



CHŁODNYM OKIEM

BIULETYN PRO MILITO
BEZPIECZEŃSTWO
OBRONNOŚĆ
WYDARZENIA
i OPINIE

Stowarzyszenie Pro Milito

Nr 3, czerwiec 2009 r.

Poważna i merytoryczna dyskusja na temat bezpieczeństwa narodowego jest jednym z celów Stowarzyszenia Pro Milito.

W bieżącym numerze przedstawiamy interesującą opinię na temat bezpieczeństwa informacyjnego, a także wnioski i postulaty wysuwane przez autora. Opinie i oceny zawarte w tym artykule nie są tożsame ze stanowiskiem Redakcji „Chłodnym okiem”, a jedynie wyrażają osobiste poglądy autora.

Redakcja



Bezpieczeństwo informacyjne

Stanisław Kowlopsi

W prezencie z okazji
XX Rocznic III Rzeczypospolitej Polskiej

Dwudziesta Rocznic suwerennej i demokratycznej Rzeczypospolitej Polskiej jest okazją do świętowania. Jest również okazją do analizowania naszych osiągnięć i potknięć oraz wyciągania konstruktywnych wniosków na przyszłość. Polska jest państwem o znaczącym potencjale demograficznym, ekonomicznym, politycznym i wojskowym, działającym w złożonym środowisku międzynarodowym. Jest członkiem Sojuszu Północnoatlantyckiego (NATO) i Unii Europejskiej (EU) i jako państwo graniczne zajmuje ważne miejsce w europejskim

systemie bezpieczeństwa, a terytorium Polski ma istotne znaczenie strategiczne. Dlatego tak ważnym obszarem działalności naszego kraju jest bezpieczeństwo narodowe oraz nasz wkład w bezpieczeństwo międzynarodowe, które zostały zdefiniowane w dokumencie: „Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej”, podpisanym 13 listopada 2007 roku przez Prezydenta RP. Jednym z najważniejszych wyzwań XXI wieku jest zapewnienie właściwego bezpieczeństwa informacyjnego (ang. Information Assurance), które jest nierozdzielnie związane z bezpieczeństwem społeczeństwa i państwa. Praktyczna realizacja zadań w obszarze bezpieczeństwa informacyjnego, zdefiniowanych w strategii bezpieczeństwa narodowego, zależy od jakości obowiązującego prawa. Polska, stając się w 1999 roku członkiem NATO oraz w 2004 roku członkiem Unii Europejskiej, zobowiązała się do przestrzegania prawa obowiązującego w NATO i EU oraz dopasowania narodowego

prawa do prawa NATO i EU, w tym prawa obowiązującego w obszarze ochrony informacji i bezpieczeństwa teleinformatycznego, jak również ochrony kryptograficznej.

W tej sytuacji uzasadnione jest uzyskanie odpowiedzi na trzy podstawowe pytania:

1. Jaki jest stan narodowego prawa dotyczącego ochrony informacji i bezpieczeństwa teleinformatycznego obowiązującego w naszym kraju?
2. Jaki jest stan dopasowania narodowego prawa do prawa NATO i EU w obszarze ochrony informacji i bezpieczeństwa teleinformatycznego?
3. Co należy jeszcze zrobić w obszarze bezpieczeństwa informacyjnego (ochrony informacji i bezpieczeństwa teleinformatycznego)?

Odpowiedź na te pytania nie wydaje się być skomplikowana, choć wymaga wiedzy i doświadczenia w tej ważnej dziedzinie oraz przeprowadzenia stosownej analizy.

Wspomnienia, czyli trochę historii

Wraz z zakończeniem II wojny światowej rozpoczął się nowy okres w rozwoju ochrony informacji. Niewątpliwie dużą rolę w tym procesie odegrał rozwój kryptologii (kryptografii i kryptoanalizy), w której coraz częściej zaczęto wykorzystywać wiedzę matematyczną i osiągnięcia technologiczne. Niestety sytuacja polityczna i uzależnienie Polski od ZSRR znacznie ograniczyły rozwój narodowej kryptologii oraz uniemożliwiły wykorzystywanie osiągnięć polskich kryptoanalityków, autorów sukcesu złamania w 1932 roku niemieckiego szyfru ENIGMA – osiągnięć polskich matematyków, inżynierów i wojskowych, pracowników Oddziału II Sztabu Głównego WP. Wraz z upływem

lat i zachodzącymi zmianami politycznymi, a szczególnie w związku z pojawieniem się nowych wyzwań w obszarze bezpieczeństwa narodowego, stopniowo w naszym kraju zaczął postępować rozwój narodowej kryptologii, zarówno w strukturach cywilnych, jak i wojskowych.

Powstałe w 1952 r. Biuro Szyfrów MSW (także funkcjonujące pod nazwą Biuro „A” MSW), posiadało pełen monopol w państwie na prowadzenie wszelkich prac związanych z ochroną informacji a przede wszystkim z kryptologią. Funkcjonariusze Biura Szyfrów MSW byli między innymi konstruktorami pierwszego w pełni polskiego elektronicznego urządzenia szyfrującego o kryptonimie „DUDEK” (Dalekopisowe Urządzenie Do Elektronicznego Kodowania), które w latach 70 i początku lat 80 ubiegłego wieku było produkowane przez Zakłady Teletechniczne TELKOM TELETRA w Poznaniu i było wykorzystywane nie tylko w naszym kraju, przynosząc uznanie polskim projektantom. Równolegle w resorcie obrony narodowej funkcjonowała komórka szyfrów, która zabezpieczała eksploatację systemów szyfrowych i kodowych w wojsku, głównie Układu Warszawskiego. W latach siedemdziesiątych ubiegłego wieku w wojsku zintensyfikowano prace w obszarze narodowej kryptografii i kryptoanalizy. W 1975 roku w Zarządzie II SG WP została utworzona wojskowa komórka kryptoanalizy. Zaczęto konstruować narodowe urządzenia kryptograficzne oraz narzędzia i urządzenia do skutecznego prowadzenia kryptoanalizy.

Wraz ze zmianami w Polsce, rozpoczętymi w dniu 4 czerwca 1989 roku, nastąpiły zmiany organizacyjne i strukturalne

oraz dalszy rozwój narodowej kryptologii. Powstałe w 1990 roku Biuro Szyfrów UOP było pierwszą jednostką organizacyjną w III RP, zajmującą się szeroko rozumianą łącznością szyfrową i kodową, organizowaną na potrzeby organów państwowych. Prace realizowane przez funkcjonariuszy tej komórki umożliwiły w krótkim czasie rozwój narodowej kryptografii. Było to możliwe dzięki przejęciu potencjału byłego Biura Szyfrów MSW i pozytywnej weryfikacji w 1990 roku poważnej części jego kadr. W powstałych w 1991 roku Wojskowych Służbach Informacyjnych została powołana komórka kryptoanalizy, która przejęła istniejący w wojsku potencjał intelektualny i techniczny w tej dziedzinie. W 1996 roku Biuro Szyfrów UOP zostało przekształcone w Biuro Bezpieczeństwa Łączności i Informatyki UOP, a po powstaniu Agencji Bezpieczeństwa Wewnętrznego (ABW), w jej strukturach został utworzony Departament Bezpieczeństwa Teleinformatycznego (DBTI). Wraz z politycznymi i gospodarczymi zmianami w Polsce, nastąpiły zmiany w prawie dotyczącym ochrony informacji. Obowiązująca od 14 grudnia 1982 roku ustawa o ochronie tajemnicy państwowej i służbowej (Dz. U. 1982, Nr 40, poz. 271), była sukcesywnie zmieniana w latach: 1989, 1990, 1996, i 1997. Jednak fundamentalna zmiana w obszarze ochrony informacji i bezpieczeństwa teleinformatycznego nastąpiła dopiero w związku z przygotowaniem Polski do wejścia do NATO. W życie weszła ustawa o ochronie informacji niejawnych z 22 stycznia 1999 roku. Zadaniem ustawy było zapewnienie ochrony narodowym informacjom niejawnym i bezpieczeństwa narodowym systemom i sieciom teleinformatycznym oraz dopasowanie polskiego prawa do wymagań prawa obowiązującego w tym obszarze w NATO.

Ustawa powołała do życia dwie służby ochrony państwa (SOP) sfery cywilnej (ABW) i wojskowej (WSI, obecnie SKW), odpowiedzialnych za całokształt bezpieczeństwa informacyjnego w Polsce, w tym ochrony kryptograficznej. Służby te stały się również krajowymi władzami bezpieczeństwa sfery cywilnej i wojskowej w relacjach międzynarodowych.

Wejście Polski do NATO oraz rozwój nowoczesnych technologii teleinformatycznych wymusiły przeprowadzenie kompleksowych zmian prawnych w obszarze bezpieczeństwa informacyjnego naszego kraju.

W dotychczasowym rozwoju ochrony informacji i bezpieczeństwa systemów i sieci służących do jej wytwarzania, przetwarzania, przesyłania i gromadzenia można wyróżnić cztery zasadnicze okresy: ochrona informacji i bezpieczeństwo naturalnych systemów komunikowania, ochrona informacji i bezpieczeństwo systemów łączności (ang. Communications Security – COMSEC), ochrona informacji i bezpieczeństwo systemów teleinformatycznych (ang. Information Systems Security – INFOSEC oraz najnowszy okres, w który wchodzi: bezpieczeństwo informacyjne (ang. Information Assurance – IA) – kompleksowe bezpieczeństwo rozległych i różnorodnych systemów informacyjnych zapewniające właściwą ochronę informacji. Bezpieczeństwo informacyjne jest definiowane jako zbiór wszelkich środków przeznaczonych do ochrony systemów informacyjnych, w celu zapewnienia informacji: poufności (ang. confidentiality), dostępności (availability), autentyczności (authentication), integralności (integrity) i niezaprzeczalności (non-repudiation) nadania.

Z przykrością należy stwierdzić, że autorzy powstałych aktów prawnych, mimo wykonania tytanicznej pracy, nie uniknęli wielu błędów, które do dnia dzisiejszego odciskają swoje piętno na bezpieczeństwie informacyjnym naszego kraju. Błędy te wynikają z niezrozumienia zasad ochrony informacji i bezpieczeństwa teleinformatycznego oraz prawa obowiązującego w NATO, jak również braku wiedzy oraz nieposiadania doświadczenia w obszarze bezpieczeństwa informacyjnego, a szczególnie w dziedzinie ochrony kryptograficznej.

Język porozumiewania się, czyli podstawowe definicje i pojęcia

Chcąc rozmawiać o ochronie informacji i bezpieczeństwie teleinformatycznym, a dziś już o bezpieczeństwie informacyjnym (ang. Information Assurance), należy posługiwać się wspólnym językiem, czyli zdefiniować podstawowe terminy i wyjaśnić podstawowe pojęcia.

W polskim prawie, ustawie o ochronie informacji niejawnych, znalazły się jedynie tylko niektóre pojęcia (art. 2), jak: tajemnica państwowa, tajemnica służbowa, służba ochrony państwa, dokument, materiał, system teleinformatyczny, sieć teleinformatyczna, akredytacja bezpieczeństwa teleinformatycznego, dokumentacja bezpieczeństwa systemu lub sieci informatycznej. Niestety zabrakło takich pojęć, jak: krajowa władza bezpieczeństwa (ang. National Security Authority), system ochrony kryptograficznej, urządzenie i narzędzie kryptograficzne, materiał kryptograficzny, certyfikacja urządzeń kryptograficznych, certyfikat ochrony kryptograficznej, dystrybucja materiałów kryptograficznych, główna kancelaria kryptograficzna, krajowy organ

dystrybucji materiałów kryptograficznych (ang. National Distribution Authority), główna kancelaria zagraniczna, itp., pomimo, że część z nich jest używana w treści ustawy oraz występują one w dokumentach NATO.

Analiza obowiązującego prawa, czyli jego wady

Większość istotnych definicji i pojęć dotyczących bezpieczeństwa informacyjnego nie znajduje się w obowiązującym prawie. Ponadto, w polskim prawie nie mówi się nic o krytycznej infrastrukturze teleinformatycznej. Nie mówi się również o informacji jawnej, zwłaszcza jawnej wrażliwej oraz ochronie takiej informacji, a także nie rozróżnia się informacji narodowej i informacji sojuszniczej (nienarodowej) oraz charakteru systemów i sieci teleinformatycznych. Ustawa o ochronie informacji niejawnych (Dz. U. 1999, Nr 11, poz. 95 z późniejszymi zmianami) mówi o informacji (materiałach), skupia się jedynie na jej poufności i wprowadza pojęcie klauzul informacji oraz przypisuje im oznaczenia.

Klauzula materiałów

Klasyfikowanie informacji niejawnej oznacza przyznanie informacji (materiałowi) w sposób wyraźny jednej z klauzul tajności. Informacje niejawne zaklasyfikowane jako stanowiące tajemnicę państwową oznaczają się klauzulą „Ścisłe Tajne” lub „Tajne”, natomiast informacje niejawne uznane za stanowiące tajemnicę służbową oznaczają się klauzulą „Poufne” lub „Zastrzeżone” (art. 23 ustawy). Materiały otrzymywane z zagranicy oraz wysyłane za granicę w celu wykonania umów międzynarodowych oznaczają się odpowiednią do treści materiałów klauzulą tajności, określoną w ustawie oraz jej zagranicznym odpowiedniku (art. 24 ustawy).

Oznaczanie materiałów

Oznaczanie materiału niejawnego klauzulą

tajności polega na umieszczeniu na nim odpowiedniej klauzuli tajności. Klauzulę tajności należy nanieść w sposób wyraźny i w pełnym brzmieniu. Wprowadzono następujące skróty w oznaczaniu klauzul tajności: „00” – dla klauzuli „Ściśle Tajne”, „0” – dla klauzuli „Tajne”, „Pf” – dla klauzuli „Poufne” oraz „Z” – dla klauzuli „Zastrzeżone”. Szczegóły są zawarte w rozporządzeniu Prezesa Rady Ministrów z 5 października 2005 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności (Dz. U. 2005, Nr 205, poz. 1696). Polski system oznaczania materiałów w porównaniu z systemem obowiązującym w NATO wypada niekorzystnie. Obowiązujące w Polsce rozporządzenie w sprawie oznaczania materiałów i umieszczania na nich klauzul tajności nie wyjaśnia wielu wątpliwości, głównie gdy chodzi o oznaczanie informacji elektronicznych. W polskim systemie nie wprowadzono pojęcia kategorii informacji i nie określono sposobów jej oznaczania, zaś informacje elektroniczne potraktowano powierzchownie, ograniczając się jedynie do oznaczania elektronicznych i papierowych nośników informacji. Należy podkreślić, że system klasyfikowania i oznaczania informacji w NATO jest bardziej profesjonalny niż nasz system i dlatego wymiana informacji zarówno w formie papierowej, jak i elektronicznej, stanowi często problemem we współpracy z NATO. Porównanie obu systemów przedstawia tabela 1.

TECHNOLOGIA ELEKTRONICZNA

NATO tworzy system oznaczania informacji elektronicznych (Labeling of NATO information), w Polsce takie próby praktycznie nie zostały jeszcze podjęte.

Brak wyszczególnienia informacji jawnej wrażliwej (tzw. „do użytku służbowego”), która w odróżnieniu od informacji publicznej jest także chroniona przez instytucje państwowe i prywatne, świadczy o niezrozumieniu problematyki przez polskiego ustawodawcę. W NATO taki materiał ma oznaczenie NATO UNCLASSIFIED (NU). W efekcie takiego stanu rzeczy pojawiają się i zapewne coraz częściej będą pojawiać się komplikacje z tego typu informacjami w czasie dalszej współpracy międzynarodowej.

Przechowywanie materiałów

Narodowe materiały niejawne są przechowywane w kancelarii tajnej (ustawa o ochronie informacji niejawnych, rozporządzenie RM i zarządzenia właściwych ministrów). Materiały niejawne wymieniane na podstawie umów międzynarodowych zawartych przez Polskę z państwami i organizacjami międzynarodowymi (sojusznicze materiały niejawne) są przechowywane w Głównej Kancelarii Zagranicznej, kancelariach tajnych zagranicznych lub w punktach obsługi dokumentów zagranicznych, tj. wydzielonej części kancelarii tajnej. Umowy sojusznicze

Tabela 1.

<p>TECHNOLOGIA PAPIEROWA <i>Jednowymiarowa struktura w Polsce</i></p> <p><i>Informacja niejawna:</i> „Ściśle Tajne” „Tajne” „Poufne” „Zastrzeżone”</p> <p><i>Informacja jawna:</i> _____</p>	<p><i>Trójwymiarowa struktura w NATO (Marking of NATO information)</i></p> <p><i>Classified Information:</i> „Cosmic Top Secret” „Atomal” „NATO Secret” „Crypto” „NATO Confidential” „Logistics” „NATO Restricted” „Releasable to ...” <Policy Identifier> <Classification> <Category></p> <p><i>Non-Classified Information:</i> „NATO Unclassified”</p>
--	--

zobowiązują stronę polską do przechowywania pewnych kategorii materiałów, np. materiałów o tematyce nuklearnej lub kryptograficznej, w szczególnie chronionych miejscach – kancelariach ATOMAL i kancelariach kryptograficznych. Polski ustawodawca nie uregulował tych kwestii w ustawie i rozporządzeniach RM, dlatego zarówno w sferze cywilnej, jak i wojskowej są stosowane różne rozwiązania tego zagadnienia.

Nowoczesne podejście do informacji

Mówiąc o informacji i zarządzaniu nią, należy mieć świadomość wielowymiarowości tych zagadnień. Jako podstawowe cechy informacji należy wymienić ich rodzaj, poufność, dostępność i integralność, zaś zarządzanie informacją należy rozpatrywać przez pryzmat technologii wytwarzania informacji (w formie papierowej i elektronicznej), przetwarzania, gromadzenia i przesyłania oraz w powiązaniu z potrzebą jej chronienia. Aby zbudować profesjonalny i bezpieczny system informacyjny państwa, który jest wspierany zaawansowanymi technologiami informacyjnymi, należy stworzyć właściwy system klasyfikowania informacji i jej oznaczania. Nowoczesny system oznaczania informacji (materiałów) powinien być spójny i logiczny, zawierać wszystkie niezbędne dane dotyczące informacji i jej bezpieczeństwa oraz obejmować informacje wytworzone zarówno w formie papierowej, jak i elektronicznej. System oznaczania informacji powinien być wielowymiarowy, a nie jednowymiarowy, jaki aktualnie obowiązuje w naszym kraju, ograniczając się jedynie do poufności informacji. Nowoczesny system klasyfikowania i oznaczania informacji powinien obejmować przynajmniej trzy cechy informacji: kategorię, poufność i dostępność.

Kategoria informacji. Można wyróżnić wiele kategorii informacji. Sposób podziału informacji na kategorie oraz liczba kategorii zależą od

różnych czynników, głównie od czynnika ludzkiego, który dokonuje takiego podziału oraz od potrzeb tematycznych i technologii wytwarzania informacji. Z tego względu trudno dokonać jednoznacznego podziału zbioru informacji na kategorie, które przykładowo mogą wyglądać następująco:

- Kategoria informacji osobowych.
- Kategoria informacji kryptograficznych.
- Kategoria informacji nuklearnych.
- Kategoria informacji logistycznych.
- Kategoria informacji finansowych.
- Kategoria pozostałych informacji.

Poufność informacji. Podział zbioru informacji według tego kryterium wyróżnia dwa typy informacji – niejawne (ang. Classified) i jawne (ang. Non-Classified). W ramach każdego typu można wydzielić różne podtypy uwzględniające poziom wymaganej ochrony informacji. Każdemu podtypowi informacji można jednoznacznie przypisać klauzulę poufności, np. informacjom niejawnym: „Ścisłe Tajne”, „Tajne”, „Poufne” i „Zastrzeżone” a informacjom jawnym: „Wrażliwe” i „Publiczne”.

Dostępność informacji. Ze względu na udostępnianie informacji, zbiór informacji można podzielić na podzbiór informacji narodowych i podzbiór informacji sojuszniczych (nienarodowych). Informacja narodowa to informacja, która nie może być udostępniona innemu państwu (nawet sojusznikowi), gdyż udostępnienie jej zagraża bezpieczeństwu lub interesowi naszego kraju. Informacja sojusznicza to informacja, która została udostępniona lub może być udostępniona innemu państwu (sojusznikowi), gdyż jest to w interesie naszego kraju. Jak widać, decyzja o udostępnieniu informacji innemu państwu jest decyzją polityczną i dlatego powinna być ona podejmowana z uwzględnieniem przede wszystkim bezpieczeństwa i interesu naszego kraju oraz zgodnie z zawartymi umowami i porozumieniami międzynarodowymi (sojuszniczymi). W praktyce

wymiana informacji jest bardziej skomplikowana, gdyż nasz kraj należy do wielu międzynarodowych organizacji oraz współpracuje z wieloma państwami i organizacjami. W interesie każdego wolnego i niezależnego państwa jest właściwe chronienie informacji narodowych, także przed dostępem sojuszników. Zatem koniecznością jest stosowanie i rozwijanie narodowej kryptografii oraz budowanie narodowych urzędów i systemów ochrony kryptograficznej.

Powyższa analiza obowiązującego w naszym kraju prawa dotyczącego ochrony informacji i bezpieczeństwa teleinformatycznego, w tym głównie ochrony kryptograficznej pokazuje szereg jego wad. Do najważniejszych z nich należy zaliczyć następujące:

- Jednowymiarowe podejście do klasyfikowania oraz oznaczania informacji w postaci papierowej i elektronicznej – brak wyróżnienia kategorii informacji.
- Brak definicji informacji narodowych i informacji sojuszniczych (nienarodowych) oraz powierzchowne podejście do wymiany informacji z innymi państwami (sojusznikami).
- Brak wyróżnienia informacji (materiałów) kryptograficznych i ich oznakowania.
- Brak definicji kategorii informacji jawnych, w tym wyróżnienia informacji jawnych wrażliwych oraz wymogu oznaczania takich informacji (materiałów).
- Brak w poświadczeniach bezpieczeństwa wskaźnika określającego, z jakich kategorii informacji może korzystać posiadacz uzyskanego poświadczenia.
- Brak uwarunkowań prawnych narodowego systemu dystrybucji materiałów kryptograficznych – jednoznacznego określenia instytucji, które mogą przewozić

materiały kryptograficzne, prowadzić wymianę materiałów kryptograficznych z państwami sojuszniczymi (ang. National Distribution Authority – NDA) oraz przechowywać i ewidencjonować materiały kryptograficzne (główna i inne kancelarie kryptograficzne).

- Brak dokumentu dla osoby upoważnionej do przewożenia materiałów kryptograficznych.
- Brak unormowań określających, kto i w jakich okolicznościach może kontrolować przewożących materiały kryptograficzne.
- Brak zasad oraz określenia instytucji odpowiedzialnych za tworzenie i implementację narodowych algorytmów kryptograficznych oraz projektowanie i produkcję narodowych urzędów i systemów ochrony kryptograficznej.

Jednak najważniejszą wadą polskiego prawa jest fakt, że zapisy ustawy nie precyzują zasad w obszarze konstruowania i produkcji narodowych urzędów i narzędzi ochrony kryptograficznej, w tym tworzenia narodowych algorytmów kryptograficznych i ich implementacji. Ustawa o ochronie informacji niejawnych oraz rozporządzenia jednoznacznie określają zasady ochrony informacji niejawnych oraz bezpieczeństwa teleinformatycznego, jak warunki bezpieczeństwa dla niejawnych systemów i sieci teleinformatycznych, ich akredytację lub certyfikację oraz certyfikację wyrobów kryptograficznych. Niestety nasze prawo, w tym głównie ustawa, nic nie mówi o tym, kto i na jakich zasadach może projektować i produkować narodowe urządzenia i systemy ochrony kryptograficznej oraz

tworzyć i implementować narodowe algorytmy kryptograficzne. Z istoty bezpieczeństwa systemów i sieci teleinformatycznych wynika, iż urządzenia i narzędzia ochrony kryptograficznej muszą być projektowane i produkowane w szczególnych warunkach bezpieczeństwa. Ustawa dopuszcza, że każdy, kto spełnia jej wymagania ma prawo konstruować urządzenia i narzędzia kryptograficzne, w tym algorytmy kryptograficzne, do wszystkich klauzul tajności informacji niejawnych. Zaś o dopuszczeniu do stosowania wyrobów ochrony kryptograficznej decydują służby ochrony państwa, stosownie do ustawowych kompetencji. Taki stan rzeczy pozostaje w sprzeczności z logiką oraz ogólnie znanymi i stosowanymi zasadami, w tym w NATO i czołowych państwach członkach NATO. Równocześnie należy zwrócić uwagę, że polskie prawo daje możliwość stosowania sojuszniczych certyfikowanych urządzeń kryptograficznych w narodowych systemach i sieciach teleinformatycznych. Jednakże stosowanie takich urządzeń nie jest praktycznie możliwe bez przeprowadzenia ich badań i wydania im polskiego certyfikatu, w przypadku, gdy będą one zastosowane w systemach i sieciach teleinformatycznych do ochrony narodowych informacji niejawnych oklazu „Poufne” i wyższej.

Wnioski, czyli co niezwłocznie należy poprawić?

Przedstawiona powyżej analiza obowiązującego prawa w naszym kraju pokazuje jedynie jego podstawowe wady dotyczące ochrony informacji i bezpieczeństwa teleinformatycznego. Poniższe wnioski są zaś jedynie nieśmiałą propozycją rozwiązań, mających na celu wywołać konstruktywną dyskusję na

ten temat, aby jak najszybciej doprowadzić do wyeliminowania istniejących wad w naszym prawie oraz usprawnić funkcjonujący system w obszarze bezpieczeństwa informacyjnego.

Do priorytetowych zadań należy zaliczyć:

- **POPRAWĘ OBOWIĄZUJĄCEGO PRAWA:**
 - W obszarze klasyfikacji i oznakowania informacji (materiałów), w tym kryptograficznych oraz dostosowanie prawa do wymagań sojuszniczych, w tym uregulowanie zasad udostępniania materiałów niejawnych sojusznikom – definicja informacji narodowych i informacji sojuszniczych.
 - Ujęcie w ramy prawne zasad przechowywania i udostępniania materiałów kryptograficznych (kancelarie kryptograficzne i poświadczenia bezpieczeństwa).
 - Ujęcie w ramy prawne budowy nowoczesnego systemu dystrybucji materiałów kryptograficznych oraz służby kurierskiej.
 - Ujęcie w ramy prawne zasad tworzenia i implementacji narodowych algorytmów kryptograficznych.
 - Ujęcie w ramy prawne stworzenia profesjonalnego narodowego systemu projektowania i produkcji narodowych urządzeń i systemów ochrony kryptograficznej oraz zasad stosowania nienarodowych urządzeń kryptograficznych w narodowych systemach i sieciach teleinformatycznych.
 - Ujęcie w ramy prawne procesu certyfikacji narodowych wyrobów kryptograficznych.

- **UTWORZENIE NARODOWEJ GRUPY FIRM W OBSZARZE KRYPTOGRAFII:**

- Objęcie „państwowym mecenatem” narodowych firm w obszarach: tworzenia narodowych algorytmów kryptograficznych i ich implementacji oraz projektowania i produkcji narodowych urządzeń i systemów ochrony kryptograficznej.

- **ROZWÓJ NARODOWYCH SYSTEMÓW I SIECI TELEINFORMATYCZNYCH:**

- Usprawnienie systemu edukacji społeczeństwa w obszarze bezpieczeństwa informacyjnego.

- Usprawnienie systemu projektowania, wdrażanie i eksploatacji narodowych systemów i sieci teleinformatycznych opartych na narodowych certyfikowanych urządzeniach ochrony kryptograficznej.

- Usprawnienie systemu projektowania, wdrażanie i eksploatacji mieszanych systemów i sieci teleinformatycznych umożliwiających bezpieczne przetwarzanie i przesyłanie niejawnych informacji narodowych i sojuszniczych – łączenie narodowych systemów i sieci teleinformatycznych z sojuszniczymi

Rozwój technologii informacyjnych i kryptologii oraz powszechność ich wykorzystywania powodują pojawienie się nowych zagrożeń dla wytwarzanych, przetwarzanych, przesyłanych i gromadzonych informacji. Tym samym pojawiają się nowe wyzwania w obszarze ochrony informacji i bezpieczeństwa teleinformatycznego. Dlatego trzeba nieustannie usprawniać system edukacji

społeczeństwa, doskonalić prawo i profesjonalnie rozwiązywać pojawiające się problemy w obszarze bezpieczeństwa informacyjnego.

Z obawą można odnosić się do przyszłości bezpieczeństwa informacyjnego w naszym kraju, śledząc panujące od dwóch lat praktyki w obszarze ochrony informacji niejawnych i bezpieczeństwa teleinformatycznego, takich jak: sposób przewożenia niejawnych dokumentów i rozliczanie się z niejawnych materiałów przez Komisję Weryfikacyjną, gubienie niejawnych dokumentów i ujawnianie niejawnych informacji przez polityków i urzędników państwowych, upublicznianie informacji o żołnierzach i pracownikach służb specjalnych, w tym także kadrach nowych wojskowych służb specjalnych oraz patrząc na nieporadność i brak profesjonalizmu w reakcji administracji państwowej oraz prokuratur na tego typu zachowania, nie mówiąc już o stanie narodowej kryptografii. Bez wyeliminowania istniejących wad w obowiązującym prawie oraz nagannych praktyk w przestrzeganiu tego prawa, ale przede wszystkim bez szybkiej poprawy stanu narodowej kryptografii, nie ma szans na zapewnienie społeczeństwu i państwu bezpieczeństwa, a tym samym na zrealizowanie zadań zapisanych w „Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej”.

Stanisław Kowłopski

4 czerwca 2009 r.

Regulamin recenzowania i przyjmowania prac do druku

Redakcja przyjmuje do druku tylko te prace, które zostaną uznane przez recenzentów i redaktorów za właściwe pod względem tematyki i stanowiące oryginalny wkład do dyskusji na temat bezpieczeństwa narodowego lub posiadają pożądane walory dydaktyczne (szkoleniowe). Podpis pierwszego autora na stronie tytułowej jest równoznaczny ze stwierdzeniem, że: • złożona praca jest własna, • praca nie była przedtem opublikowana lub złożona do druku, • wszyscy autorzy wymienieni na stronie tytułowej wyrazili zgodę na złożenie tej pracy do publikacji na łamach biuletynu „Chłodnym okiem”. Nadesłane prace zostają poddane wstępnemu przeglądowi przez Redakcję „Chłodnym okiem”. W przypadku uznania pracy za ewidentnie niewłaściwą do publikacji na łamach „Chłodnym okiem”, otrzymane materiały (pocztą) wysyłane są do głównego autora w trybie natychmiastowym, bez dalszej recenzji.

Również wracając do głównego autora bez recenzji prace niedokończone lub przygotowane niezgodnie z Instrukcjami dla autora (zob. poniżej), jednak w takim przypadku można złożyć zwróconą pracę ponownie, po stosownej korekcie. O fakcie zarejestrowania pracy w Redakcji z podaniem numeru pracy w rejestrze, zostanie poinformowany listownie lub pocztą elektroniczną główny autor. Zarejestrowane prace wysyłane są do trzech zakwalifikowanych recenzentów w celu wykonania oceny wartości pracy. Proces recenzowania pracy nie powinien trwać dłużej niż dwa tygodnie, jednak Redakcja nie może zagwarantować określonego terminu podjęcia decyzji. Redakcja przyjmuje pracę do druku, jeżeli przynajmniej dwaj recenzenci są zgodni, że praca nadaje się do druku w prezentowanej formie. Jeżeli jednak recenzenci różnią się w swoich opiniach lub uważają, że manuskrypt powinien być zaakceptowany dopiero po dokonaniu stosownych korekt, Redakcja może podjąć stosowną decyzję o wysłaniu pracy do innego recenzenta w celu uzyskania rozstrzygnięcia lub zwróceniu pracy autorom do korekty. Ostateczna decyzja akceptacji pracy do druku, akceptacji pracy pod warunkiem wykonania korekty lub decyzja o odrzuceniu pracy należy do uprawnień Redakcji i nie podlega odwołaniu. Redakcja nie musi uzasadniać podjętych decyzji. Zezwolenia na druk Materiałom wykorzystanym z innych źródeł musi towarzyszyć pisemna zgoda pierwszego autora, jak i wydawcy pierwotnej publikacji, w której materiał ten został opublikowany, w których wyrażona jest zgoda na przedruk na łamach „CHŁODNYM OKIEM”. Odnośnie prac, które są jeszcze w druku, należy uzyskać zgodę na piśmie, od co najmniej jednego autora. Zgodę należy uzyskać również od osoby, która udostępniła dane niepublikowane lub informacje ustne wykorzystywane w artykule.

Odpowiedzialność cywilna Stowarzyszenie PRO MILITO i Redakcja czynią wszelkie starania, aby zapewnić rzetelność informacji, opinii i stwierdzeń zawartych w artykule ukazującym się w „CHŁODNYM OKIEM”. Niemniej jednak za treść artykułów i reklam odpowiada wyłącznie autor. Zgodnie z powyższym ani Stowarzyszenie, ani Rada Biuletynu nie ponoszą odpowiedzialności za skutki ewentualnych nierzetelności. Cały regulamin wydawniczy został opublikowany na stronie www.promilito.pl/regulamin-wydawniczy.htm



CHŁODNYM OKIEM

Biuletyn Stowarzyszenia Pro Milito

Nr 3, czerwiec 2009

Rada Wydawnicza

Przewodniczący Rady Wydawniczej Gen. broni Tadeusz Wilecki

płk prof. dr hab. Kazimierz Łastawski
płk prof. dr hab. Krzysztof Klukowski
wiceadm. Marek Toczek
płk dr Janusz Maćkowiak
płk prof. dr hab. Józef Marczak
ppłk dr Zygmunt Maciejewski

Zespół Redakcyjny

Redaktor Naczelny Gen. dyw. Julian Lewiński

Z-cy Redaktora Naczelnego
płk dr. Janusz Maćkowiak
gen Zenon Poznański
płk Jacek Praga

Redaktor Prowadzący Wojciech Łuczak

Chłodnym Okiem - Biuletyn Stowarzyszenia Pro Milito zrzeszającego żołnierzy rezerwy i w stanie spoczynku oraz byłych pracowników wojska. Zbieramy, porządkujemy, prezentujemy i komentujemy na naszych łamach informacje z wiarygodnych źródeł dotyczące istotnych spraw dla bezpieczeństwa narodowego. Poruszamy sprawy związane z szeroko pojętą obronnością kraju i popularyzujemy je w społeczeństwie. Stajemy w obronie dobrego imienia, reputacji i wiarygodności polskiego żołnierza, w tym także żołnierzy rezerwy i w stanie spoczynku. Współpracujemy z organizacjami krajowymi i zagranicznymi.

STOWARZYSZENIE
PRO MILITO

00-834 WARSZAWA
ul. Pańska 81/83 lok 536

www.promilito.pl
Nasz adres e-mail:
promilito@interia.pl

Czytelnik wysyłając swój e-mail na nasz adres tym samym wyraża zgodę na otrzymywanie od nas korespondencji i informacji elektronicznej na temat naszej działalności, a także wyraża zgodę na wpisanie jego danych wraz z adresem e-mail do naszej bazy danych. W przypadku rezygnacji z otrzymywania informacji drogą elektroniczną prosimy o powiadomienie nas o tym w swoim liście.

Regulamin Wydawniczy zawierający zasady recenzowania i przyjmowania prac do druku zawarty jest na stronie internetowej www.promilito.pl/regulamin-wydawniczy.htm.