Zofia Kałuża

Bezpieczeństwo sieci i systemów teleinformatycznych

Kultura Bezpieczeństwa. Nauka-Praktyka-Refleksje nr 10, 51-60

2012

STREFA STUDENTA

Zofia Kałuża - BEZPIECZEŃSTWO SIECI I SYSTEMÓW TELEINFORAMTYCZNYCH[121]

Wymagania podstawowe

Zapewnienie odpowiedniego poziomu bezpieczeństwa[122] systemowi sieci teleinformatycznych dla potencjalnego użytkownika lub danej jednostki organizacyjnej było zawsze zadaniem trudnym, leczo obecnie jest to już znaczący problem.. Bezpieczeństwo teleinformatyczne to bezpieczeństwo systemów i sieci teleinformatycznych. System taki tworzą urządzenia, narzędzia, metody postępowania i procedury stosowane przez wyspecjalizowanych pracowników, w sposób zapewniający wytwarzanie, przechowywanie, przetwarzanie lub przekazywanie informacji.[123] Natomiast sieć teleinformatyczna to organizacyjne i techniczne połączenie systemów teleinformatycznych. Podstawowe wymagania w zakresie bezpieczeństwa narzuca art. 18 ust. 1 ustawy określając kto jest odpowiedzialny za bezpieczeństwo ochrony informacji zatem również za system i sieć teleinformatyczną. Są to zadania dla kierownika jednostki administracyjnej, to on opracowuje zasady działania i eksploatacji systemu bezpieczeństwa sieci. W tym celu kierownik komisji organizacyjnej powołuje osoby funkcyjne: administratora (ów)- osobę lub zespól osób odpowiedzialnych za prawidłowe za prawidłowe funkcjonowanie systemu lub sieci oraz za przestrzegania narzuconych zasad, określonych wymogów bezpieczeństwa- inspektora bezpieczeństwa teleinformatycznego, który będzie miał obowiązek kontroli zgodności systemów i sieci ze szczególnymi wymaganiami bezpieczeństwa. Dostęp do tego typu informacji w przypadku tych osób powinien być poprzedzony specjalistycznym przeszkoleniem upoważnionych do tego rodzaju szkolenia osób, czyli przez służby ochrony państwa- ABW lub SKW. Natomiast podstawowe wymagania w zakresie bezpieczeństwa teleinformatycznego wynikają z Rozporządzenia Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. z 2005 r. Nr 171 poz. 1433) realizuje się poprzez szereg działań organizacyjnych polegających na ochronie fizycznej tzn. *„umieszczenie urządzeń systemu lub sieci teleinformatycznej w strefie bezpieczeństwa, strefie administracyjnej lub w specjalnej strefie w zależności od klauzuli tajności”* ilości zagrożeń, następujących kryteriów tzn: poufność-

[121] Praca jest fragmentem pracy licencjackiej Pani Zofii Kałuży - studentki WSBPiI „Apeiron” w Krakowie oraz członkini Koła Naukowego Administracji Autonomicznym Systemem Bezpieczeństwa WSBPiI „Apeiron”. Została napisana po kierunkiem dra Bogusława Płonki.

[122] J. Piwowarski, *Bezpieczeństwo jako pożądany stan oraz jako wartość*, [w:] *Bezpieczeństwo jako wartość*, „Wydanie pokonferencyjne z II Konferencji Naukowej z cyklu „Bezpieczeństwo jako wartość” zorganizowanej przez Wyższą Szkołę Bezpieczeństwa Publicznego i Indywidualnego „Apeiron” w Krakowie, 18 kwietnia 2008”, Kraków 2010.

[123] T. Szewc, *Publicznoprawna ochrona informacji*, Wyd. C.H. Beck, Warszawa 2007, s. 190.

dostęp do informacji musi być ograniczony do kręgu użytkowników posiadających poświadczenie bezpieczeństwa. Integralność- informacja powinna być zachowana w swojej oryginalnej postaci. Dostępność- czyli informacje należy udostępnić na żądanie osób upoważnionych. Rozliczność, autentyczność, niezawodność. W zakresie ochrony fizycznej urządzeń systemów i sieci teleinformatycznych przetwarzających informacje niejawne (w tym środków zabezpieczających pomieszczenia przed nieuprawnionym dostępem, podglądaniem i podsłuchem) należy stosować przepisy zawarte w: wytycznych w zakresie bezpieczeństwa fizycznego kancelarii kryptograficznych, stacji łączności kryptograficznej oraz pomieszczeń terminali i autonomicznych stanowisk komputerowych przeznaczonych do przetwarzania informacji niejawnych- DBBT-301 B[124] oraz wytycznych w sprawie instalacji urządzeń przeznaczonych do przetwarzania informacji niejawnych- BTPO-71 A.[125] Wszelkie zastosowane środki i metody ochrony fizycznej systemu lub sieci teleinformatycznej powinny zatem odzwierciedlać w szczególnych wymaganiach bezpieczeństwo danego systemu. Ochrona elektromagnetyczna- literatura podaje, ze stosuje się ją w celu zapewnienia odpowiedniego poziomu bezpieczeństwa, nadaje procedury, które zależą od klasyfikacji przechowywanej informacji, zabezpieczenia urządzenia jak również poziomu zabezpieczenia miejsca. Wytyczne dotyczące tej kategorii ochrony reguluje zapis wytycznych w sprawie instalacji urządzeń przeznaczonych do przetwarzania informacji niejawnych- BTPO- 701 A dla MON.[126] Ochrona kryptograficzna polega na zastosowaniu mechanizmów gwarantujących utrudnienie przyjęcia informacji poprzez ich przekształcenie w sposób znany, określony odpowiednio upoważnionej osobie (użytkownikowi). Metoda ta to zabezpieczenie informacji niejawnych poprzez szyfrowanie oraz stosowanie innych mechanizmów kryptograficznych gwarantujących zachowanie informacji w swojej oryginalnej postaci, za wyjątkiem gdy jest ona legalnie modyfikowana. Metody, środki ochrony kryptograficznej stosowane przy przekazywaniu informacji niejawnych stanowiących tajemnicę państwową lub służbową określaną *poufne* powinny być opisywane w szczególnych wymogach bezpieczeństwa sieci i systemów.

Bezpieczeństwo transmisji zapewni się przez podłączenie systemu lub sieci teleinformatycznej do powszechnie dostępnego urządzenia. System pod warunkiem ochrony kryptograficznej poprzez metodę szyfrowania informacji niejawnych. Ochrona niezawodności transmisji dla tego rodzaju systemu lub sieci powinna być zawarta w szczególnych wymaganiach. Bezpieczeństwo transmisji wchodzące w skład podstawowych wymagań bezpieczeństwa teleinformatycznego ma określone wymagania dotyczące podłączenia systemów lub sieci przetwarzających informacje niejawne stanowiące tajemnice państwową *ściśle tajne* do innych sieci. W przypadku wzajemnego podłączenia dwóch lub więcej systemów należy zapewnić nienaruszalność cech bezpieczeństwa każdego z tych systemów. Jako ostatnie wymagania podstawowe można wyróżnić kontrolę dostępu do urządzeń. Procedury kontroli dostępu służą do nadawania lub odbieranie prawa dostępu danego użytkownika do zasobów. Z ich właściwe funkcjonowanie odpowiada administrator systemu, warunki oraz sposób przydzielania uprawnień użytkownikom tych systemów sieci teleinformatycznych określa Kierownik jednostki organizacyjnej. Natomiast warunki oraz sposób przydzielania użytkownikom kont i haseł określa administrator systemu.[127] Oto niekute zasady i procedury haseł: hasło musi składać się z kombinacji małych i dużych liter

[124] Załącznik nr 2 z dnia 27 października 2008 r. do Minimalne Wojskowe wymagania organizacyjno- użytkowe dla zadania inwestycyjnego/remontowego.
[125] Dziennik Urzędowy Ministra Obrony Narodowej nr 7 poz. 3004, Warszawa 2007 r.
[126] tamże, poz. 3010.
[127] Http://www.iniejawna.pl

oraz cyfr i znaków specjalnych i musi być unikalne. Hasło powinno być przydzielone użytkownikowi. Wszelkie elementy hasła powinny być rejestrowane przez system itp. powinna być też określona długość hasła. Hasło powinno być okresowo zmieniane itp. należy też zaznaczyć, iż systemy i sieci teleinformatyczne przetwarzające informacje niejawne powinny prowadzić automatyczną ewidencję dotyczącą określonych zdarzeń. Okres przechowywania rejestrów dostępu do tajemnicy państwowej wynosi 5 lat., *poufne* 2 lata, *zastrzeżone* rok. Do podstawowych wymagań zalicza się także przeszkolenie z zakresu bezpieczeństwa teleinformatycznego wszystkich pracowników upoważnionych do pracy z danymi systemami i informacjami.

Dokumentacja

Dla każdego systemu lub sieci teleinformatycznej zachodzi konieczność opracowania dokumentów *szczególnych wymagań bezpieczeństwa* systemu lub sieci teleinformatycznej oraz procedur bezpiecznej eksploatacji (art. 6 ust. 1 ustawy o ochronie informacji niejawnych) dokumenty o nazwie SWB (Szczególne Wymagania Bezpieczeństwa) są dokumentami tworzonymi w celu dopuszczenia systemu lub sieci do wytwarzania, edytowania lub archiwizowania dokumentów niejawnych posiadających klauzulę *zastrzeżone, poufne, tajne, ściśle tajne.* Dokument ten określa budowę, konfigurację i specyfikę pracy oraz zagrożenia systemu lub sieci teleinformatycznych wynikające z nieprawidłowego dostępu do danych niejawnych. Szczególne wymagania bezpieczeństwa SWB najczęściej opracowuje pełnomocnik ochrony, administrator systemu oraz inspektor bezpieczeństwa teleinformatycznego konsultując się ze specjalistami bezpieczeństwa teleinformatycznego służb ochrony państwa upoważnionymi do zatwierdzenia danego dokumentu.[128] Zasady opracowania Szczególnych Wymagań Bezpieczeństwa zostały opisane w rozdziale 3 Rozporządzenia Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego „*Z przepisów zawartych w przeznaczonym rozdziale wynika, że dokumenty SWB opracowuje się po przeprowadzeniu szacowania ryzyka dla informacji niejawnych, które mają być przetwarzane w danym systemie Ti z uwzględnieniem warunków charakteryzujących dla jednostki organizacyjne."* Zaprojektowana zgodnie z zaleceniami ABW i charakterystyką systemu Siecie Ti powinny określać klauzule tajności, w której informacje będą przetwarzane. Ponadto w dokumentach należy wskazać:

- Osoby odpowiedzialne za wdrażanie środków zapewniających bezpieczeństwo,
- Zadania osób odpowiedzialnych za bezpieczeństwo informacji niejawnych,
- Granice i lokalizacje stref kontrolowanego dostępu oraz środki ochrony,
- Środki ochrony kryptograficznej, elektromagnetycznej i technicznej
- Zasady zarządzania ryzykiem,
- Zasady szkolenia z zakresu bezpieczeństwa sieci Ti.[129]

Tak zaprojektowanych dokument SWB stanowi podstawę opracowania innego dokumentu *Procedury Bezpiecznej Eksploatacji.* Przeznaczenie dokumentu oraz sposób jego opracowania

[128] M. Ciecierski, *Ochrona Informacji niejawnych i biznesowych*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych, Uniwersytet Śląski w Katowicach, Materiały IV Kongresu, Wyd. Redakcja Naukowa Katowice 2008, s.81, 82.
[129] T. Szewc, *Publicznoprawna ochrona informacji*, Wyd. C.H. Beck, Warszawa 2007, s. 191.

i akredytacji określa ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych. Natomiast zakres informacji, które powinny znaleźć się w tym dokumencie określa Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego. Dla tych podmiotów, które podczas tworzenia systemów i sieci teleinformatycznych w swoich jednostkach organizacyjnych starają się o wydanie takiego dokumentu przez odpowiednie służby, którymi są Departament Bezpieczeństwa Teleinformatycznego ABW. Na tej podstawie określa się tryb postępowania w budowaniu systemu określonej klasyfikacji informacji niejawnej. Odpowiednie służby określają czas trwania takiej procedury. Tajemnica służbową można budować system po upływie 30 dni jeżeli w tym terminie SOP nie wniesie zastrzeżenia (art. 61 ust. 5 ustawy). Upływ tego terminu kończy procedurę dopuszczenia systemu do przetwarzania informacji niejawnych stanowiących tajemnicę służbową nazwaną *akredytacją bezpieczeństwa teleinformatycznego* wymagany dla systemów sieci, w których znajduje się tajemnica państwowa. Tu wdrożenie systemu nie będzie możliwe dopóki służby ochrony państwa nie zatwierdzają dokumentu. Jednakże uruchomienie systemu nastąpi dopiero z chwilą otrzymania *certyfikatu akredytacyjnego* dopuszczającego do tajemnicy państwowej. Kolejnym dokumentem certyfikującym na podstawie art. 19 ust. 3 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tekst jednolity Dz.U. z 2010 r. nr 29 poz. 154) oraz zarządzania nr 12 (DBTi ABW) § 1 zarządzenie określa zasady postępowania funkcjonariuszy i pracowników Jednostki Certyfikującej oraz Zespołów Badawczych Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego zwanej DBTi ABW podczas realizacji zadań, z których mowa w art. 60 ust. 3,4 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, zwanej dalej *ustawą,*[130]użyte w zarządzaniu określa oznaczają sposób, podstawowe pojęcie oraz osoby odpowiedzialne za wydawanie odpowiedniego dokumentu podmiotowi, który w systemie stosuje ochronę kryptograficzną, a wykorzystywane urządzenia podlegają certyfikacji. Na tej podstawie przeprowadza się badania i wydaje certyfikaty ochrony kryptograficzne. Wyżej wymienione czynności związane z uzyskaniem certyfikatów oraz akredytacji bezpieczeństwa teleinformatycznego i ochrony kryptograficznej ustawodawca określił jako element odpłatny. Na zasadach wskazanych w Rozporządzeniu Prezesa Rady Ministrów z dnia 30 września 2005 r. w sprawie wysokości opłat za przeprowadzanie przez służby ochrony państwa czynności z zakresu bezpieczeństwa teleinformatycznego (Dz.U. Nr 200 poz. 1652), jak również art. 63 ustawy z dnia 22 stycznia 1999 r., który mówi, że *„za przeprowadzenie czynności pobiera się opłaty”* tak opracowany dokument akredytacji i certyfikacji podlega jeszcze jednej regulacji prawnej dot. Decyzji administracyjnej w rozumieniu KPA ze wszystkimi tego konsekwencjami tzn. wymagania odpowiednie do prowadzenie postępowania (dotyczy w/w dokumentu), formy prawa do zaskarżania itp. Uzyskany dokument użytkownik danej sieci lub systemu powinien mieć udostępniany gdy będzie tego potrzebować.

Zabezpieczenia techniczne

Jednym z głównych czynników umożliwiających osiąganie zamierzonych celów działania w każdej jednostce organizacyjnej, administracyjnej, publicznej, intelektualnej itp.

[130] Zarządzenie nr 12 z dnia 20 lipca 2010 r. Szefa ABW w sprawie badań i certyfikacji urządzeń kryptograficznych i środków ochrony elektromagnetycznej, wykorzystywanych do ochrony informacji niejawnych, prowadzonych przez Departament Bezpieczeństwa Teleinformatycznego ABW.

jest prawidłowo i skutecznie działający system bezpieczeństwa informacyjnego. Dlatego zabezpieczenie systemu musi być procesem dynamicznym i ciągłym, gdyż tylko wtedy ma szansę dostosować się do niezwykle szybko zmieniających się zagrożeń. Posiadana informacja, a zwłaszcza informacja szczególnie chroniona może decydować o zachowaniu pozycji na rynku konkurencyjności tak uznanie zagrożeń bezpieczeństwa i obronności. Jest istotne z punktu widzenia bezpieczeństwa dotyczące całej struktury teleinformatycznej, a zwłaszcza systemów i sieci Ti przetwarzającej, przesyłającej dane dot. Różnego rodzaju tajemnic prawnie chronionych. Niezwykle ważnym elementem jest prawidłowy dobór zabezpieczenia różnego rodzaju środkami ochrony. Prawdopodobieństwo wystąpienia incydentów można zmniejszyć oporze stosowanie odpowiedniego sprzętu, urządzenia, oprogramowania itp. Zgodnie z zaleceniami ustawodawcy ar. 62 ust. 2 ustawy redaguje warunki dot. Wymagań w stosunku do systemów i sieci teleinformatycznych w zakresie ochrony. Natomiast rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. (Dz.U. Nr 171 poz. 1433 §14) określa zasady szczególnych wymagań bezpieczeństwa technicznego i organizacyjnego związanego z przetwarzaniem informacji w systemach sieciach teleinformatycznych. Dlatego tworząc bezpieczeństwo systemu i sieci należy skorzystać z pewnej zasady, która brzmi *„bezpieczeństwo całego systemu jest tak mocne jak jego najsłabszy element”* [131]

Dany sprzęt z jakim spotykamy się, na co dzień w domu, pracy jest różnorodny dlatego ochrona tego sprzętu powinna przeciwdziałać nie tylko zagrożeniu nieupoważnionego di stepu do informacji, ale również niebezpiecznym czynnikom mogącym wpływać na działanie urządzeń. Urządzenia przetwarzające dane powinny zostać umiejscowione w taki sposób by zminimalizować niepożądany dostęp do obszarów roboczych oraz ograniczyć do minimum brak nadzoru podczas ich używania. Administrator, inspektor wraz z odpowiedzialnym specjalistą od zabezpieczenia systemów i sieci powinien tak zaprojektować obszar, w którym znajdują się urządzenia, aby wykluczyć publiczny dostęp do nich. Tworząc taką strefę należy pamiętać również o urządzeniach pomocniczych takich jak drukarki sieciowe, kserokopiarki czy urządzenia faksowe, które należy również odpowiednio zabezpieczyć. Należy te przedmioty tak zlokalizować, aby znajdowały się w pomieszczeniu o ograniczonym dostępie. Dla tego typu urządzeń opracowano odpowiednie oznakowania, według literatury są to dwa rodzaje:

Nalepka naklejona w miejscu widocznym w sposób trwały, zabezpieczająca informacji i dotycząca numeru ewidencyjnego oraz inicjały użytkownika danej komórki organizacyjnej oraz odpowiedniej przyznanej klauzuli.

Naklejony w widocznym miejscu pasek w odpowiednim kolorze dopasowany do rodzaju klasyfikacji informacji: kolor czerwony- informacje o klauzuli *tajne,* żółty- do klauzuli *poufne,* niebieski- do klauzuli *zastrzeżone.* Natomiast elementy urządzeń pomocniczych powinny być oplombowane w taki sposób, aby modyfikacja danego sprzętu była niemożliwa bez naruszenia plomb. Następnym wątkiem, o którym również należy wspomnieć podczas planowania zabezpieczeń technicznych jest konserwacja sprzętu zainstalowanego do systemu i sieci przetwarzających informację niejawną, powinna być wykonana tylko w strefach bezpieczeństwa dostosowanych do klauzuli tajności przez osoby posiadające odpowiednie uprawnienia. W skład zabezpieczenia teleinformatycznego wchodzi również kontrola dostępu. Procedury dostępu służą do nadawania lub dobierania dostępu danego użytkownika dla zasobów informacyjnych. W zabezpieczeniach danego systemu

[131]A. Guzik, *Zagrożenia dla bezpieczeństwa informacji i ich identyfikacja*, [w:] Ochrona Mienia i Informacji, listopad/ grudzień 6/ 2009, s.9.

najczęściej stosuje się metodę uwierzytelnienia użytkowników nadania im identyfikatorów (niepowtarzalnych nazw lub numerów) i stosowanie haseł w odpowiednim stopniu skomplikowania (odpowiedniej długości, zestawienie użytych znaków liter i cyfr oraz znaków specjalnych).[132]Ochrona zabezpieczenia powinna przeciwdziałać nie tylko zagrożeniom nieupoważnionego dostępu do informacji, ale również niebezpiecznym czynnikom środowiskowym, które mogą wpływać na działanie urządzeń. Rozwiązaniem tej kwestii zabezpieczania jest system monitorowaniu, może on pomóc wykryć czynnik, który mógłby wpływać niekorzystnie na pracę urządzeń przetwarzających informacje lub spowodować ich awarię. Dla głębszego zastosowania zabezpieczenia lub bezpieczeństwa teleinformatycznego można wspomnieć o ochronie elektromagnetycznej polegającej na podsłuchu, dzięki któremu można uzyskać informacje poprzez odbiorniki radiowe. W obecnej globalizacji zdolności elektromagnetyczne posiada prawie każde urządzenie. Osoby odpowiedzialne za systemy i sieci teleinformatyczne wprowadzają ściśle kontrolowane strefy ochronne, korzystanie z monitorów plazmowych lub ciekłokrystalicznych. Bardzo ważnym elementem kontroli oraz zabezpieczenia jest ochrona nośników danych. Ten element powinien być zarejestrowany w odpowiednim dzienniku nośników elektronicznych. Należy też pamiętać, że najczęściej funkcje systemowe usuwające dane z nośników nie gwarantują 100% pewności, że danych tych nie da się ponowie odczytać. Dlatego w tym rozdziale o zabezpieczeniach technicznych warto również rozważyć fizyczne niszczenie wszystkich niepotrzebnych już urządzeń. Nośniki służące do przechowywania danych osobowych, które również podlegają zabezpieczeniu ze strony technicznej mają określony wymóg usunięcia z nich danych w sposób uniemożliwiający ich odzyskanie. Jest to uregulowane Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji, przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informacyjne do przetwarzania danych osobowych (Dz.U. z 204 r. Nr 100 poz. 1024). Oprócz wyżej wymienionych zabezpieczeń w literaturze można spotkać wiele różnych podziałów technicznych metod bezpieczeństwa. Zróżnicowane są ze względu na charakter ich działania i należą:

- Metody identyfikacyjne, mające na celu ograniczenie w sposób selektywny dostępu ludzi do tych elementów systemu, do których dostęp jest uzasadniony, a także ograniczenie dostępu nieupoważnionemu.
- Metody ograniczające, które stanowią barierę ograniczającą dostęp do systemów, dopuszczając do korzystania z nich po identyfikacji i uwierzytelnieniu zgodnie z posiadanym upoważnieniem do pracy w systemie.
- Metody alarmujące, tworzą cały zestaw środków konwencjonalnych. Specjalne zamki w drzwiach, urządzeniach, szafy pancerne, plomby, systemy alarmowe, urządzenia do rozpoznawania głosu, linii papilarnych, urządzeń kryptograficznych.[133]

Urządzenie służy do szyfrowania dostępu do informacji niejawnych. Stosuje się w celu utrudnienia przejęcia informacji poprzez ich przekształcenie. W sposób tylko znany osobie upoważnionej do tego typu ochrony urządzeń. Natomiast ochrona w systemie lub siec polega na stosowaniu metod, środków zabezpieczenia danej informacji prawem ochrony przez szyfrowanie oraz stosowania innych zasad kryptograficznych. Aby urządzenie to działało w sieci musi spełnić określone wymagania dot. bezpieczeństwa tzn. uzyskanie

[132] W. Dragoń, D. Mąka, *Skawina M., Jak chronić tajemnice? Ochrona informacji w instytucjach państwowych i przedsiębiorstwach prywatnych*, wyd. Bellona, Warszawa 2004, s. 139.
[133] tamże, s. 140.

odpowiedniego dokumentu czyli certyfikatu procedur bezpiecznej eksploatacji wydanego przez służby ochrony państwa. Technika kryptograficzna znajduje najszersze zastosowanie przy ochronie tajemnicy państwowej.

Dalsza część projektowania technicznego zabezpieczania sieci to ciągłość zachowania pracy w danej jednostce organizacyjnej poprzez zapewnienie ciągłości zasilania w energię elektryczną. W zależności od szacowanego ryzyka i poziomu ciągłości działania, który należy zapewnić możemy zastosować odpowiednie rozwiązania poprzez:

- zasilacze awaryjne (UPS)
- generator awaryjny
- zwielokrotnione linie zasilające w przypadku przerwy w dostawie energii elektrycznej.

Dlatego tego typu rozwiązanie ze strony technicznej ma na celu kontynuację pracy przez urządzenia służące przetwarzaniu informacji, ale również zapewnieniu działania oświetlenia i łączności. Następnym elementem tej układanki zabezpieczenia technicznego sieci i systemów TI jest zabezpieczenie komunikacyjnej. Wyposażenie jej, okablowanie powinno być chronione przed podsłuchem lub uszkodzeniem. Jeżeli jest to możliwe, to należy unikać tras biegnących przez obszary publiczne. Takie okablowanie powinno zostać poprowadzone pod ziemią, a punkty rozdzielcze sieci powinny znajdować się w zamkniętych skrzynkach teleinformatycznych. Dlatego w obecnej erze można zastosować okablowanie światłowodowe, które poprawia bezpieczeństwo.

Niezależnie od sposobu wytwarzania, przechowywania i udostępniania informacji jak również niezależnie od formy i sposobu ich wdrażania w jednostkach organizacyjnych i innych podmiotach do tego upoważnionych należy zawsze kierować się tymi samymi zasadami uregulowanymi prawnie. Dlatego procesy uświadamiające, szkolenia oraz edukacja w zakresie bezpieczeństwa powinny mieć charakter ciągły.

Zasady korzystania przez użytkownika

Świadomość to wiedza, która pozwala zidentyfikować zagrożenia i podjąć właściwe działania. Dlatego też należy się najpierw nauczyć, a następnie tę wiedzę wykorzystać[134]. Dlatego tak ważne jest wykorzystanie tej świadomości przez użytkowników danej jednostki decyzyjnej, w której to utworzono odpowiednie zabezpieczenia dot. informacji ustawowo chronionych, a odpowiedzialność za nie ponoszą pracownicy uprawnieni do dostępu i tworzący pion ochrony. To właśnie ich świadomość powinna być przykładem do prawidłowego i bezpiecznego korzystania z danego rodzaju urządzeń znajdujących się w odpowiednich strefach bezpieczeństwa. W tym etapie buduje się Politykę Bezpieczeństwa informacji, zasad korzystania z niej.[135] Pracownicy są często największym zagrożeniem dla bezpieczeństwa urządzeń przetwarzających informacje. Należy zatem przedstawić kolejne pojęcie tzn. *świadomy,* czyli będący na najwyższym poziomie rozwoju.[136] W tym przypadku może oznaczać zwiększenie bezpieczeństwa. Za świadomość bezpieczeństwa w danej komórce odpowiada kierownik jednostki organizacyjnej, a w przypadku omawianego tematu

[134] J. Grzechowiak, *Świadomość pracowników jako element kształtowania polityki bezpieczeństwa firmy*, [w:] *CSO Magazyn Zarządzający Bezpieczeństwem,* Grudzień 2006, Nr 4/06, s. 11.
[135] J. Depo, J. Piwowarski, *Bezpieczeństwo informacyjne. Informacje niejawne. Część pierwsza oraz część druga*, Kraków 2012, s. 83; J. Piwowarski, *Społeczeństwo informacyjne a kultura bezpieczeństwa*, [w:] „Zeszyt Naukowy Apeiron" WSBPiI w Krakowie, grudzień 2011, nr 6, s. 163.
[136] tamże, s. 12.

również pełnomocnik ds. ochrony, administrator systemu bezpieczeństwa, którzy są upoważnieni do przekazywania bezpiecznych zasad podczas korzystania z systemów i sieci teleinformatycznych. Każdy pracownik korzystający z komputerów oraz innego pomocniczego sprzętu w danej dziedzinie powinien odbyć odpowiednie przeszkolenie w zakresie bezpieczeństwa ochrony informacji, a przestrzegania zasad bezpieczeństwa dot. ochrony informacji niejawnej powinno być wpisane w zakres jego kompetencji. Analizując zagrożenia mogące przyczynić się do powstania sytuacji wyjątkowej, należałoby uwzględnić wiele czynników takich jak: Polityka *czystego biurka* pomaga zapobiegać ujawnieniu lub kradzieży informacji, rozsądek nakazujący nie zostawiać na wierzchu żadnych dokumentów, kiedy na pewien okres czasu tracimy kontrolę nad nimi, niepotrzebne w danym momencie dokumenty papierowe, nośniki danych, taśmy, należy bezwzględnie chować w zamykanych szafach, pod żadnym pozorem dokumenty i nośniki danych nie powinny pozostać niezabezpieczone po zakończeniu pracy- w razie włamania, pożaru lub stanu wyjątkowego mogłyby dostać się w niepowołane ręce lub zostać zniszczone.

Punktami, które należy szczególnie kontrolować są urządzenia pomocnicze takie jak drukarki sieciowe i kserokopiarki, to ich mechanizm dostarcza w postaci wytworzonego dokumentu sporo cennych informacji dla osób nieupoważnionych do wglądu w ten materiał. Dlatego każdy pracownik danej komórki lub pionu, w którym jest zatrudniony, a jeśli jest to pion ochrony, powinien zacząć traktować informacje jako cenny dokument danej *firmy*, powinien zabezpieczyć dokument natychmiast po wykonaniu przez urządzenie zleconego działania. Użytkownik danego systemu to potencjalny podmiot, który w określonych warunkach, z odpowiednim dostępem do sieci i systemu korzysta z niego. To na nim ciąży odpowiedzialność i lojalność w stosunku do urządzeń przetwarzających i przesyłających dane i odnosi się do serwerów oraz urządzeń przenośnych np. laptopów. Gdzie powinna obowiązywać zasada *czystego ekranu*- każdorazowe odejście od stanowiska pracy powinno zostać poprzedzone zablokowaniem klawiatury i włączeniem wygaszacza ekranu zabezpieczonego hasłem. Oczywiście nie musi to wymagać wykonania akcji ze strony użytkownika, może odbywać się to automatycznie pod warunkiem, że czas akcji zabezpieczenia jest wystarczająco krótki (należy tu dopasować go do klasyfikacji przetwarzanych danych lub innych informacji i ryzyka ich utraty). Użytkownik korzystając z urządzeń przenośnych; laptopów, palmtopów, telefonów komórkowych w miejscach publicznych i innych niechronionych wymaga ostrożności, by nie ujawnić osobom nieupoważnionym cennej informacji. Urządzenia oraz nośniki danych zabierane z danej komórki nie powinny być bez nadzoru w miejscach publicznych. Zaleca się natychmiast przewożenie komputerów przenośnych jako bagażu podręcznego, nie należy pozostawiać dokumentów, nośników danych i sprzętu w hotelach ani w samochodzie bez kontroli. Użytkownik sprzętu przenośnego, na którym przechowuje się informacje powinien zapoznać się również z zaleceniami dot. ochrony sprzętu przed działaniem silnego pola elektromagnetycznego, które to może spowodować uszkodzenie danego urządzenia. Użytkownicy systemów i sieci teleinformatycznych, którzy korzystają z urządzeń objętych odpowiednimi dokumentami powinni zwracać szczególną uwagę na stan bezpieczeństwa miejsca pracy. Dotyczy to przede wszystkim ekranu monitora, który powinien być tu odpowiednio ustawiony, aby ograniczał możliwość odczytu z ekranu przez podmioty nieuprawnione, czyli osoby postronne. Dany użytkownik systemu ma obowiązek zachowania tajemnicy haseł i identyfikatorów osobistych jak również przestrzegania udostępniania ich innym osobom. Użytkownik znajdujący się w strefie o odpowiednich umowach dotyczących bezpieczeństwa powinien również znać ogólne zasady dot. codziennej pracy. Potencjalny pracownik, który nawet na chwilę opuszcza pokój powinien zamknąć go na klucz, a po

zakończeniu pracy dokumenty, komputer, nośniki danych powinny być przechowywane w zamkniętych zabezpieczonych, ognioodpornych szafach. Natomiast na zakończenie pracy należy zamknąć aktywne sesje oraz wyrejestrować się z serwerów lub też można zastosować oprogramowanie blokujące klawiaturę i wygaszacz ekranu z hasłem tylko dostępnym danemu użytkownikowi.

Cała wyżej wymieniona struktura to szereg zasad, które powinny odpowiadać za prawidłowe bezpieczeństwo sieci, być respektowane przez użytkowników danego systemu bezwzględnie. Na podział dotyczący stref bezpieczeństwa, ochrony czy zwykłego korzystania ze sprzętu przez potencjalnego użytkownika. Ale niestety duża cześć naszych przyzwyczajeń, dróg na skróty i uproszczeń powoduje narażenie danego podmiotu, jednostki organizacyjnej, instytucji lub sektora publicznego na utratę informacji. Aby ww. punkty zostały prawidłowo wyjaśnione należy sobie uświadomić, że dbałość o bezpieczeństwo musi stać się codziennym

elementem pracy owych setek działań nieuregulowanych w procedurach i wewnętrznych przepisach informacyjnych kontaktów i spotkań- tego, co tworzy kulturę organizacji. Należy określić jedną regułę. Bezpieczeństwo musi zamieszkać w podświadomości.[137]

[137]M. Jaworski, *Pierwszy krok do ochrony informacji*, [w:] *CSO magazyn zarządzających biznesem*, Czerwiec 2006 nr 2/2006, s. 14.

Bibliografia

1. Ciecierski M., *Ochrona Informacji niejawnych i biznesowych*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych, Uniwersytet Śląski w Katowicach, Materiały IV Kongresu, Wyd. Redakcja Naukowa Katowice 2008.
2. Depo J., Piwowarski J., *Bezpieczeństwo informacyjne. Informacje niejawne. Część pierwsza oraz część druga*, Kraków 2012.
3. Dragoń W., Mąka D*., Skawina M., Jak chronić tajemnice? Ochrona informacji w instytucjach państwowych i przedsiębiorstwach prywatnych*, wyd. Bellona, Warszawa 2004.
4. Dragoń W., Mąka D*., Skawina M., Jak chronić tajemnice? Ochrona informacji w instytucjach państwowych i przedsiębiorstwach prywatnych*, wyd. Bellona, Warszawa 2004.
5. Guzik A., Zagrożenia dla bezpieczeństwa informacji i ich identyfikacja, [w:] Ochrona Mienia i Informacji, listopad/ grudzień 6/ 2009.
6. Jaworski M., *Pierwszy krok do ochrony informacji*, [w:] *CSO magazyn zarządzających biznesem*, Czerwiec 2006 nr 2/2006.
7. Piwowarski J., *Bezpieczeństwo jako pożądany stan oraz jako wartość*, [w:] *Bezpieczeństwo jako wartość*, „Wydanie pokonferencyjne z II Konferencji Naukowej z cyklu „Bezpieczeństwo jako wartość" zorganizowanej przez Wyższą Szkołę Bezpieczeństwa Publicznego i Indywidualnego „Apeiron" w Krakowie, 18 kwietnia 2008", Kraków 2010.
8. Piwowarski J., *Społeczeństwo informacyjne a kultura bezpieczeństwa*, [w:] „Zeszyt Naukowy Apeiron" WSBPiI w Krakowie, grudzień 2011, nr 6.
9. Szewc T., *Publicznoprawna ochrona informacji*, Wyd. C.H. Beck, Warszawa 2007.