prywatnym, powinny być budowane z wielką rzetelnością. Muszą być określone obowiązki i odpowiedzialność właścicieli, dostawców i użytkowników systemów. Należy wzmacniać świadomość oraz budować etykę korzystania z systemów informacyjnych. Środki, dobre praktyki i procedury zapewniające bezpieczeństwo systemów powinny uwzględniać aspekty techniczne, administracyjne, organizacyjne, handlowe, edukacyjne i prawne. Poziomy zabezpieczeń, koszty, środki, praktyki i procedury powinny być odpowiednio dobrane i proporcjonalne do wartości systemów. Jednocześnie należy brać pod uwagę to, że wymagania dla poszczególnych systemów są różne. Trzeba na bieżąco szacować ryzyko wystąpienia szkody oraz jak poważne i jak prawdopodobne byłyby szkody i ich zasięg. W przypadku naruszeń bezpieczeństwa systemów bardzo istotne jest zapewnienie „działania w porę", polegającego na współpracy wszystkich użytkowników, w tym na poziomie międzynarodowym. Systemy, szczególnie systemy informatyczne państwa, powinny być skoordynowane i zintegrowane ze sobą, a także tworzyć spójny system bezpieczeństwa. Każde państwo musi chronić zasoby, sieci i systemy teleinformatyczne przed zamierzonymi i niezamierzonymi szkodliwymi działaniami w cyberprzestrzeni. W interesie wspólnoty międzynarodowej jest, aby każde państwo zaostrzyło politykę ochrony własnej cyberprzestrzeni.

Trzeba jednak zdać sobie sprawę, że nawet najlepsze uregulowania prawne czy wdrażanie najnowocześniejszych systemów zabezpieczeń nie uchronią informacji przed cyberatakami. To człowiek jest najsłabszym ogniwem, dlatego szczególnie ważne jest budowanie świadomości i odpowiedzialności poprzez edukację społeczeństwa na temat zagrożeń związanych z cyberprzestrzenią. Świadomość ludzka jest najlepszą ochroną.

## Streszczenie

Wymagania stawiane sieciom i urządzeniom teleinformatycznym zróżnicowane są w zależności od „wagi" przetwarzanych informacji. Szczególne wymagania muszą spełniać systemy i sieci teleinformatyczne przetwarzające informacje niejawne. W artykule przedstawiono uwarunkowania bezpieczeństwa zarówno informacji, jak i systemów teleinformatycznych. Szczegółowo odniesiono się do instrukcji zarządzania systemem teleinformatycznym oraz do ochrony fizycznej procesu przetwarzania informacji niejawnych.

**Słowa kluczowe:** administrator, bezpieczeństwo, informacja, system, ochrona.

## Summary

Requirements for networks and ICT devices vary depending on the "weight" of the information being processed. Particular requirements must be met by teleinformation systems and networks that process undisclosed information. The article presents the conditions for the security of both information and ICT systems. The detailed reference is made to the IT system management instructions and to the physical protection of classified information processing.

**Key words:** administrator, security, information, system, protection.

## Literatura:

1. Ciekanowski Z. (red.), *Infrastruktura bezpieczeństwa publicznego. Ogólnokrajowe i lokalne wyzwania cywilizacyjne,* Wydawnictwo Wyższej Szkoły Zarządzania i Prawa im. Heleny Chodkowskiej, Warszawa 2010.
2. Kałużyńska-Jasak M. (2016), *Wskazówki dotyczące sposobu opracowania instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.* Pobrane z: http://www.giodo.gov.pl/163/id_art/1064/j/pl/.
3. Liderman K., *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012.
4. *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* (Dz. U. z 2004 r. Nr 100, poz. 1024).
5. *Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych dla zabezpieczenia informacji niejawnych (*Dz. U. z 2012 r., poz. 683).