Sebastian KALETA
doktorant na Wydziale Bezpieczeństwa Narodowego
Akademii Obrony Narodowej

BEZPIECZEŃSTWO INFORMACJI NIEJAWNYCH W SYSTEMACH I SIECIACH TELEINFORMATYCZNYCH SIŁ ZBROJNYCH RZECZYPOSPOLITEJ POLSKIEJ

Słowa kluczowe: bezpieczeństwo narodowe, bezpieczeństwo teleinformatyczne, cyberprzestrzeń, infrastruktura krytyczna, ochrona informacji niejawnych, siły zbrojne.

STRESZCZENIE

W XXI wieku, w którym ranga informacyjnego wymiaru bezpieczeństwa znacznie wzrosła, a informacja stała się towarem pożądanym, wręcz strategicznym, jej pozyskanie i umiejętne wykorzystanie może przyczynić się do sukcesu organizacji. Szczególnie istotne znaczenie posiadają informacje niejawne, których nieuprawnione ujawnienie może wiązać się z zagrożeniem bezpieczeństwa państwa i jego obywateli.

W artykule wskazano główne zagrożenia dla systemów teleinformatycznych Sił Zbrojnych Rzeczypospolitej Polskiej, przetwarzających informacje niejawne. Omówiono także strukturę i zadania elementów systemu reagowania na incydenty komputerowe w resorcie obrony narodowej.

Niezwykle intensywny rozwój technologiczny, zauważalny zwłaszcza w drugiej połowie XX wieku, jest procesem świadczącym o niemalże nieograniczonych możliwościach ludzkiego umysłu. Poziom rozwoju technologicznego stanowi wyzwanie dla ludzkości, ale jednocześnie oddziałuje na jej bezpieczeństwo. Jest również jednym z najważniejszych czynników określających bezpieczeństwo państw i warunki realizacji przez nie swej polityki. Nieograniczone możliwości techniczne rodzą nowe potrzeby i oczekiwania, które są bodźcem do poszukiwania nowych rozwiązań technologicznych. To z kolei, powoduje uzależnienie państw oraz ich

obywateli od funkcjonowania infrastruktury teleinformatycznej, zwiększając jej znaczenie w kontekście polityki bezpieczeństwa narodowego[1]. W skrajnych przypadkach infrastruktura teleinformatyczna może stać się zagrożeniem. Poziom oraz charakter potencjalnych zakłóceń i zagrożeń uzależniony jest od poziomu techniki. Doskonałym tego przykładem był „Problem roku 2000" związany z „krytycznymi datami": 9 i 19 września 1999 roku, 1 stycznia 2000 roku, 29 lutego 2000 roku oraz 1 marca 2000 roku. Uzależnienie od systemów teleinformatycznych sprawiło, że należało spodziewać się możliwości wystąpienia zakłóceń w takich sektorach działalności państwa jak bankowość, gospodarka, media, itp. Kolejnym przykładem są zdarzenia, które miały miejsce w Estonii w 2007 roku. Doszło tam do zakłóceń funkcjonowania ruchu internetowego. Znacząco wzrosła ilość danych przesyłanych na rządowe serwery, co w efekcie doprowadziło do ich przeciążenia i w konsekwencji niedostępności portali instytucji rządowych dla użytkowników Internetu. W wyniku zalewu danymi – w ilości kilkakrotnie większej niż przepustowość estońskiej infrastruktury – została ona praktycznie sparaliżowana.

Od powstania w 1990 roku Internetu, szczególne znaczenie dla bezpieczeństwa narodowego zyskał wymiar technologiczny globalizacji, związany z wysoką dynamiką zmian w sferze komunikacji i informacji oraz postępującą integracją systemów informatycznych i telekomunikacyjnych. Pogłębiło to charakter procesów globalizacyjnych, przenosząc procesy gospodarcze, społeczno-polityczne, kulturowe, itp. w cyberprzestrzeń[2]. W dobie powszechnej informatyzacji, rozwoju technologicznego, pojawiają się nowe zagrożenia, które nie występowały w minionych czasach np. kradzież wirtualnych pieniędzy. W dzisiejszych czasach utrata bazy danych systemu informatycznego może spowodować paraliż firmy, a kradzież jednego serwera doprowadzić do upadku organizacji. Rozmaite systemy komputerowe i inne narzędzia elektroniczne są dziś wykorzystywane w każdej gałęzi gospodarki

[1] Bezpieczeństwo narodowe to najważniejsza wartość, potrzeba narodowa i priorytetowy cel działalności państwa, jednostek i grup społecznych, a jednocześnie proces obejmujący różnorodne środki, gwarantujące trwały, wolny od zakłóceń byt i rozwój narodowy (państwa), w tym ochronę i obronę państwa jako instytucji politycznej oraz ochronę jednostek i całego społeczeństwa, ich dóbr i środowiska naturalnego przed zagrożeniami, które w znaczący sposób ograniczają jego funkcjonowanie lub godzą w dobra podlegające szczególnej ochronie – W. Kitler, *Bezpieczeństwo Narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Warszawa 2011, s. 31.

[2] Cyberprzestrzeń – cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami – *Rządowy Program Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016*.

oraz na wszystkich szczeblach struktur państwowych. Poprzez użycie odpowiednich narzędzi i technik teleinformatycznych istnieje możliwość wpłynięcia nie tylko na procesy zachodzące w samej infrastrukturze teleinformatycznej, ale także w systemach z nią powiązanych.

Istotnym zagrożeniem może być oddziaływanie w cyberprzestrzeni, skierowane w systemy i sieci teleinformatyczne infrastruktury krytycznej. Skutkiem takich działań mogą być zarówno straty materialne, jak i sparaliżowanie istotnych sfer życia publicznego[3].

Oznacza to konieczność odpowiedniej ochrony infrastruktury opartej na technologiach informatycznych, a w szczególności tzw. infrastruktury krytycznej[4]. Szczególną rolę odgrywają sieci teleinformatyczne, ponieważ są one jednym z elementów infrastruktury krytycznej oraz spoiwem integrującym działanie jej pozostałych składników.

Powołany przez Prezesa Rady Ministrów Zespół ds. Krytycznej Infrastruktury Teleinformatycznej uzgodnił definicję infrastruktury teleinformatycznej: *systemy i sieci teleinformatyczne, których nieprawidłowe funkcjonowanie lub uszkodzenie, niezależnie od przyczyn i zakresu, może spowodować istotne zagrożenie dla życia lub zdrowia ludzi, interesów obronności oraz bezpieczeństwa państwa i obywateli albo narazić te interesy na co najmniej znaczną szkodę*[5].

Do krytycznych systemów i sieci teleinformatycznych zaliczamy infrastrukturę teleinformatyczną podmiotów następujących sektorów:

– energetycznego (elektrownie, spółki paliwowe),
– finansowego i bankowego (NBP, banki komercyjne, warszawska Giełda Papierów Wartościowych),
– zbrojeniowego i obrony narodowej (spółki zbrojeniowe, jednostki wojskowe),

---

[3] *Strategia Bezpieczeństwa Narodowego,* Warszawa 2007, pkt 2.2.36.

[4] Infrastruktura krytyczna – *systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy: zaopatrzenie w energię i paliwa; łączności i sieci teleinformatycznych, finansowe; zaopatrzenia w żywność i wodę; ochrony zdrowia; transportowe i komunikacyjne; ratownicze; zapewniające ciągłość działania administracji publicznej; produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych*. – Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym*, Dz. U. z 2007 r., nr 89, poz. 590 ze zm., art. 3 ust. 2.

[5] *Sprawozdanie przewodniczącego Zespołu ds. Krytycznej Infrastruktury Teleinformatycznej*, 28 kwietnia 2005 r.

– rządowego (urzędy centralne, administracja publiczna, dyplomacja),
– naukowego (instytuty badawcze),
– służb (Policja, BOR, SG),
– operatorów telekomunikacyjnych (podmioty komercyjne),
– innych (strategiczne zakłady, zaopatrzenie),

a także systemy i sieci przeznaczone do przetwarzania informacji niejawnych[6], na które należy zwrócić szczególną uwagę, ponieważ dbałość o niezagrożone warunki funkcjonowania państwa czy innych organizacji, wiąże się nierozerwalnie z potrzebą ciągłego monitorowania otoczenia oraz bronienia dostępu do własnych tajemnic. We współczesnym świecie informacja (niezależnie od formy jej występowania – elektronicznej czy papierowej) stanowi zasób strategiczny państw i organizacji. Jest podstawą sprawnego funkcjonowania firm, administracji oraz życia jednostek i jednocześnie gwarantem ich istnienia. Pozyskanie informacji we właściwym czasie i prawidłowe jej przetworzenie może stać się źródłem sukcesu organizacji, np. przyczyniając się do wzrostu konkurencyjności na rynku czy intensyfikacji rozwoju. Konsekwencje naruszenia bezpieczeństwa poprzez nieuprawnione ujawnienie informacji, także tych przetwarzanych w systemach teleinformatycznych, mogą okazać się katastrofalne w skutkach, gdyż bezpieczeństwo informacji oraz poufność danych są gwarantem ochrony materialnych i niematerialnych zasobów państw, organizacji jak i pojedynczych obywateli. Ochrona ważnych zasobów informacyjnych jest sferą działania państwa, ściśle związaną z jego bezpieczeństwem. Skuteczne działanie wymaga utajnienia części informacji w taki sposób, aby potencjalny przeciwnik nie mógł przeciwdziałać przyjętemu zamierzeniu. Utajnienie oznacza trafną weryfikację zakresu informacji podlegających ochronie. Pozyskanie przez obce instytucje informacji, szczególnie niejawnych o najwyższych klauzulach tajności (ściśle tajne[7],

[6] M. Ludwiszewski, *Monitoring stanu bezpieczeństwa teleinformatycznego państwa*, [w:] *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, M. Terlikowski, Warszawa 2009, s. 126.

[7] Zgodnie z art. 5. ust. 1 ustawy z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych*, Dz. U. z 2010 r., nr 182, poz.1228, informacjom niejawnym nadaje się klauzulę „ściśle tajne" jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że: zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej; zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej; zagrozi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej; osłabi gotowość obronną Rzeczypospolitej Polskiej; doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizacje zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie.

tajne[8]), niewątpliwie wpłynęłoby na stan bezpieczeństwa państwa, poprzez stworzenie zagrożenia dla jego niepodległości, suwerenności, integralności terytorialnej, czy też osłabienia gotowości obronnej. Nietrudno wyobrazić sobie, jakie mogłyby być konsekwencje pozyskania przez obcy wywiad informacji na temat struktury, organizacji i funkcjonowania systemu kierowania państwem oraz dowodzenia siłami zbrojnymi w czasie zagrożenia państwa lub wojny, czy też planowanego ataku na wrogie ugrupowania przeciwnika na kilka godzin przed uderzeniem. Również utrata informacji o niższych klauzulach tajności (poufne[9], zastrzeżone[10]) może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych. Dlatego też ochrona informacji

---

[8] Informacjom niejawnym nadaje się klauzulę „tajne", jeżeli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej przez to, że: uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej; pogorszy stosunki Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi; zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych Rzeczypospolitej Polskiej; utrudni wykonywanie czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione; w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości; przyniesie stratę znacznych rozmiarów w interesach ekonomicznych Rzeczypospolitej Polskiej; tamże art. 5 ust. 2.

[9] Informacjom niejawnym nadaje się klauzulę „poufne", jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że: utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej; utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową sił zbrojnych Rzeczypospolitej Polskiej; zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli; utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości; zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej; wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej; tamże, art. 5 ust. 3.

[10] Informacjom niejawnym nadaje się klauzulę „zastrzeżone", jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej; tamże, art. 5 ust. 4.

niejawnych[11] powinna być traktowana jako jeden z kluczowych elementów bezpieczeństwa państwa i jego obywateli.

Konsekwencje naruszenia bezpieczeństwa, a tym samym ujawnienia informacji, mogą okazać się katastrofalne w skutkach, gdyż poufność danych oraz bezpieczeństwo informacji są gwarantem ochrony niematerialnych i materialnych zasobów państwa. Administracja państwowa czy też organizacje, których działalność związana jest z bezpieczeństwem państwa, posiadają informacje znacznie większej wagi. Ujawnienie ich może spowodować wyjątkowo poważna szkodę dla kraju, np. zagrozić jego niepodległości, bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu, czy tez utrudnić prowadzenie polityki zagranicznej. Dlatego też dbałość o bezpieczne warunki egzystencji państwa czy organizacji, wiąże się nierozerwalnie z potrzebą ciągłego rozpoznawania otoczenia i bronienia dostępu do własnych tajemnic. Ciągły rozwój technologiczny stwarza możliwość przesyłania informacji przy użyciu systemów teleinformatycznych. Z jednej strony gwarantują one znacznie szybszy i ciągły dostęp do informacji, z drugiej zaś strony łatwość zaatakowania systemów teleinformatycznych nakłada na organizacje obowiązek zapewnienia im skutecznej ochrony. Systemy informatyczne stanowią kluczowe elementy procesu podejmowania decyzji w organizacjach wojskowych i cywilnych. Ich dotychczasowy rozwój i zakresy wdrożeń pozwalają prognozować, że obszary zastosowań informatycznych będą obejmować coraz większe przestrzenie funkcjonalne. Teoretycznie został stworzony niemalże nieograniczony dostęp do ogromnych zbiorów informacji, w tym: finansowych, przemysłowych, marketingowych, technologicznych, wojskowych i innych.

Celem niniejszego artykułu jest ukazanie zagrożeń dla bezpieczeństwa informacji niejawnych przetwarzanych w systemach teleinformatycznych oraz wymogów mających zapewnić to bezpieczeństwo w resorcie obrony narodowej.

Siły Zbrojne są szczególnie uzależnione od systemów informatycznych, a ich wzrastająca informatyzacja wymusza potrzebę wypracowania skutecznych środków polityki bezpieczeństwa informacji. Konieczność szybkiego i ciągłego dostępu do informacji stanowiła podstawę do utworzenia w siłach zbrojnych systemów teleinformatycznych umożliwiających przesyłanie informacji niejawnych, a co za tym idzie, wypracowania skutecznego systemu ich ochrony.

Mając na uwadze fakt, iż ranga informacyjnego wymiaru bezpieczeństwa w ostatnim czasie wyraźnie wzrasta, w efekcie czego zaczęło być ono traktowa-

[11] Informacje niejawne – to informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania; tamże, art. 1 ust. 1.

ne jako odrębny aspekt polityki bezpieczeństwa, można sformułować następującą tezę: w związku z rosnącym zapotrzebowaniem na informacje, systemy oraz sieci teleinformatyczne należy projektować w taki sposób, aby możliwie skutecznie chronić je przed dostępem nieuprawnionych do nich instytucji, agend bądź osób i jednocześnie zapobiec przed niepożądanym pozyskaniem informacji. Należy też stworzyć skuteczny system organów kontrolujących stan bezpieczeństwa informacji niejawnych przetwarzanych w systemach i sieciach teleinformatycznych.

Za początek powstania sieci teleinformatycznych umożliwiających przetwarzanie informacji niejawnych można przyjąć 1969 rok, kiedy w USA, na zlecenie Departamentu Obrony, powstała pierwsza sieć teleinformatyczna ARPANET. Celem utworzenia sieci było sprawdzenie możliwości zaprojektowania i stworzenia struktury sieciowej, zdolnej do działania bez jednego, wyróżnionego punktu centralnego lub też po usterce pewnej jej części. Ujawniło to militarny jej charakter, ponieważ rozproszona struktura sieciowa zdecydowanie lepiej nadaje się do prowadzenia działań w warunkach wojennych i pozwala zachować komunikację, mimo awarii lub zniszczenia jej części. Powstanie sieci zapoczątkowało połączenie ze sobą dwóch ośrodków badawczych w Los Angeles i Santa Barbara, realizując założenia narzucone przez wojsko, czyli brak jednego, wyróżnionego punktu centralnego. W 1983 roku eksperyment został uznany za udany i rozpoczęto odłączanie od całości struktury węzłów służących wojsku, w wyniku czego powstały trzy sieci zawierające informacje o klauzuli ściśle tajne i tajne.

Wraz za wzrostem znaczenia informacji rosną zagrożenia dla jej bezpieczeństwa. Systemy informacyjne i sieci informatyczne są narażone (podatne na szerokie spektrum zagrożeń) na zagrożenia bezpieczeństwa pochodzące z wielu różnych źródeł, łącznie z użyciem komputera, szpiegostwem, sabotażem, wandalizmem, pożarem, czy powodzią[12].

Szczególne znaczenie ma ochrona informacji niejawnych – przechowywanych lub przekazywanych w postaci elektronicznej. Ważnym zadaniem jest opracowanie i wdrożenie przejrzystych zasad dostępu uprawnionych organów państwa do treści przesyłanych drogą elektroniczną. Wymaga to ciągłego dostosowywania prawa telekomunikacyjnego, aby – mimo – szybkiego postępu technologicznego – stale odpowiadały współczesnym realiom, uwzględniając bezpieczeństwo Polski[13].

Zagrożenia bezpośrednio wpływające na system teleinformatyczny i przetwarzaną w nim informację można sklasyfikować następująco:

---

[12] A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem informacyjnym*, Warszawa 2010, s. 22.

[13] *Strategia…*, dz. cyt., pkt 3.8.80.

- siły wyższe (klęski żywiołowe, katastrofy finansowe, zmiany prawa, itp.), których możliwymi skutkami są: zniszczenie informacji i zasobów fizycznych, utrata dostępności, obniżenie poziomu ochrony.
- nieuprawnione i przestępcze działania ludzi, w tym:
  - zagrożenia związane z kradzieżami fizycznymi i zagubieniami sprzętu, oprogramowania i dokumentów, których możliwe skutki to: głównie utrata dostępności i poufności informacji;
  - zagrożenia związane z podsłuchami różnego typu sprzętu i oprogramowania, których możliwe skutki to: utrata poufności informacji;
  - nieuprawnione działania personelu, których możliwe skutki to: utrata dostępności, integralności i poufności informacji, obniżenie poziomu ochrony;
  - nieuprawnione działania osób postronnych – możliwe skutki: utrata dostępności, integralności i poufności informacji, obniżenie poziomu ochrony;
- błędy personelu obsługującego system komputerowy, których możliwymi skutkami są: utrata dostępności, integralności i poufności informacji, obniżenie poziomu ochrony.
- skutki złej organizacji pracy, w tym zagrożenia związane z błędami w ochronie fizycznej i technicznej, co stwarza możliwość utraty dostępności, integralności i poufności.
- awarie i uszkodzenia sprzętu oraz wady oprogramowania, których możliwymi skutkami są: głównie utrata dostępności informacji oraz obniżenie poziomu ochrony[14].

Piotr Sienkiewicz i Tomasz Goban-Klaus jako zagrożenia informacji w sieciach teleinformatycznych wskazują na sabotaż i zagrożenia nieumyślne oraz infiltrację. Do pierwszej grupy zaliczyli zagrożenia charakteryzujące się występowaniem strat bez pośredniego informacyjnego czy materialnego zysku. Natomiast celem infiltracji jest działanie osób nieuprawnionych, dążących do zapewnienia sobie dostępu do informacji[15].

Jednym z największych zagrożeń dla utraty poufności informacji stanowią osoby, które pomimo tego, iż posiadają poświadczenie bezpieczeństwa uprawniające do dostępu do tych informacji, mogą w sposób świadomy lub poprzez nieuwagę, czy też własne zaniedbanie, dopuścić do ujawnienia informacji niejawnych. Osoby

[14] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2008, s. 42.

[15] A. Wisz, *Bezpieczeństwo informacji w wojskowych sieciach teleinformatycznych*, s. 73, www.bbn.gov.pl\download\1\1002\bezpieczenstwoinformacji.pdf (dostęp: 01.06.2013 r.).

posiadające poświadczenie bezpieczeństwa, a więc dające rękojmię zachowania tajemnicy są zobowiązane do:

- nieujawniania tych informacji osobom nieuprawnionym, także po rozwiązaniu umowy o pracę lub zakończeniu służby wojskowej;
- nieprowadzenia rozmów na tematy związane z treścią dokumentów niejawnych w obecności osób nieuprawnionych;
- nieprzekazywania informacji niejawnych przez nieutajnione środki łączności;
- niewynoszenia poza teren jednostki organizacyjnej dokumentów, materiałów lub przedmiotów niejawnych bez zezwolenia właściwego przełożonego oraz bez należytego zabezpieczenia;
- wykonywania i przechowywania dokumentów niejawnych w miejscach do tego przeznaczonych, w sposób uniemożliwiający ich ujawnienie;
- sporządzania notatek zawierających informacje niejawne w zaewidencjonowanych nośnikach informacji (notatnikach, dyskietkach itp.);
- powiadamiania swoich przełożonych lub pełnomocnika do spraw ochrony informacji niejawnych o wszelkich zjawiskach zagrażających ujawnieniu informacji niejawnych.

Żołnierze zawodowi są obowiązani zachować w tajemnicy wszystkie informacje niejawne, z którymi zapoznali się podczas/lub w związku z pełnieniem czynnej służby wojskowej, w tym również informacje stanowiące tajemnicę innego państwa chronioną na zasadzie wzajemności na podstawie zawartych umów międzynarodowych. Obowiązek zachowania tajemnicy trwa zarówno w czasie pełnienia zawodowej służby wojskowej, jak i po zwolnieniu z niej.

Jednym z najistotniejszych zagrożeń dla informacji niejawnych przetwarzanych w systemach teleinformatycznych są działania w cyberprzestrzeni, którą charakteryzuje:

– aterytorialność – czyli uniezależnienie od ograniczeń geograficznych. Działania wymierzone w bezpieczeństwo jakiegokolwiek państwa można zainicjować z jego własnego terytorium oraz właściwie z każdego miejsca na świecie;
– niski koszt rozpoczęcia i prowadzenia zamierzonych działań – ograniczający się właściwie do nabycia sprzętu komputerowego, odpowiedniego oprogramowania i dostępu do sieci;
– relatywnie duża możliwość zachowania anonimowości przez podmiot dokonujący ataku lub innego szkodliwego działania.

Istotne znaczenie dla ochrony informacji niejawnych odgrywa także bezpieczeństwo elektromagnetyczne, ponieważ każde urządzenie elektroniczne (elektryczne) jest źródłem ubocznych emisji elektromagnetycznych, które mogą być skorelowane z przetwarzaną informacją. W kategorii urządzeń przeznaczonych

do przetwarzania informacji niejawnych mieszczą się zarówno złożone podsystemy (np. komputery, urządzenia zobrazowania na ekranie), jak i najprostsze urządzenia elektryczne (np. dalekopisy, maszyny do pisania).

Najłatwiejsze do odbioru, a w związku z tym najbardziej niebezpieczne z punktu widzenia ewentualnej infiltracji elektromagnetycznej, są urządzenia, w których zobrazowanie informacji lub przepływ danych następuje w sposób szeregowy, np.: monitory ekranowe (w tym również monitory z aktywną matrycą czy z ekranem LCD) czy drukarki laserowe.

Do urządzeń, które należy poddać bezwzględnej ochronie zaliczamy: komputery, monitory oraz inne urządzenia zobrazowania informacji, drukarki, skanery, plotery, urządzenia sieciowe (huby, routery), urządzenia transmisji danych (np. modem) i urządzenia kryptograficzne.

Ochrona systemów teleinformatycznych przetwarzających informacje niejawne

Na bezpieczeństwo trzeba spojrzeć z szerszej perspektywy, aby je zagwarantować należy systematycznie zarządzać najważniejszymi dla firmy informacjami, które obejmują ludzi, procesy i systemy informatyczne. Każdy z trzech wymienionych obszarów jest równie istotny dla bezpieczeństwa informacji. Wszędzie tam, gdzie przekazywana jest informacja pomiędzy zleceniodawcą a odbiorcą, coraz częściej pojawia się wymóg gwarancji bezpieczeństwa, tj.

– poufności, czyli ochronę przed ujawnieniem informacji nieuprawnionemu odbiorcy;
– dostępności, czyli gwarancji uprawnionego dostępu do informacji, zawsze, gdy jest to niezbędne;
– integralności, czyli ochrony przed zniekształceniem lub modyfikacją informacji przez osobę do tego nieuprawnioną.

Zapewnienie odpowiedniego poziomu bezpieczeństwa systemowi teleinformatycznemu jest zazwyczaj kosztownym przedsięwzięciem, ale koszty poniesione w tym celu zwykle zwracają się wielokrotnie podczas eksploatacji takiego systemu. Warunkiem tego jest przemyślane i kompleksowo ujęte planowanie systemu zabezpieczeń już w początkowej fazie jego projektowania. Planując bezpieczeństwo projektowanego systemu należy mieć na celu jego skuteczność, a więc uwzględnić fizyczne, techniczne, sprzętowo-programowe i organizacyjno-kadrowe metody ochrony. Należy więc podejść do tego problemu w sposób kompleksowy, a więc:

• zastosować zabezpieczenia uwzględniające elementy osobowe, techniczne, programowe lub organizacyjne wykorzystywane w procesach ochronnych do

działań, których celem jest zapewnienie odpowiedniego poziomu ochrony logicznej i fizycznej informacji oraz elementów systemu teleinformatycznego;

- ś zabezpieczenia powinny być zorganizowane tak, żeby zapewnić wykrycie naruszenia bezpieczeństwa i prób takich działań oraz skuteczną ochronę mimo przełamania części zabezpieczeń. Warunkami dodatkowymi do wymogu kompleksowości są spójność (rozumiana jako brak luk w systemie ochrony, które mogłyby utworzyć ścieżki penetracji bez przełamywania zabezpieczeń) oraz niesprzeczność (rozumiana jako brak kolizji między zastosowanymi zabezpieczeniami)[16].

Dostępne informacje pozwalają sądzić, że ochrona fizyczna jest najstarszym, ale ciągle pewnym sposobem ochrony zasobów informacyjnych. Stanowi pierwszą linię obrony przed zagrożeniami. Zgodnie z normą PN-ISO/IEC17799, jej celem jest zapobieganie nieuprawnionemu dostępowi, uszkodzeniom i ingerencji w pomieszczenia instytucji i jej informacje. Brak odpowiednich zabezpieczeń fizycznych może nieść za sobą katastrofalne skutki, począwszy od kradzieży sprzętu, komputerowych nośników informacji, przez awarię zasilania lub systemu klimatyzacji. Brak zasobów, ich uszkodzenie, czy też ich niedostępność, może zakłócić ciągłość jego funkcjonowania. Punktem wyjścia do zbudowania skutecznego systemu ochrony fizycznej zasobów informacyjnych jest przeprowadzenie analizy ryzyka[17]. Poziom ochrony zasobów informacyjnych zależy od poziomu ryzyka związanego z materializacją zagrożeń. Zakłada się, że skuteczny system ochrony fizycznej ma uniemożliwić dostęp osobom nieuprawnionym do elementów systemów i sieci teleinformatycznych[18].

Artykuł 45 ustawy o ochronie informacji niejawnych określa, iż w jednostkach organizacyjnych, w których są przetwarzane informacje niejawne, należy stosować środki bezpieczeństwa fizycznego adekwatne do poziomu zagrożeń. Ma to na celu ochronę informacji oraz uniemożliwienie do nich dostępu osobom nieuprawnionym. Informacje należy chronić w szczególności przed: działaniem obcych służb specjalnych, zamachem terrorystycznym lub sabotażem, kradzieżą lub zniszczeniem materiału, próbą wejścia osób nieuprawnionych do pomieszczeń, w których są przetwarzane informacje niejawne oraz nieuprawnionym dostępem do informacji o wyższej klauzuli tajności, niż wynikającym z posiadanych uprawnień.

Ochrona fizyczna systemu lub sieci teleinformatycznej polega na:

---

[16] K. Liderman, *Analiza ryzyka i ochrona…*, dz. cyt., s. 15.

[17] Analiza ryzyka powinna obejmować analizę wartości zasobów informatycznych, analizę zagrożeń, analizę podatności oraz analizę aktualnego zabezpieczenia zasobów informatycznych.

[18] A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem informacyjnym…*, dz. cyt., s. 63.

- umieszczeniu urządzeń systemu lub sieci teleinformatycznej w strefie ochronnej;
- zastosowaniu środków zapewniających ochronę fizyczną, w szczególności przed: nieuprawnionym dostępem, podglądem i podsłuchem.

Zabezpieczenia techniczne obejmują następujące punkty: kontrolę dostępu, ochronę przeciwpożarową, systemy zasilania gwarantowanego, klimatyzację i chłodzenie, zabezpieczenia proceduralne oraz ochronę przed emisją elektromagnetyczną[19].

Na sprzętowo-programową ochronę systemu składają się: odpowiednia ochrona dostępu na poziomie logicznym oraz odpowiedni poziom kryptograficznej ochrony tajności, a także integralności informacji. W jej obszarze znajdują się również: monitorowanie przepływu pakietów w sieci i działań użytkowników; zapewnienie odpowiedniego poziomu dostępności informacji przez redundancje sprzętowe i programowe, w tym odpowiednio zbudowane systemy zasilania gwarantowanego oraz zapewnienie właściwego niszczenia informacji zapisanej na komputerowych nośnikach i na wydrukach z systemu komputerowego[20]. Istotnym elementem jest również niezawodność transmisji, która polega na zapewnieniu integralności i dostępności informacji niejawnych przekazywanych w systemach i sieciach teleinformatycznych. Zapewnia się ją w szczególności poprzez zapewnienie zapasowych łączy telekomunikacyjnych.

Organizacyjno – kadrowa ochrona systemu obejmuje: właściwe udokumentowanie systemu ochrony informacji; klasyfikację informacji i przyznawanie praw dostępu do niej, a także właściwe przydzielenie zakresu odpowiedzialności za ochronę informacji. Ponadto do tego rodzaju ochrony zaliczamy: organizację nadzoru i kontroli w zakresie ochrony informacji; szkolenia i treningi z zakresu bezpieczeństwa oraz zasady reagowania na incydenty z zakresu bezpieczeństwa teleinformatycznego[21]. Bezpieczeństwo teleinformatyczne należy zapewnić poprzez ochronię informacji, które są przetwarzane w systemach i sieciach teleinformatycznych przed utratą właściwości gwarantujących to bezpieczeństwo, a zwłaszcza przed utratą poufności, dostępności i integralności. Bezpieczeństwo teleinformatyczne należy zagwarantować przed rozpoczęciem oraz w trakcie przetwarzania informacji niejawnych w systemie lub sieci teleinformatycznej. W tym celu odpowiednio wcześniej musi powstać dokumentacja określająca wymogi bezpieczeństwa, a systemowi musi zostać udzielona akredytacja.

---

[19] Tamże, s. 62.

[20] K. Liderman, *Analiza ryzyka i ochrona…*, dz. cyt., s. 14.

[21] Tamże.

Akredytacja bezpieczeństwa teleinformatycznego jest dopuszczeniem systemu teleinformatycznego do przetwarzania informacji niejawnych i ma na celu zapewnienie, że w systemie teleinformatycznym zostały wdrożone mechanizmy i procedury gwarantujące bezpieczne przetwarzanie informacji niejawnych o określonej klauzuli tajności. Ze względów formalnych proces akredytacji podzielony jest na: akredytację bezpieczeństwa systemów przetwarzających informacje niejawne o klauzuli „zastrzeżone"; akredytację bezpieczeństwa systemów przetwarzających informacje niejawne o klauzuli „poufne" i wyżej oraz akredytację bezpieczeństwa systemów przetwarzających informacje niejawne międzynarodowe. Obowiązkowi akredytacji nie podlegają systemy teleinformatyczne, które znajdują się bezpośrednio poza strefami ochronnymi oraz służą bezpośrednio do pozyskiwania i przekazywania w sposób niejawny informacji oraz utrwalania dowodów w trakcie realizacji czynności operacyjno-rozpoznawczych lub procesowych przez uprawnione do tego podmioty.

Dokumentacja bezpieczeństwa systemu teleinformatycznego

Obowiązujące przepisy nakładają konieczność opracowania dokumentacji zawierającej procedury i zasady konieczne do zabezpieczenia systemów teleinformatycznych. Należą do niej: dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego oraz dokument procedur bezpiecznej eksploatacji.

Dokumentację szczególnych wymagań bezpieczeństwa systemu teleinformatycznego opracowuje się na etapie projektowania systemu, po przeprowadzeniu wstępnego szacowania ryzyka dla bezpieczeństwa informacji niejawnych, które mają być przetwarzane w systemie teleinformatycznym z uwzględnieniem warunków charakterystycznych dla jednostki organizacyjnej, w której dane informacje mają być przetwarzane i samego systemu. W oparciu o wyniki analizy ryzyka dobiera się zabezpieczenia. Zastosowane zabezpieczenia powinny być efektywne kosztowo i uwzględniać wymagania wynikające z przepisów prawa, wymagania biznesowe i wymagania będące wynikiem analizy ryzyka.

W dokumentacji powinny znajdować się dane o systemie lub sieci teleinformatycznej obejmujące: rodzaje oraz klauzule tajności informacji niejawnych, które będą przetwarzane w systemie; grupę użytkowników systemu wyodrębnioną ze względu na posiadane uprawnienia do pracy w systemie; tryb pracy; przeznaczenie i funkcjonalność; wymagania eksploatacyjne dla wymiany informacji i połączeń z innymi systemami teleinformatycznymi. Ponadto, w dokumencie szczególnych wymagań bezpieczeństwa zawiera się informacje o metodyce użytej w procesie sza-

cowania ryzyka dla bezpieczeństwa informacji oraz raport z tego procesu, zastosowanych zabezpieczeniach, poświadczeniach bezpieczeństwa lub innych formalnych uprawnieniach do dostępu do informacji niejawnych; bezpieczeństwie fizycznym; ochronie elektromagnetycznej; stosowanych urządzeniach lub narzędziach kryptograficznych; ciągłości działania, ustawieniach konfiguracyjnych; dokonywaniu przeglądów diagnostycznych i napraw, zapobieganiu incydentom bezpieczeństwa teleinformatycznego, w tym ochronie przed oprogramowaniem złośliwym; zasadach wprowadzania poprawek lub uaktualnień oprogramowania; ochronie nośników; identyfikacji i uwierzytelnianiu użytkowników i urządzeń; kontroli dostępu; audycie wewnętrznym; zarządzaniu ryzykiem a także zmian w systemie, w tym dotyczących aktualizacji dokumentacji bezpieczeństwa systemu teleinformatycznego oraz warunkach ponownej akredytacji systemu i wycofania z eksploatacji[22].

Kolejnym wymaganym dokumentem jest dokument procedur bezpiecznej eksploatacji, który opracowuje się na etapie wdrażania systemu teleinformatycznego. Warunkiem jest wcześniejsze przeprowadzenie szacowania ryzyka dla bezpieczeństwa informacji niejawnych z uwzględnieniem wprowadzonych zabezpieczeń. Dokument ten uaktualnia się na etapie eksploatacji systemu. W dokumencie procedur bezpiecznej eksploatacji określa się szczegółowy wykaz procedur bezpieczeństwa wraz z dokładnym opisem sposobu ich wykonania, który obejmuje: administrowanie systemem oraz zastosowanymi środkami zabezpieczającymi; bezpieczeństwo urządzeń; bezpieczeństwo oprogramowania; zarządzanie konfiguracją sprzętowo-programową, plany awaryjne; monitorowanie i audyt systemu, zarządzanie nośnikami i materiałami kryptograficznymi; stosowanie ochrony elektromagnetycznej; reagowanie na incydenty bezpieczeństwa teleinformatycznego; szkolenia użytkowników oraz wprowadzania i wyprowadzania danych z systemu[23].

System reagowania na incydenty komputerowe w resorcie obrony narodowej

W resorcie obrony narodowej, w celu zapewnienia realizacji i koordynacji procesów zapobiegania, wykrywania i reagowania na incydenty komputerowe w systemach i sieciach teleinformatycznych, powołano System Reagowania na Incydenty Komputerowe (SRnIK). Jest to trzypoziomowa struktura, w skład której wchodzą:

1. Centrum Koordynacyjne, którego funkcję spełnia Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki.

[22] Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. *w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego*, Dz. U. Nr 159 poz. 948, § 25.

[23] Tamże, § 26.

2. Centrum Wsparcia Technicznego, którego funkcję spełnia Centrum Zarządzania Systemami Teleinformatycznymi.
3. Administratorzy systemów i sieci teleinformatycznych w jednostkach i komórkach organizacyjnych.

Nadzór nad funkcjonowaniem Systemu Reagowania na Incydenty Komputerowe (SRnIK) sprawuje Dyrektor Departamentu Informatyki i Telekomunikacji Ministerstwa Obrony Narodowej, który m.in. przeprowadza przeglądy SRnIK oraz podejmuje działania stosowne do wyników tych przeglądów, pełni rolę punktu kontaktowego SRnIK w stosunku do organizacji narodowych i międzynarodowych, organizuje resortowe systemy i sieci teleinformatyczne z uwzględnieniem procesów realizowanych w ramach SRnIK, tworzy politykę wykorzystania systemów i sieci teleinformatycznych resortu obrony narodowej, organizuje szkolenia z zakresu reagowania na incydenty komputerowe, a także zatwierdza „Podręcznik reagowania na incydenty komputerowe w resorcie obrony narodowej" oraz „Standardowe Procedury Operacyjne SRnIK w resorcie obrony narodowej"[24]. Powołano także Zespół do prowadzenia cyklicznych analiz zagrożeń dla przetwarzania w systemach i sieciach teleinformatycznych, w tym m.in. określenia przyczyn wystąpienia incydentów komputerowych oraz sposobów postępowania zapobiegających występowaniu ich w przyszłości.

W skład Systemu Reagowania na Incydenty Komputerowe wchodzi Centrum Koordynacyjne, którego funkcję spełnia Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki. Do najważniejszych zadań Centrum można zaliczyć: koordynowanie procesu reagowania na incydenty komputerowe w systemach i sieciach teleinformatycznych; określanie zasad funkcjonowania SRnIK; prowadzenia działań pro aktywnych, polegających na analizie infrastruktury teleinformatycznej i opracowaniu zaleceń zapobiegających wystąpieniu incydentów[25].

Kolejny elementem SRnIK jest Centrum Wsparcia Technicznego, które jest uprawnione i właściwe do m.in.: monitorowania w trybie ciągłym stanu bezpieczeństwa systemów i sieci teleinformatycznych; zbierania informacji o zdarzeniach oraz tworzenia na ich bazie raportów o stanie bezpieczeństwa w nadzorowanych systemach i sieciach teleinformatycznych; prowadzenia, w porozumieniu z właściwymi pionami ochrony, kontroli konfiguracji systemów i sieci teleinformatycznych

[24] Decyzja nr 357/MON Ministra Obrony Narodowej z dnia 29 lipca 2008 r. *w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej*, § 3.

[25] Tamże, § 4.

z wykorzystaniem środków technicznych, w celu ustalenia aktualnego stanu zabezpieczenia tych systemów i sieci[26].

Do najważniejszych zadań administratorów systemów i sieci teleinformatycznych w jednostkach i komórkach organizacyjnych należy m.in.: przestrzeganie obowiązujących dokumentów normatywnych i zaleceń w zakresie przeciwdziałania naruszeniom bezpieczeństwa systemów i sieci teleinformatycznych; nadzorowanie użytkowników administrowanych przez nich systemów i sieci teleinformatycznych w zakresie przestrzegania ustalonych procedur bezpieczeństwa[27].

Istotny wpływ na jakość i efektywność pracy elementów wchodzących w skład SRnIK jest fakt szeroko zakrojonej współpracy następującymi instytucjami: Agencją Bezpieczeństwa Wewnętrznego (Rządowym Zespołem do spraw Reagowania na Incydenty Komputerowe); Służbą Kontrwywiadu Wojskowego; Departamentem Ochrony Informacji Niejawnych Ministerstwa Obrony Narodowej, Żandarmerią Wojskową; Zarządem Planowania Systemów Dowodzenia i Łączności P6 Sztabu Generalnego Wojska Polskiego, Centrum Koordynacyjnym systemu reagowania na incydenty komputerowe w Organizacji Traktatu Północnoatlantyckiego; krajowymi i międzynarodowymi organami koordynującymi systemy reagowania na incydenty komputerowe i pionami ochrony właściwych jednostek organizacyjnych.

*****

Znaczenie teleinformatycznej infrastruktury krytycznej we współczesnym świecie jest tak wielkie, że stała się ona bardzo ważnym elementem funkcjonalnym nie tylko sił zbrojnych, ale i całego państwa. Można być niemalże pewnym, że w przyszłości nowoczesne armie będą coraz częściej wykorzystywać cyberprzestrzeń do prowadzenia działań mających na celu unieszkodliwienie infrastruktury krytycznej innych państw. Dlatego konieczne jest konsekwentne i rygorystyczne przestrzeganie polityki bezpieczeństwa teleinformatycznego.

W Strategii bezpieczeństwa narodowego znajduje się zapis mówiący o tym, *że należy tworzyć i rozwijać długofalowe plany ochrony kluczowych systemów teleinformatycznych przed uzyskiwaniem dostępu do danych przez podmioty do tego niepowołane, zakłócaniem normalnego ich funkcjonowania, kradzieżą tożsamości i sabotażem. Trzeba stale oceniać możliwości wtargnięcia do systemów teleinformatycznych, przygotować możliwe formy odpowiedzi na ataki oraz rozwijać metody ewaluacji poniesionych strat informacyjnych. Priorytetem państwa będzie wspieranie narodowych programów i technologii informacyjnych*[28].

[26] Tamże, § 5.

[27] Tamże, § 6.

[28] *Strategia…*, dz. cyt., pkt. 79, s. 20.

Pomimo, wydawałoby się, kompleksowego ujęcia systemu bezpieczeństwa, siły zbrojne nie uchronią się przed próbami włamania lub przypadkami wprowadzania wirusa do systemów teleinformatycznych. Dlatego też należy stale monitorować potencjalne zagrożenia, przewidywać kolejne, a wraz z rozwojem technologicznym, dążyć do ciągłego doskonalenia zabezpieczeń zarówno systemów i sieci teleinformatycznych, jak i informacji w nich przetwarzanych. Szczególnie uwagę należy zwrócić na ochronę informacji niejawnych, ponieważ ich ujawnienie może spowodować zagrożenie dla Rzeczypospolitej i jej obywateli. Nie należy szczędzić też środków finansowych na ten cel, ponieważ straty związane z ujawnieniem informacji niejawnych mogą okazać się znacznie większe i nie dadzą przeliczyć się na żadne pieniądze.

Bibliografia

Bezpieczeństwo Narodowe Polski w XXI wieku, (red. nauk.) R. Jakubczak, J. Flis, Warszawa 2006.

Bezpieczeństwo teleinformatyczne państwa, (red. nauk.) M. Madej, M. Terlikowski, Warszawa 2009.

Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, AON Warszawa 2011.

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2008.

Nowak A., Scheffs W., *Zarządzanie bezpieczeństwem informacji*, Warszawa 2010.

Sienkiewicz P., *Szanse i zagrożenia rozwojowe w warunkach społeczeństwa informacyjnego*, Warszawa 2001.

Transsektorowe obszary bezpieczeństwa narodowego, (red. nauk.) K. Liedel, Warszawa 2011.

Wisz A., *Bezpieczeństwo informacji w wojskowych sieciach teleinformatycznych* – www.bbn.gov.pl\download\1\1002\bezpieczenstwoinformacji.pdf

Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym*, (Dz. U. z 2007 r., nr 89, poz. 590).

Ustawa z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych*, (Dz.U. z 2010 r., nr 182, poz. 1228).

Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. *w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego*.

Decyzja Nr 357/MON Ministra Obrony Narodowej z dnia 29 lipca 2008 r. *w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej*.

Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej, Warszawa 2007.

Rządowy program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016.

Sprawozdanie przewodniczącego Zespołu ds. Krytycznej Infrastruktury Teleinformatycznej, 28 kwietnia 2005 r.

*****

SECURITY OF CLASSIFIED INFORMATION SYSTEMS AND INFORMATION NETWORKS TECHNOLOGY IN THE DEPARTMENT OF NATIONAL DEFENCE

Keywords: national security, information security, cyberspace, critical infrastructure, protection of classified information, the armed forces

SUMMARY

In the twenty-first century, in which the rank of information security dimension has increased considerably, and the information became a commodity desired, even strategic, its acquisition and appropriate use can contribute to the success of the organization. Of particular importance are the classified information whose unauthorized disclosure could be a threat to the security of the state and its citizens.

The article highlights the key threats to IT systems of the Polish Armed Forces processing classified information. Structure and tasks of the elements of the Computer Emergency Response in the Ministry of National Defense have also been discussed.