Prof. dr hab. ***Tadeusz BĄK,*** *dr inż.* ***Zbigniew CIEKANOWSKI***
(Państwowa wyższa szkoła techniczno – ekonomiczna w Jarosławiu)

WPŁYW INFRASTRUKTURY TELEKOMUNIKACYJNEJ NA BEZPIECZEŃSTWO INFORMACJI

Streszczenie

W opracowaniu wpływ infrastruktury telekomunikacyjnej na bezpieczeństwo informacji, przedstawiony jest jak informacja narażona na różnego rodzaju zagrożenia. Przedstawiono szereg niebezpieczeństw, spowodowanych przejęciem kontroli nad informacją nie tylko przez nieuprawnione działanie w sieci teleinformatycznej jej użytkowników lub pojedyncze osoby, ale również przez zorganizowane grupy o nastawieniu antyspołecznym i antypaństwowym. W podsumowaniu zdiagnozowano podstawowe zagrożenia w dziedzinie bezpieczeństwa informacyjnego i wskazano prawne środki zapobiegania zagrożeniom oraz systemu legislacyjnego, który pozwoli dostosować się do zapobiegania nowym rodzajom przestępstw teleinformatycznych

Słowa kluczowe: ataki, bezpieczeństwo, infrastruktura telekomunikacyjna, informacja, zagrożenia.

Wstęp

Bezpieczeństwo to stan bądź proces, gwarantujący istnienie podmiotu oraz możliwość jego rozwoju.[1]

Bezpieczeństwo to stan, który daje poczucie pewności istnienia i gwarancje jego zachowania oraz szanse na doskonalenie. Jest to jedna z podstawowych potrzeb człowieka. Odznacza się brakiem ryzyka utraty czegoś dla podmiotu szczególnie cennego – życia, zdrowia, pracy, szacunku, uczuć, dóbr materialnych i dóbr niematerialnych. Bezpieczeństwo jest naczelną potrzebą człowieka i grup społecznych, jest także podstawową potrzebą państw i systemów międzynarodowych; jego brak wywołuje niepokój i poczucie zagrożenia. Człowiek, grupa społeczna, państwo, organizacja międzynarodowa starają się oddziaływać na swoje otoczenie zewnętrzne i sferę wewnętrzną, by usuwać a przynajmniej oddalać zagrożenia, eliminując własny lęk, obawy, niepokój i niepewność. Zagrożenia mogą być skierowane na zewnątrz i do wewnątrz; tak samo powinny być skierowane działania w celu ich likwidowania.

Wyróżnia się następujące rodzaje bezpieczeństwa:

1. ze względu na obszar jakie obejmuje – bezpieczeństwo globalne, bezpieczeństwo międzynarodowe, bezpieczeństwo regionalne, bezpieczeństwo narodowe;

2. ze względu stosunek do obszaru państwa – bezpieczeństwo zewnętrzne i bezpieczeństwo wewnętrzne;

3. ze względu na dziedzinę w jakiej występuje – bezpieczeństwo militarne, bezpieczeństwo polityczne, bezpieczeństwo energetyczne, bezpieczeństwo ekologiczne, bezpieczeństwo informatyczne, bezpieczeństwo społeczne, bezpieczeństwo kulturowe; bezpieczeństwo fizyczne i bezpieczeństwo socjalne; bezpieczeństwo strukturalne i bezpieczeństwo personalne.

Potrzeby społeczeństwa w dziedzinie bezpieczeństwa (wg W. Kitlera) [2]

1. potrzeba bezpieczeństwa i porządku publicznego
2. potrzeba bezpieczeństwa powszechnego
3. potrzeba ochrony zdrowia oraz bezpieczeństwa sanitarno-epidemiologicznego
4. potrzeba ochrony środowiska i gospodarki odpadami
5. potrzeba ochrony dorobku kulturowego i tożsamości narodowej
6. potrzeba bezpieczeństwa ekonomicznego
7. potrzeba oświaty i wychowania
8. potrzeba bezpieczeństwa narodowego

[1] Ryszard Zięba (red.), *Bezpieczeństwo międzynarodowe po zimnej wojnie*, Warszawa 2008
[2] *Słownik terminów z zakresu psychologii dowodzenia i zarządzania*, Warszawa 2000

1. Bezpieczeństwo RP[3]

W ten zbiór wartości do pewnego stopnia wpisują się podstawowe cele polskiej polityki bezpieczeństwa, określone następująco:

- ochrona suwerenności i niezawisłości Rzeczypospolitej;
- utrzymanie nienaruszalności granic i integralności terytorialnej kraju;
- zapewnienie bezpieczeństwa obywateli Polski, w tym praw człowieka i podstawowych wolności oraz demokratycznego porządku;
- stworzenie niezakłóconych warunków do cywilizacyjnego i gospodarczego rozwoju Polski oraz wzrostu dobrobytu jej obywateli;
- ochrona dziedzictwa narodowego i tożsamości narodowej
- realizacja zobowiązań sojuszniczych, a także obrona i promowanie interesów państwa polskiego.

Przemysł jest to dział produkcji materialnej, w którym wydobywanie zasobów przyrody i dostosowanie ich do potrzeb ludzi odbywa się na dużą skalę, na zasadzie podziału pracy i za pomocą maszyn.[4]

Funkcje przemysłu[5]

- produkcyjna (pozyskiwanie i przetwarzanie)
- społeczna (miejsca pracy, rozwój techniki produkcji, polepszenie warunków życia)
- przestrzenna (rozwój miast, przyspieszenie procesów urbanizacyjnych, przekształcenie środowiska)
- ekonomiczna (produkcja różnorodnych dóbr, energii lub wydobywanie surowców mineralnych)

Bezpieczeństwo przemysłowe to wszelkie działania związane z zapewnieniem ochrony informacji niejawnych udostępnianych przedsiębiorcy w związku z umową lub zadaniem wykonywanym na podstawie przepisów prawa.

Warunkiem dostępu przedsiębiorcy do informacji niejawnych w związku z wykonywaniem umów albo zadań wynikających z przepisów prawa, zwanych dalej „umowami", jest zdolność do ochrony informacji niejawnych.

2. Rodzaje ataków

W ostatnich latach nastąpił w Polsce gwałtowny rozwój infrastruktury telekomunikacyjnej. Sytuacja ta umożliwiła szerokie wykorzystywanie w procesach

zarządzania i kierowania nowoczesnych technik przekazu i przetwarzania informacji. Znaczenie obiegu informacji w instytucji państwowej, przedsiębiorstwie, organizacji militarnej, czy też koncernie działającym w sieci teleinformatycznej, porównać można do znaczenia krwioobiegu w organizmie ludzkim. Każda organizacja dysponująca informacjami, wykorzystuje do ich przechowywania, przetwarzania i przesyłania systemy teleinformatyczne (schemat 1). Pojawiło się szereg niebezpieczeństw, spowodowanych przejęciem kontroli nad informacją nie tylko przez nieuprawnione działanie w sieci teleinformatycznej jej użytkowników lub pojedyncze osoby, ale również przez zorganizowane grupy o nastawieniu antyspołecznym i antypaństwowym. Potencjalne możliwości nieuprawnionego działania w sieci teleinformatycznej jej użytkowników lub osób nie będących jej użytkownikami nazywane są zagrożeniami. Zagrożenia mogą występować przypadkowo lub być skutkiem działania celowego. Działania celowe, nazywane atakiem na system (schemat 2), mogą być realizowane bez aktywnego oddziaływania - atak pasywny lub z oddziaływaniem na system atak aktywny.

[3] R. Jakubczak, J. Flis – *Bezpieczeństwo Narodowe Polski w XXI wieku*, Warszawa 2006

[4] http://przemysl.gleby.net/

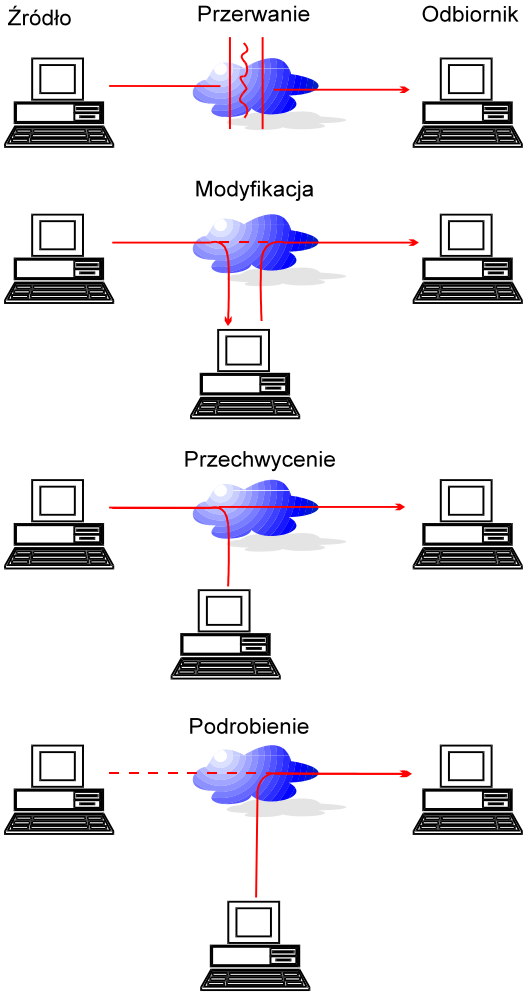
[5] http://www.sciaga.pl/tekst/63711-64-funkcje_przemyslu

Schemat nr 1. *Uproszczony schemat ochrony danych w sieci teleinformatycznej*

Źródło: opracowanie własne na podstawie, Z Ciekanowski, *Infrastruktura telekomunikacyjna jako element kształtowania bezpieczeństwa ekonomicznego Polski na przełomie XX – XXI wieku,* AON, Warszawa 2005 , s. 458

Atak pasywny polega na podsłuchiwaniu (szeroko pojętym) i monitorowaniu przesyłanych informacji. Celem ataku pasywnego może być dążenie do ujawnienia treści wiadomości lub uzyskanie informacji o samym ruchu informacji.

Atak pasywny to szeroko rozumiany podsłuch lub podgląd w celu zdobycia informacji niejawnej i/lub analiza ruchu w sieci dla zlokalizowania ważnych obiektów i stanowisk kierowania. Jest on najczęściej etapem przygotowawczym do wykonania ataku aktywnego na system.



Schemat nr 2. *Ataki na bezpieczeństwo w sieciach teleinformatycznych*

Źródło: opracowanie własne na podstawie, Z Ciekanowski, *Infrastruktura telekomunikacyjna jako element kształtowania bezpieczeństwa ekonomicznego Polski na przełomie XX – XXI wieku,* AON, Warszawa 2005 , s. 459

Atak aktywny dąży do modyfikowania strumienia informacji lub tworzenia fałszywych informacji. W działaniach tych mieszczą się: podszywanie się pod osobę uprawnioną i blokowanie działania. Rezultatem skutecznego ataku na system może być zmiana jego stanu i sposobu działania. Istnieją różne metody zablokowania systemu teleinformacyjnego. Jedną z najprostszych do przeprowadzenia metod jest atak polegający na tak silnym przeciążeniu działania systemu wówczas praca w nim okazuje się niemożliwa.

Ten rodzaj sabotażu może sparaliżować pracę organizacji w takim stopniu, że nie będzie ona mogła normalnie funkcjonować. Napastnik zaleje system falą komunikatów, listów elektronicznych, połączeń modemowych i żądań usług sieciowych w tak dużym stopniu, że system nie będzie praktycznie robił nic poza próbami wykonania tych wszystkich zleceń. Bardziej wyrafinowane ataki polegają na przekierowywaniu żądań usług systemu w inne, zupełnie niewłaściwe miejsca. Znany jest przykład takiego przeprogramowania połączeń modemowych, że każde połączenie było kierowane na przypadkowy błędny numer. Szczególną bolączką jest fakt, że ochrona przed blokadą usług systemu jest bardzo trudna – w praktyce wiąże się z izolowaniem systemu od otoczenia sieciowego. Zagrożenia atakiem występują, gdy istnieją możliwości:

1. Nieuprawnionego dostępu do przechowywanych, przetwarzanych lub przesyłanych informacji niejawnych bez oddziaływania na system;
2. Nieuprawnionego oddziaływania na system, których wykorzystanie może powodować:
   - zmiany w funkcjonowaniu sieci telekomunikacyjnej, w tym przerwanie lub czasowe zablokowanie realizowanych usług;
   - dostęp do przesyłanych, przetwarzanych lub przechowywanych informacji;
   - zniszczenie informacji lub innych zasobów;
   - fałszowanie lub nieuprawnioną modyfikację informacji;
   - dezinformację.

Chcąc jednak uzyskać kryptograficznie bezpieczny i spójny system teleinformatyczny (łączności), należy oprócz eksploatacji tych urządzeń zrealizować szereg przedsięwzięć organizacyjno – technicznych. Eksploatacja sieci teleinformatycznej (łączności) bez systemu ochrony informacji może umożliwić przeciwnikowi (wykorzystującemu istniejące luki w systemie ochrony) dostęp do informacji niejawnych, a działając w sposób aktywny może spowodować zniszczenie zasobów informacji i zdezorganizowanie funkcjonowania sieci.

Funkcje zaimplementowane w urządzeniach utajniających powinny realizować wiele różnych zadań kryptograficznych. Dla poprawnej pracy tych urządzeń niezbędne jest dostarczenie określonej ilości danych kluczowych, ich wymiana w określonym czasie i bieżący nadzór nad eksploatacją. Funkcje te możliwe są do zrealizowania przez odpowiednie zaprojektowanie i wykonanie urządzeń utajniających.

3. Zagrożenia atakiem

Specyfika eksploatacji sieci teleinformatycznej powoduje występowanie szeregu czynników sprzyjających powstawaniu zagrożeń bezpieczeństwa informacji. Poznanie ich pozwala prawidłowo projektować strukturę systemu, oraz konstrukcję i funkcje urządzeń.

Do czynników sprzyjających powstawaniu zagrożeń bezpieczeństwa informacji zaliczyć należy:

- rozproszenie zasobów teleinformatycznych na dużym terenie;
- eksploatowanie niewłaściwego sprzętu komputerowego;
- eksploatowanie "pirackiego" oprogramowania (systemowego i użytkowego);
- stosowanie do ochrony informacji nieetatowych środków ochrony (mechanizmów programowych i urządzeń technicznych);

- stosowanie sprzętu i oprogramowania nie sprawdzonego na obecność tzw. "pluskiew" programowych i sprzętowych;
- niechęć użytkowników i projektantów do stosowania środków ochrony informacji;
- niedocenianie zagrożeń bezpieczeństwa informacji w przez użytkowników.

Zagrożeniami bezpieczeństwa informacji mogą być występujące czynniki i elementy składowe systemu:

- ujawniająca emisja elektromagnetyczna komputerów, terminali i aparatury kanałowej oraz wrażliwość tych elementów na zakłócenie elektromagnetyczne;
- możliwość zdalnej penetracji zasobów informatycznych systemu;
- dołączanie podsłuchowych urządzeń rejestrujących;
- dołączanie niesankcjonowanych terminali;
- nielegalne wykorzystanie terminali użytkowników;
- stosowanie nielegalnego oprogramowania;
- czynniki losowe – zaniki napięcia, przesłuch, błędy w komutacji, zakłócenia w transmisji, powodzie, pożary;
- awarie urządzeń;
- niesolidność personelu wywołana niedoszkoleniem, bezmyślnością lub spowodowana szantażem.

W systemie teleinformatycznym eksploatowanych jest szereg różnych urządzeń i kanałów. Elementy te tworzą kilka podstawowych, zasadniczych podsystemów teleinformatycznych. W każdym z tych podsystemów występuje potrzeba określenia jednoznacznych i ścisłych wymagań dotyczących ochrony kryptograficznej. Do podsystemów tych zaliczyć należy:

- □ podsystem telekomunikacyjny;
- □ podsystem informatyczny;
- □ podsystemu kierowania i zarządzania siecią łączności;
- □ podsystem dystrybucji.

Jednocześnie z zasadniczymi funkcjami użytkowymi na te podsystemy powinny być nałożone elementy realizujące podsystem ochrony informacji.

4. Wymagania podsystemów

Podsystem ten powinien spełniać następujące wymagania:

- powinien być szczelny, spójny i chronić informację przed nielegalnym ujawnieniem, modyfikacją, przekształceniem i zniszczeniem;
- powinien zapewniać ochronę informacji od momentu jej powstania u użytkownika do momentu jej wykorzystania i celowego legalnego zniszczenia;
- powinien spełniać wymagania użytkownika w zakresie ochrony i być przez użytkowników w pełni akceptowany;
- środki i metody ochrony powinny uwzględniać przewidywany charakter zagrożeń bezpieczeństwa.

Podsystem ten powinien być modyfikowalny. Do budowy podsystemu ochrony informacji należy stosować środki techniczne, programowe i administracyjno – organizacyjne. Użytkownikom należy zostawić swobodę w stosowaniu dodatkowych środków ochrony ich własnej informacji pod warunkiem, że uzyskają odpowiedni atest. Przy projektowaniu i wdrażaniu podsystemu ochrony należy uwzględnić koszty jego budowy i eksploatacji.

Ochrona informacji w sieciach teleinformatycznych obejmuje aspekty zabezpieczania fizycznego, organizacyjnego, przesyłania i przetwarzania danych. Jeśli informacja przesyłana między elementami sieci jest utajniana, lecz nie ma fizycznych ograniczeń w dostępie do systemu, to utajnianie może okazać się bezcelowe. W sieci teleinformatycznej ochrony wymagają:

- informacje i dane (łącznie z oprogramowaniem i danymi związanymi z zabezpieczeniami, np.: klucze, uprawnienia dostępu, itp.);
- usługi komunikacyjne i przetwarzanie danych;
- urządzenia.

Dla elementów tych istnieją następujące zagrożenia:

- zniszczenie informacji i/lub innych zasobów (nieświadome lub złośliwe);
- fałszowanie lub modyfikacja informacji;
- kradzież, usunięcie lub zgubienie informacji;
- ujawnienie informacji niejawnych;
- przerwanie usługi;
- zmiana uprawnień.

Środki ochrony, zmniejszające ryzyko uzyskania dostępu do danych przez osoby nieupoważnione, ogólnie można podzielić na dwie kategorie: ograniczenie dostępu do zasobów systemu zgodnie z ustaloną polityką ochronną instytucji lub organizacji oraz kodowanie informacji (utajnianie) za pomocą metod kryptograficznych.

Przyszli użytkownicy systemów, urządzeń czy też oprogramowania, które mają służyć do przechowywania, przetwarzania i przesyłania informacji o charakterze niejawnym, muszą mieć pewność, że wyrób który zamierzają kupić spełnia wymagania bezpieczeństwa teleinformacyjnego. Wiara w werbalne zapewnienia producentów czy dealerów o bezpieczeństwie teleinformacyjnym tej kategorii wyrobów jest niewystarczająca.

Użytkownik powinien polegać na wynikach formalnej i bezstronnej oceny, dokonanej przez uprawniony do tego organ. Ocena wyrobu wymaga dobrze zdefiniowanego kryterium oceny zabezpieczenia oraz istnienia jednostki certyfikującej, uprawnionej do wydania potwierdzenia, że oceny dokonane przez laboratorium badawcze zostały przeprowadzone właściwie. Ocena możliwości zabezpieczających systemu może być rozpatrywana jako część większej formalnej procedury przyjęcia systemu teleinformatycznego do stosowania w konkretnym środowisku.

5. Kompleksowa ochrona informacji

Obecnie na zagrożenia procesów informacyjnych i infrastruktury teleinformatycznej najbardziej narażone są wysoko rozwinięte wielkie państwa, ale również kraje takie jak Polska, mogą spodziewać się potencjalnego ataku.

Kompleksowa ochrona informacji w sieciach teleinformatycznych obejmuje:

- aspekt prawny;
- zabezpieczenia fizyczne i organizacyjne;
- ochronę przed emisją ujawniającą;
- ochronę kryptograficzną.

Z oceny krajowych specjalistów i ekspertów wynika, że zagrożenia dostępu do sieci teleinformatycznej i naruszenia poufnych danych - w tym chronionych ustawą danych osobowych – nie spotykają się z właściwym zrozumieniem ze strony instytucji i podmiotów gospodarczych, które często traktują stały monitoring informacyjny jako dodatkowy, zbędny wydatek. Tak błędnie pojmowana oszczędność może przynieść katastrofalne skutki podczas zagrożeń, pomimo, że spektrum środków ochrony systemów i sieci jest coraz większe oraz tańsze.

Zagadnienia ochrony informacji w polskiej strategii bezpieczeństwa były przedmiotem analizy, już w latach osiemdziesiątych. W Akademii Sztabu Generalnego Wojska Polskiego powstawały prace omawiające znaczenie systemów informacyjnych w siłach zbrojnych[6].

[6] S. Koziej, *Rajdy bojowe,* Warszawa 1987; S. Koziej, *Teoria sztuki wojennej*, Warszawa 1993.

Problemem obiegu informacji o znaczeniu strategicznym zajmowała się Rada Ministrów[7], a także Ministerstwo Obrony Narodowej[8]. W opracowanych dokumentach kompetencje w zakresie bezpieczeństwa informacyjnego zostały powierzone Agencji Bezpieczeństwa Wewnętrznego. ABW powstała ze struktur UOP, pracuje aktualnie nad kompleksową strategią ochrony bezpieczeństwa teleinformatycznego, gdyż do jej ustawowych zadań należy m.in. zapewnienie bezpieczeństwa systemów i sieci teleinformatycznych, w których są wytwarzane, przechowywane, przetwarzane lub przekazywane informacje niejawne stanowiące tajemnicę państwową lub służbową.

Zadania ABW w tym zakresie realizuje wyspecjalizowany zespół Departamentu Bezpieczeństwa Teleinformatycznego zwany Jednostką Certyfikującą. Pod wpływem nadchodzących z USA doniesień o atakach na sieci rządowe, od lat dziewięćdziesiątych, w Polsce podjęto zagadnienie ochrony dostępu do danych gromadzonych przez służby publiczne. Sukcesywnie były prowadzone prace nad stworzeniem projektu regulacji prawnych, w randze ustawy bądź rozporządzenia.

Inne zalecenia specjalistów z zakresu ochrony informacji zostały włączone sektorowych dokumentów m.in.: przepisów o rachunkowości, o ochronie danych osobowych, w prawie bankowym i ustawie o ochronie informacji niejawnych.

Na podstawie dokonanej analizy doświadczeń NATO i USA, w roku 2002 przyjęto wypracowaną przez MSWiA definicję polskiej infrastruktury krytycznej, uzgadniając, że narodowa strategia skupiona będzie wokół kategorii „bezpieczeństwa teleinformatycznego". Za infrastrukturę krytyczną państwa uznano „obiekty i urządzenia oraz służby odpowiedzialne za ich ochronę, systemy sieci teleinformatycznej istotne dla bezpieczeństwa ekonomicznego i dobrobytu państwa oraz jego efektywnego funkcjonowania"[9]. Z definicji tej wynika, że wymienione gałęzie gospodarki narodowej, mieszczą się w ramach infrastruktury krytycznej, nazywanej „obszarami informacji szczególnie wrażliwej z punktu widzenia bezpieczeństwa państwa"[10]. Ochroną infrastruktury krytycznej zajmuje się Krajowy System Ochrony Krytycznej Infrastruktury Teleinformatycznej (KSOKITI). Obecnie Agencja Bezpieczeństwa Wewnętrznego patronuje szkoleniom informacyjnym poświęconym upowszechnianiu wiedzy na temat zagrożeń cybernetycznych w wyniku, których, wydawane są certyfikaty inspektorów bezpieczeństwa teleinformatycznego.

Porównując amerykańskie i polskie doświadczenia oraz stan przygotowań naszego kraju do walki z zagrożeniami w dziedzinie teleinformatyki, dokonano oceny możliwości ataków na polską infrastrukturę informacyjną, w wyniku, czego uznano, że prawdopodobieństwo zmasowanych i celowych działań zagrażających bezpieczeństwu informacyjnemu jest niewielkie. Zmienną, podnoszącą stopień zainteresowania Polską jako przedmiot ataku, staje się natomiast coraz większe zaangażowanie się w walkę ze światowym terroryzmem, które sytuuje nasz kraj wśród głównych sojuszników Stanów Zjednoczonych. Ryzyko realne jest, zatem dotąd niewielkie, lecz ryzyko potencjalne – sukcesywnie rośnie. Stopień bezpieczeństwa teleinformatycznego jest, zatem pochodną aktywności sojuszniczej Polski.

Prezes Rady Ministrów w dokumencie z 22 lipca 2002 roku, ustanowił odpowiedzialność Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego w zakresie: akredytacji bezpieczeństwa systemów i sieci teleinformatycznych, badań i certyfikacji środków ochrony kryptograficznej, elektromagnetycznej i fizycznej oraz organizacji szkoleń w dziedzinie bezpieczeństwa teleinformatycznego[11].

---

[7] Rozporządzenie Prezesa Rady Ministrów z dnia 9 września 2002 r. w sprawie wymiany informacji istotnych dla bezpieczeństwa zewnętrznego i międzynarodowej pozycji Rzeczypospolitej Polskiej, „Dz. U. 2002 nr 150, poz. 1234.

[8] Decyzja nr 182/MON z dnia 6 października 2000 r. w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej (dokument wewnętrzny).

[9] R. Kośla, *Ochrona infrastruktury krytycznej w Polsce - aktualny stan prac*; [URL http://www.cert.pl].

[10] Tamże.

[11] Tamże.

Znane dzisiaj metody ochrony informacji nie gwarantują absolutnego bezpieczeństwa i dalekie są od ideału, a zjawiska włamań do sieci nie dają się wyeliminować. Włamania do systemów teleinformatycznych przynoszą znaczne straty finansowe i często utratę zaufania do instytucji, której powierzono poufne informacje. Zgodnie z ustaloną i prowadzoną polityką ochronną w danej instytucji, istnieje szereg różnych metod i środków ochrony informacji. Do podstawowych z nich zaliczyć należy:

- metody organizacyjno-administracyjne:
- ograniczenie dostępu do informacji niejawnych;
- ograniczenie uprawnień osób funkcyjnych w systemie zarządzania;
- metody i środki programowe:
- hasła dostępu do zbiorów;
- uprawnienia;
- uwierzytelnienie i identyfikacja;
- zamknięte grupy użytkowników;
- środki techniczne:
- osłony ekranujące;
- kabiny ekranujące;
- ekranowanie pomieszczeń;
- urządzenia o obniżonym poziomie ujawniającej emisji elektromagnetycznej;
- światłowody;
- środki ochrony przed nieuprawnionym dostępem do sprzętu;
- środki ochrony przed nieuprawnionym dostępem do programów;
- szyfrowanie informacji:
- szyfrowanie kanałowe;
- szyfrowanie baz danych;
- uwierzytelnianie użytkownika.

Usługi ochrony danych zapewniają uzyskanie pewnych gwarancji w zakresie wiarygodności systemu teleinformatycznego:

- poufność – ochrona przed atakiem pasywnym;
- uwierzytelnienie – zapewnienie autentyczności informacji i osób: zagwarantowanie, że informacja pochodzi z takiego źródła, które jest przy niej wymieniane lub też osoba jest tą, za którą się podaje;
- nienaruszalność – zapewnienie integralności komunikacji, tzn. tego, że informacja jest odbierana w takiej postaci, w jakiej została wysłana;
- niezaprzeczalność – niemożliwość zaprzeczenia faktowi wysłania lub odebrania informacji;
- kontrola dostępu – możliwość kontrolowania dostępu do informacji (systemów) drogą identyfikacji i uwierzytelniania;
- dyspozycyjność – ograniczanie skutków ataku w sferze dostępności informacji.

Mechanizmy zabezpieczające obejmują następujące działania:

- □ szyfrowanie informacji;
- □ uwierzytelnianie informacji (podpisy cyfrowe);
- □ ochrona antywirusowa;
- □ identyfikacja i uwierzytelnianie osób uprawnionych.

Kryptograficzne metody ochrony są ważnym elementem bezpieczeństwa informacji w sieciach teleinformatycznych i chociaż mają zasadnicze znaczenie, same nie gwarantują pełnego bezpieczeństwa informacji. Celem kryptograficznej ochrony informacji w systemie teleinformatycznym jest:

a) wyeliminowanie dostępu do zasobów podsystemu osobom nieuprawnionym;
b) zapewnienie dostępu do zasobów legalnym użytkownikom w ramach ich uprawnień;
c) zapewnienie poufności informacjom niejawnym przechowywanym na dyskach;

d) zapewnienie poufności, integralności i uwierzytelniania informacjom niejawnym przesyłanym w sieci teleinformatycznej.

Jeśli informacja jest szyfrowana, ale nie ma fizycznych ograniczeń w dostępie do systemu lub brak jest zabezpieczeń przed emisją ujawniającą, to szyfrowanie nie zapewni wysokiego poziomu bezpieczeństwa. Odpowiednio zaprojektowane i wdrożone szyfry zdecydowanie ograniczają możliwości działania nawet wyrafinowanego przeciwnika. Brak kryptograficznej ochrony informacji w sieci może powodować, że bezcelowe są inne działania (np. ochrona przed emisją ujawniającą). Metody kryptograficzne są wykorzystywane do:

- zapewnienia poufności informacjom przechowywanym i przesyłanym w sieci;
- zachowania integralności przesyłanych i przechowywanych danych;
- uwierzytelniania informacji;
- zapewnienia integralności połączenia (uniemożliwienie odbioru informacji przez innego niż adresat użytkownika);
- wiarygodnej identyfikacji i uwierzytelniania użytkowników i stacji;
- wiarygodnej weryfikacji uprawnień użytkowników do korzystania z zasobów sieci poprzez sterowanie dostępem (autoryzację) do danych;
- ochrony przed fałszywymi powtórzeniami;
- maskowania przepływu informacji między obiektami sieci.

Pełną poufność przesyłanych informacji zapewnić można tylko przez szyfrowanie u źródła i deszyfrowanie dopiero przy jej ujściu. Istotnym problemem jest wtedy dystrybucja kluczy szyfrowych. Zmiana kluczy odbywać się musi w taki sposób, aby nie powodowała utraty spójności sieci.

Wykorzystywanie tego samego klucza przez wielu użytkowników grozi jego dekonspiracją (np. wskutek utraty urządzenia utajniającego z kluczem), a w konsekwencji ujawnieniem wszystkich informacji zaszyfrowanych z jego użyciem. Stąd wymaga się, aby w każdej relacji i seansie łączności do szyfrowania informacji był wykorzystywany inny klucz. Do identyfikacji użytkownika wykorzystywane są tzw. inteligentne karty SIM, zawierające mikroprocesor z pamięcią. W pamięci są zapisane: numer użytkownika oraz jego prywatny tajny klucz szyfrowy. W SIM są zaimplementowane algorytmy szyfru jednokierunkowego, wykorzystywane w procesie identyfikacji i uwierzytelniania użytkownika oraz do wypracowania klucza wykorzystywanego w procesie szyfrowania przesyłanych informacji. Podstawowe pojęcia z zakresu ochrony danych to: atak na bezpieczeństwo danych, mechanizm zabezpieczający i usługa ochrony danych.

Warunkiem koniecznym wprowadzenia urządzeń kryptograficznych powinno być zapewnienie pełnego bezpieczeństwa podczas prowadzenia wymiany informacji. Pewną część tych zadań można zrealizować przez utajnianie (szyfrowanie) informacji. Chcąc jednak uzyskać kryptograficznie bezpieczną i spójną sieć teleinformatyczną, należy oprócz eksploatacji tych urządzeń zrealizować inne przedsięwzięcia techniczno-eksploatacyjne.

Pierwszym etapem ochrony informacji jest projekt urządzenia przetwarzającego niejawną, nie utajnioną informację (np. mikrokomputer wykorzystywany do tworzenia niejawnych dokumentów). Można próbować tak zaprojektować i wykonać urządzenie, aby poziomy emisji ujawniających były jak najmniejsze. Takie działania prowadzą do uzyskania odpowiedniego poziomu zabezpieczenia urządzenia, czyli zakresu wykorzystania rozwiązań technologicznych jako integralnej części konstrukcji urządzenia w celu obniżenia poziomu emisji ujawniającej.

Naturalnym sposobem ograniczania poziomu emisji ujawniającej jest uniemożliwienie przeciwnikowi zbliżenia się do przetwornika informacji. W ten sposób pojawia się koncepcja stref bezpieczeństwa emisji warunkowanych wartościami tłumienności na ich granicy lub w terenie otwartym odległościami do ich granic.

Wymienione metody ochrony, tzn. zabezpieczenie urządzenia, zabezpieczenie miejsca oraz strefa bezpieczeństwa emisji, w konkretnym przypadku muszą zapewnić odpowiedni poziom zabezpieczenia informacji, – czyli wymagany stopień obniżenia poziomu emisji ujawniającej w celu uniemożliwienia odtworzenia informacji z wymaganą wiernością i w zadanym czasie. Miarą poziomu

zabezpieczenia informacji jest wartość współczynnika protekcji w odpowiedniej odległości od jej przetwornika. Przedstawiona powyżej wielowariantowa możliwość zapewnienia stanu bezpieczeństwa emisji pozwala elastycznie wybierać to rozwiązanie, które w danej sytuacji jest najlepsze z technicznego i ekonomicznego punktu widzenia.

Omówiona problematyka bezpieczeństwa emisji regulowana jest w NATO. Należy jednakże podkreślić, że poszczególne kraje członkowskie niezależnie od zobowiązań NATO-wskich stosują swoje narodowe normy, które stworzyły swoje wymagania narodowe nie udostępniane innym krajom, nawet sojusznikom. Postęp w komputeryzacji nie spowodował jednak doskonalenia systemów zabezpieczenia przed dostępem do informacji klasyfikowanych przez „Ustawę z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych". W Polsce dość skutecznie chroni się bazy danych firm przed hakerami działającymi w sieciach komputerowych oraz zwykłymi włamaniami np. do linii transmisyjnych. Zupełnie inny wymiar ma ochrona przed włamaniami do systemów komputerowych dokonywanych przy użyciu nowoczesnych systemów skanujących dane „namierzonego" komputera. W naszym kraju normy te nie były dotychczas stosowane. Zabezpieczenie komputerów przed emisją ujawniającą w wielu instytucjach i urzędach centralnych z przedstawionych powyżej przyczyn nie jest najlepsze, a szczególnie w instytucjach placówkach naukowych. Można mieć nadzieję, że w najbliższych latach, konieczność tworzenia społeczeństwa informacyjnego, a przede wszystkim obecności państwa w strukturach NATO i UE pozwoli na nadrobienie zaistniałych zaległości i stworzenia skutecznych systemów zabezpieczeń i ochrony informacji w systemach komputerowych jak i samych komputerów.

6. Ocena zagrożeń

Etapy realizacji podsystemu bezpieczeństwa i ochrony w systemach teleinformatycznych.

Ocena zagrożeń jest pierwszym etapem pracy przy analizie bezpieczeństwa sieci, obejmuje ona:

a) identyfikację słabych punktów systemu;
b) analizę prawdopodobieństwa występowania zagrożeń z uwzględnieniem słabych punktów systemu;
c) ocenę konsekwencji wykorzystania każdego zagrożenia indywidualnie oraz w powiązaniu z innymi zagrożeniami;
d) oszacowanie kosztów każdego ataku (w tym ocenę na ile udany atak ułatwia następne);
e) oszacowanie kosztów potencjalnych środków przeciwdziałania, w tym również ewentualnego pogorszenia parametrów funkcjonalnych systemu.

Następnym etapem realizacji ochrony powinno być zrealizowanie przedsięwzięć organizacyjno-administracyjnych. Opracowane powinny być one z uwzględnieniem następujących zasad:

1. Informacja powinna być przekazana, udostępniona lub przedstawiona do oceny tylko tym użytkownikom, którzy są do tego odpowiednio uprawnieni.
2. Użytkownicy powinni mieć dostęp do zasobów tylko w zakresie swojego uprawnienia.
3. Każda próba nieuprawnionego działania w systemie powinna być wykrywana, rejestrowana i sygnalizowana służbom nadzoru.
4. Działania użytkowników systemu łączności, mające wpływ na żywotność systemu, powinny być one rejestrowane w dzienniku kontrolnym z podaniem danych identyfikujących użytkownika, rodzaju i terminu wykonywanej operacji.
5. Prowadzeniu dziennika użytkownicy powinni być poinformowani, ale nie powinni mieć do niego dostępu. Dostęp do dziennika powinien być zagwarantowany dla służb nadzoru.

Następnym etapem powinien być więc wybór odpowiednich urządzeń utajniających. W celu zrealizowania ww. założeń, w urządzeniach tych powinny być zainstalowane następujące niezbędne elementy:

- ściśle sprecyzowane algorytmy obsługi, uwzględniające wprowadzenie hasła;
- konieczność pracy z identyfikatorem osobistym, wykorzystywanym m.in. do tworzenia grup użytkowników;
- segmenty realizujące funkcje archiwizacji podstawowych zdarzeń;
- segmenty realizujące procedury zdalnej dystrybucji;

- procedury transmisyjne;
- algorytmy zabezpieczające dane kluczowe przechowywane w urządzeniach.

Podstawowym etapem w organizowaniu systemu ochrony jest rozpoznanie obszaru ochrony. Przede wszystkim trzeba określić, z czego składa się sieć: jak wygląda schemat sieci, punkty dostępu do sieci i kto z nich korzysta. Ponadto należy dokonać oceny wartościowej informacji. Jakie zasoby informacyjne są na tyle ważne, aby je chronić, i gdzie są zlokalizowane?

Szkolenie personelu w zakresie ochrony informacji jest sprawą poza wszelką dyskusją, choć często zaniedbywaną. Niezbędna jest ciągła współpraca personelu zajmującego się ochroną z komórkami organizacyjnymi przedsiębiorstwa, jak również wspomaganie, zrozumienie i elastyczność wobec użytkownika końcowego. Proces edukacyjny dla całego personelu powinien być dostosowany do oczekiwań i potrzeb każdej grupy pracowniczej, w przeciwnym razie ochrona będzie pomijana, wyłączana lub ignorowana. Ustalenie polityki ochrony i przeszkolenie personelu są wstępem do wprowadzenia w życie planu ochrony - realizacja tego zadania powinna być w miarę „bezbolesna" i płynna.

Zakończenie

Znanych jest kilka podejść do problemu ochrony informacji, mających wpływ na całą architekturę systemu ochrony. Nie są to rozwiązania idealne, ponieważ żaden system nie jest w stanie spełnić wszystkich wymagań.

Jakość podsystemu bezpieczeństwa i ochrony zależy od prawidłowego opracowania założeń, wyboru odpowiednich urządzeń utajniających oraz zrealizowania przedsięwzięć organizacyjno-administracyjnych. Zaproponowana konstrukcja urządzeń utajniających powinna umożliwić wdrożenie modułu do wielu urządzeń podsystemu łączności. Przyjęta technologia powinna pozwolić na ciągły rozwój urządzeń już opracowanych, wdrożonych i eksploatowanych. Kolejne wersje urządzenia lub określone ich funkcje mogą być wprowadzane przez upoważnione osoby u użytkownika, po dołączeniu dowolnego urządzenia telekomunikacyjnego lub informatycznego.

Bezpieczeństwo sieci to nie tylko środki techniczne i programowe systemów ochrony. Bezpieczeństwo to zarówno problem środków ochrony, jak i zarządzania zasobami oraz informacją. Jest ono w rzeczy samej pochodną dobrej organizacji i właściwej polityki ochrony wprowadzanej na wszystkich szczeblach organizacyjnych. Problem ochrony sieci instytucji, przedsiębiorstwa należy rozpatrywać na wszystkich szczeblach jego struktury organizacyjnej nie wyłączając z tego ścisłego zarządu. Polityka ochrony musi być jednoznaczna i przejrzysta, a każdy pracownik firmy powinien być z nią zaznajomiony. Sama technologia nie może zapewnić pełnego bezpieczeństwa. Ochrona to przede wszystkim właściwe zarządzanie i organizacja.

Strategia bezpieczeństwa informacyjnego państwa nie została jeszcze w pełni określona, o tym decyduje poziom rozwoju sieci, komputeryzacja sektora publicznego i poziom zrozumienia nowych zagrożeń przez podmioty gospodarcze szczególnie prywatne. Powstaje ona na możliwościach dostosowań polskiej gospodarki do modelu społeczeństwa informacyjnego i zmian a przede wszystkim w sektorze telekomunikacyjnym. Program dostosowawczy *ePolska* jest inicjatywą pomostową, która odpowiada na unijne dyrektywy, sugerujące przygotowanie państw kandydackich do jednolitego modelu społecznego (program *eEuropa+)*. Diagnozuje podstawowe zagrożenia w dziedzinie bezpieczeństwa informacyjnego i wskazuje prawne środki zapobiegania. Polski system legislacyjny powoli dostosowuje się do nowych rodzajów przestępstw teleinformatycznych.

Należy jednak opracować strategie szkoleniowe, prowadzić stały monitoring sieci i systemów, zapewnić szeroką kampanię informacyjną na temat zagrożeń bezpieczeństwa teleinformatycznego. Z tworzeniem systemu muszą być powiązane: harmonizacja systemu prawnego i zmiany legislacyjne, wprowadzające m.in. ściganie z urzędu przestępstw teleinformatycznych (szczególnie komputerowych).

Bibliografia:

1. **Z. Ciekanowski,** Infrastruktura telekomunikacyjna jako element kształtowania bezpieczeństwa ekonomicznego Polski na przełomie XX – XXI wieku, AON, Warszawa 2005
2. **R. Jakubczak**, J. Flis – Bezpieczeństwo Narodowe Polski w XXI wieku, Warszawa 2006
3. **R. Kośla,** Ochrona infrastruktury krytycznej w Polsce - aktualny stan prac; [URL http://www.cert.pl].
4. **S. Koziej,** Rajdy bojowe, Warszawa 1987; w Teoria sztuki wojennej, Warszawa 1993.
5. **Słownik** terminów z zakresu psychologii dowodzenia i zarządzania, Warszawa 2000
6. **Zięba (red.),** Bezpieczeństwo międzynarodowe po zimnej wojnie, Warszawa 2008
7. **Rozporządzenie** Prezesa Rady Ministrów z dnia 9 września 2002 r. w sprawie wymiany informacji istotnych dla bezpieczeństwa zewnętrznego i międzynarodowej pozycji Rzeczypospolitej Polskiej, „Dz. U. 2002 nr 150, poz. 1234.
8. **Decyzja** nr 182/MON z dnia 6 października 2000 r. w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej (dokument wewnętrzny).
9. http://www.sciaga.pl/tekst/63711-64-funkcje_przemyslu
10. http://przemysl.gleby.net/