FRĄCZEK Mariusz[1]

Zagrożenia i bezpieczeństwo informacji w sieciach teleinformatycznych logistyki

WSTĘP

Współczesna logistyka ma wiele twarzy i jest obszarem rozważań w gronie ekspertów łączących doświadczenia teoretyczne z praktyką, stanowi dyscyplinę naukową[2] i obejmuje planowanie i przygotowanie realizacji dostaw zaopatrzenia oraz świadczeniu usług niezbędnych we wszystkich obszarach gospodarki, stanowi również dziedzinę wiedzy o procesie zarządzania łańcuchem dostaw[3].

Dynamiczny rozwój technologii informacyjnych ma coraz większy wpływ na wszystkie aspekty życia człowieka. Komputer jest urządzeniem, które stało się ogólnodostępne, a możliwość gromadzenia, przetwarzania oraz przekazywania różnych informacji powoduje, iż wzrasta ilość oferowanych przy jego udziale usług. Ma to również odzwierciedlenie w szeroko rozumianej logistyce, która obszarem swoich zainteresowań obejmuje między innymi transport, zarządzanie łańcuchami dostaw, organizację i zarządzanie różnymi centrami logistycznymi, prowadzenie działalności logistycznej poprzez sieci komputerowe (e-logistyka), zarządzanie dystrybucją oraz magazynowaniem, modelowanie systemów logistycznych, wdrażanie platform informatycznych dla logistyki, czy chociażby automatyczną identyfikację produktów. Dostępna literatura przedmiotu w szczególności podkreśla jej ukierunkowanie na racjonalne działanie, które należy postrzegać zarówno w sferze pracy koncepcyjnej (zarządzanie), jak i w sferze praktycznej, czyli realizacji szeregu prac, zadań i przedsięwzięć stanowiących działalność logistyczną.

Doświadczenia zawodowe autora wskazują, że jednym z warunków prawidłowego funkcjonowania logistyki jest stosowanie nowoczesnych urządzeń i narzędzi służących do komunikacji. Telefon (stacjonarny, komórkowy, satelitarny) jest obok komputera drugim najważniejszym środkiem decydującym o szybkości realizacji zamówień klienta lub wykonania usługi. To z kolei przekłada się na wzrost efektywności procesów logistycznych we wszystkich organizacjach oraz szczeblach. Warunkiem ciągłego rozwoju jest posiadanie dostępu do wiarygodnej oraz aktualnej informacji. Można zatem przyjąć, iż powszechne użycie urządzeń komputerowych do procesów informacyjnych stworzyło zupełnie nową jakość. Stanowi także fundament budowy infrastruktury logistycznego systemu informacji LIS (*ang. Logistics Information System*), którego podstawowe elementy to:

a) technika elektronicznej wymiany dokumentacji - EDI (*ang. Electronic Data Interchange*);
b) technika automatycznej identyfikacji - AI (*ang. Automatic Identification*);
c) stacjonarna infrastruktura telekomunikacyjna;
d) systemy łączności mobilnej (w tym komórkowej GSM oraz satelitarnej);
e) system nawigacji obiektów ruchomych GPS (*ang. Global Positioning System*).

W ocenie autora, warto zwrócić uwagę na postępujący wzrost wszelkich procesów informacyjnych w logistyce, gdzie sprawny przepływ towarów warunkuje:

1. Zbieranie, weryfikowanie i gromadzenie informacji wejściowej.
2. Selekcję, przetwarzanie i zobrazowanie informacji.
3. Dystrybucję i edycję informacji planistycznej oraz wykonawczej.

[1] dr inż. Mariusz FRĄCZEK, adiunkt w Zakładzie Teleinformatyki i Bezpieczeństwa Cyberprzestrzeni, Instytut Dowodzenia, Wydział Zarządzania i Dowodzenia, Akademia Obrony Narodowej, Warszawa, al. Gen. Chruściela 103, 00-910, Warszawa, tel.: 226-813-331, e-mail: m.fraczek@aon.edu.pl.

[2] Badania naukowe w logistyce koncentrują się na planowaniu, przygotowaniu, użyciu i przepływie przedmiotów, osób, energii, informacji i usług w celu osiągnięcia pożądanych korzyści.

[3] Łańcuch dostaw (łańcuch logistyczny) to proces wytwarzania i dystrybucji dóbr, czyli działalność związana z przepływem towaru, poczynając od źródła surowców, poprzez wszystkie fazy ich przetwarzania, aż do postaci, w której dany towar jest dostarczany do konsumentów.

Podobnie, jak w wielu innych dziedzinach, aktualna informacja przekazywana w czasie rzeczywistym stanowi fundament działania logistyki, jednakże na podkreślenie zasługuje, iż można w niej wyróżnić wiadomości (dane) świadczące o jej odrębności do których należą:

a) baza indeksowa (indeksy materiałowe, kody i adresy dostawców i odbiorców, kody operacji finansowych i inne),
b) baza normatywna logistyki zaopatrzenia (normy i wskaźniki zużycia, normy zapasów materiałowych, wykazy asortymentów zaopatrzeniowych, wykazy dostawców itp.);
c) baza katalogowa (katalogi i cenniki materiałów, oferty handlowe, prospekty i informatory itp.).

Zdaniem autora, w wzajemnych korelacjach gospodarczych trudno sobie obecnie wyobrazić przepływ towarów i realizację usług logistycznych na skalę mikro, regionu czy też globalną bez zastosowania sieci komputerowych. Dziś logistyka wsparta jest i coraz częściej funkcjonuje w oparciu o techniki informatyczne, dostęp do sieci Internet oraz zdolność do przekazywania przy ich pomocy różnorodnych danych. Warto jednak pamiętać, iż nie da się rozwijać działalności logistycznej opartej wyłącznie na sieci informatycznej bez infrastruktury telekomunikacyjnej (rozumianej potocznie wyłącznie poprzez usługi telefoniczne).

1. IDENTYFIKACJA CZYNNIKÓW MAJĄCYCH WPŁYW NA OCHRONĘ INFORMACJI W LOGISTYCE

Eksploatacja sieci informatycznych dla logistyki związana jest z koniecznością zapewnienia im odpowiedniego do potrzeb danej organizacji poziomu ochrony. Powinien on być dostosowany do ważności gromadzonych, przetwarzanych oraz wymienianych informacji. Funkcjonowanie systemów komputerowych w logistyce zależy od wielu czynników, które determinują organizację pracy oraz realizację wdrożonych rozwiązań. Przekłada się to również na poziom bezpieczeństwa wymiany informacji, a największego znaczenia nabiera określenie do jakiego celu dany system został dedykowany i co dzięki niemu zostanie usprawnione. Stąd też być może wynika różnorodność systemów informatycznych dedykowanych dla logistyki (np. systemy typu: ERP, MRP, CRM, EDI, B2C, B2B oraz WMS). To pozwala na spełnianie różnych oczekiwań ich użytkowników. Wydaje się także oczywiste, że ich zastosowanie jest odmienne dla małej firmy transportowej, a zupełnie inaczej taka sieć powinna być zbudowana dla potrzeb dystrybucji i zaopatrywania w szeroką gamę asortymentów sieci hipermarketów czy też korporacji przemysłowych. Powyższe stanowi odzwierciedlenie heterogeniczności stosowanych rozwiązań czego najlepszym przykładem jest zapewnienie potrzeb sił zbrojnych czy też instytucji i organów podległych Ministerstwu Spraw Wewnętrznych, a więc odpowiedzialnych za bezpieczeństwo państwa i jego obywateli. W wyżej wymienionym kontekście ważne staje się udzielenie odpowiedzi na pytanie, **jakie są potrzeby budowy lub wdrożenia systemu informatycznego dla logistyki i jakie powinien on spełnić wymagania (oczekiwania)?**

Organizacja każdego systemu teleinformatycznego nierozerwalnie związana jest z budową infrastruktury, która będzie miała zasadnicze znaczenie dla wymiany informacji. Zatem można przyjąć, że wymagania stawiane ochronie informacji w logistyce pośrednio odnoszą się wyłącznie do sieci komputerowych, a także rozpoznanych oraz przewidywanych zagrożeń. Nie mniejszą rolę do spełnienia będą miały użyte systemy komunikacji mobilnej. Jednakże należy mieć na uwadze, iż druga grupa urządzeń oraz środków statystycznie jest mniej narażona na różnego rodzaju ataki mogące powodować istotne zakłócenia lub przerwy w funkcjonowaniu logistyki. Powyższe powoduje zatem naturalną konieczność ogólnego wyjaśnienia pojęć: „wymagania" oraz „zagrożenie".

Słownik języka polskiego[4] pojęcie „wymaganie" definiuje, że jest to *„norma, warunek lub zespół warunków, którym ktoś lub coś musi odpowiadać"*. „Wymaganie" charakteryzowane jest również jako *„norma, warunek lub zespół warunków, którym ktoś lub coś musi odpowiadać; postulat, żądanie"*[5], a także rozumiane poprzez jego synonimy, takie jak: *„żądanie, domaganie się, postulowanie,*

[4] M. Szymczak (red. naukowa), S*łownik języka polskiego,* tom III, PWN, Warszawa 1992, s. 818.
[5] M. Szymczak (red. naukowa), S*łownik …*, op. cit., s. 818.

roszczenie, wola, życzenie, dyrektywa, postulat, sugestia, wskazanie, zalecenie, warunek, ultimatum, wymóg, zastrzeżenie, obligatoryjność, konieczność, potrzeba, przymus"[6].

Termin „**zagrożenie"** pochodzi od czasownika ***grozić*** - *„stwarzać stan niebezpieczeństwa, być niebezpiecznym, zagrażać,* natomiast groźba oznacza *zapowiedź niebezpieczeństwa, kary, zemsty, pogróżka"*[7], *„rzeczownik od zagrozić, sytuacja lub stan, które komuś czymś zagrażają lub w których ktoś czuje się zagrożony, także ktoś stwarza taką sytuację"*[8], a także definiowana jest jako „*sytuacja będąca sygnałem czegoś, co może nastąpić, zwykle złego, niepożądanego lub niebezpiecznego"*[9]. Synonimem słowa zagrożenie są takie pojęcia, jak[10]: „*niebezpieczeństwo, groźba, ryzyko, niepewność, niepokój, niestabilność, obawa".* Pojęcie **„zagrożenie"** w odniesieniu do sieci komputerowej (systemu informatycznego) zostało zdefiniowane przez K. Lidermana[11] jako: *„potencjalne naruszenie zabezpieczenia systemu informatycznego"* oraz *„podatność (ang. vulnerability) to wada lub luka w strukturze fizycznej, organizacji, procedurach, personelu, zarządzaniu, administrowaniu, sprzęcie lub oprogramowaniu, która może być wykorzystana do spowodowania szkód w systemie informatycznym lub działalności człowieka".*

Obserwacje bezpośrednie autora wskazują, iż zapewnienie bezpieczeństwa poszczególnym sieciom informatycznym w logistyce nie ma charakteru stałego oraz nie wszędzie stanowi fundament ich funkcjonowania. Jest uzależniona od kilku czynników, do których zaliczono:

a) charakter działalności logistycznej (prywatny/ instytucjonalny/ zorganizowany w większą całość);
b) znaczenie informacji przechowywanych w jej zasobach (najczęściej ściśle określonych bazach danych) oraz kosztów poniesionych strat z tego tytułu;
c) określenie czy zbudowana sieć komputerowa dla danego podmiotu posiada fizyczne połączenie z siecią globalną Internet[12], czy też jest to tzw. „system zamknięty" eksploatowany wyłącznie wewnątrz przedsiębiorstwa (firmy[13]/ w wojsku, policji itp.);
d) kto i na jakich zasadach ma dostęp do zgromadzonych zasobów informacyjnych (w tym także niejawnych lub decydujących o kluczowym rozwoju danej organizacji).

Warto też zauważyć, iż przedsiębiorstwa oraz instytucje wykonujące zadania lub projekty związane z bezpieczeństwem i obronnością państwa powinny posiadać odpowiednio chronione pomieszczenia (kancelarie), w których mogą być przetwarzane informacje klasyfikowane. Praktyka wskazuje, iż w logistyce także dokonuje się oceny wartości informacji oraz określa, które z nich powinny być chronione oraz w jakim zakresie. Podstawę wprowadzenia form, sposobów i skuteczności mechanizmów ochrony informacji uzależniono od kategorii jej ważności, a także wyrażono zgodę na stosowanie przyjętych rozwiązań w myśl *Ustawy o ochronie informacji niejawnych*[14]. Zgodnie z tym aktem prawnym informacje dzieli się ze względu na charakter ich ważności dla państwa, różnych instytucji (w tym sił zbrojnych), firm oraz osób prywatnych (patrz rozdział drugi ustawy).

Autor jest zdania, że literatura przedmiotu jednoznacznie nie wskazuje na to, które zagrożenia będą stanowiły największe niebezpieczeństwo dla eksploatowanej sieci komputerowej, bowiem wszystko jest uzależnione od jej wielkości i charakteru działania, jak również ważności przekazywanych poprzez nie informacji. Wobec powyższego celowym jest wskazanie ogólnego podziału zagrożeń na następujące kategorie:

I. Zagrożenia zewnętrzne - mają miejsce wówczas, gdy może dojść do zagrożeń utraty lub uszkodzenia danych, braku możliwości obsługi sieci informatycznej, w wyniku celowego lub przypadkowego działania ze strony osób nieuprawnionych, działających od zewnątrz w odniesieniu

[6] P. Żmigrodzki, *Słownik synonimów i antonimów,* wyd. EUROPA, Wrocław 2007, wyd. 2, s. 407.
[7] *Słownik współczesnego Języka Polskiego*, wyd. WILGA, Warszawa 1999, tom I, s. 701.
[8] *Uniwersalny Słownik Języka Polskiego,* PWN, Warszawa 2003, tom V, s. 460.
[9] A. Markowski, *Nowy Słownik Poprawnej Polszczyzny,* PWN, Warszawa 1999, s. 1277.
[10] Żmigrodzki P., *Słownik synonimów...,* op. cit., s. 421.
[11] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008. s. 40.
[12] Charakterystyka takich zagrożeń znajduje się w dostępnej literaturze, a także w wyspecjalizowanych periodykach dotyczących sieci komputerowych. Jeśli sieć komputerowa jest połączona z Internetem, to jest narażona na próby naruszenia spójności poprzez powszechnie znane zagrożenia mogące mieć miejsce (np.: włamania, wirusy, trojany, ataki typu DoS, szpiegostwo przemysłowe, uszkodzenie lub modyfikacja baz danych, zmiany w sterowaniu siecią) oraz takie, które dotychczas nie zostały rozpoznane.
[13] Mogą to być np. nowoczesne projekty lub rozwiązania techniczne, czy też składniki i receptury leków lub kosmetyków.
[14] *Ustawa o ochronie informacji niejawnych* z dnia 5 sierpnia 2010 r. Dz.U.10.18.1228.

do danej sieci. Wśród zagrożeń zewnętrznych, będących skutkiem celowego lub nieumyślnego oddziaływania człowieka wyszczególnia się:

a) niepokoje społeczne:
b) katastrofy przemysłowe:
c) ataki terrorystyczne;
d) łamanie zasad klasyfikowania informacji i ich przekazywanie poprzez sieci jawne;
e) zaniedbania lub zaniechanie działań mających wpływ na sprawność techniczną użytkowanego sprzętu, organizację, gromadzenie, jak również klasyfikację dokumentów podlegających zniszczeniu (m.in.: notatki, brudnopisy, maszynopisy).
f) utratę lub zniekształcenie danych poprzez wadliwą pracę urządzeń lub oprogramowania; zmiany w zdalnym sterowaniu sieciami (zmiana zabezpieczeń, konfiguracji, uprawnień dostępu, brak możliwości zarządzania lub sterowania siecią informatyczną).

II. Zagrożenia wewnętrzne występują wówczas, „*gdy zachodzi lub zaszła możliwość utraty lub uszkodzenia danych, utrata możliwości obsługi sieci teleinformatycznej, w wyniku celowego bądź przypadkowego działania ze strony osób nieuprawnionych działających w zewnętrznym otoczeniu sieci*”[15]. W przypadku zagrożeń wewnętrznych literatura przedmiotu wskazuje, iż mogą one być np. skutkiem *„zniszczenia danych spowodowanego błędami w oprogramowaniu systemowym, użytkowym lub wprowadzeniem oprogramowania złośliwego”*[16].

Zagrożenia wewnętrzne ochrony informacji w sieci komputerowej logistyki mogą mieć miejsce na każdym stanowisku pracy. Ich występowanie lub brak ściśle powiązany jest z osobami posiadającymi do nich dostęp (personel/ administrator). Są związane z procesem ustawicznego gromadzenia, analizy i przetwarzania różnych postaci danych, a także zwiększających się możliwości ich przekazania innym uprawnionym użytkownikom. Mogą być również skutkiem braku nadzoru nad dokumentacją techniczną systemu (zwłaszcza jego organizacji i lokalizacji). Zagrożenia te mogą powstawać już na etapie niewłaściwego projektowania i budowy sieci komputerowej w określonej lokalizacji, a jeśli jest ich więcej niż jedna, to także pomiędzy nimi.

Literatura przedmiotu pozwala stwierdzić, że nie wszystkie niebezpieczeństwa związane z funkcjonowaniem sieci komputerowej można jednoznacznie przypisać do jednego z powyżej wskazanych zagrożeń. Mogą bowiem wystąpić takie, które można przypisać do co najmniej dwóch, a do głównych z nich zaliczono:

a) kradzieże sprzętu i urządzeń lub ich celowe niszczenie (w tym ich oprogramowania);
b) dostęp osób nieuprawnionych do danych (przeglądanie, kopiowanie, przypadkowe lub celowe - np.: nieautoryzowany serwis, szpiegostwo gospodarcze) oraz ich przekazywanie poza sieć lub system informatyczny;
c) celowe uszkodzenie lub niszczenie danych.

III. Zagrożenia fizyczne występują nieodłącznie w powiązaniu z niszczeniem infrastruktury sieci, urządzeń bądź samych obiektów, w których poszczególne elementy sieci są zainstalowane (celowe działania człowieka lub skutki klęski żywiołowej).

Dostępna literatura przedmiotu wskazuje także na **atrybuty**[17] **decydujące o bezpieczeństwie informacji** w sieciach oraz systemach informatycznych. Są to:

1. Utrata poufności - definiowana jako nieautoryzowane ujawnienie informacji przez nieuprawniony dostęp do sieci lub systemu informatycznego. Utrata poufności może być spowodowana poprzez: pokonanie zabezpieczeń fizycznych lub programowych, niekontrolowany dostęp osób nieuprawnionych, kradzież informacji, nieautoryzowany serwis, podsłuch lub podgląd, jak również elektromagnetyczną emisję ujawniającą.

---

[15] J. Janczak, G. Świdzikowski, *Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym*, Warszawa AON, 2004, s. 16.

[16] **oprogramowanie „złośliwe”** - *„synonimy: wirus komputerowy, złośliwy program, wirus klasyczny; program lub kod zdolny do przenikania do systemów, dysków lub indywidualnych plików, zazwyczaj bez wiedzy i zgody użytkownika. Po skutecznej infekcji dalsze działanie zależy od określonego typu wirusa i obejmuje: replikację jedynie w zainfekowanym systemie; infekcję dalszych plików podczas ich uruchamiania lub tworzenia; kasowanie lub uszkadzanie danych w systemach i plikach - marnowanie zasobów systemowych bez powodowania szkód. Termin program złośliwy obejmuje wirusy klasyczne, robaki, konie trojańskie i inne szkodnik*”. Źródło: B. Lent (redakcja naukowa), *Bezpieczeństwo w telekomunikacji i teleinformatyce*, tom 3, Biblioteka Bezpieczeństwa Narodowego, Warszawa 2007, Słownik terminów, s. 171.

[17] Por. K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008; Liderman K., *Podręcznik administratora bezpieczeństwa teleinformatycznego*, Warszawa 2003.

2. **Utrata integralności** - rozumiana jako nieautoryzowana modyfikacja informacji oraz utrata prawidłowego i spójnego działania zasobów obliczeniowych. Czynniki mogące spowodować utratę integralności to: uszkodzenie systemu operacyjnego lub użytkowego, a także urządzeń, modyfikacja baz danych, infekcje wirusowe.
3. **Utrata dostępności** - pod pojęciem utrata dostępności rozumie się odmowę autoryzowanego dostępu lub opóźnienie operacji krytycznych pod względem czasu lub celu w wyniku wadliwego działania oprogramowania lub urządzeń, celowego lub nieumyślnego wprowadzenia wirusa do sieci komputerowej oraz brak zasilania.

W opinii autora na podkreślenie zasługuje, iż organa bezpieczeństwa teleinformatycznego państwa (Agencja Bezpieczeństwa Wewnętrznego oraz Służba Kontrwywiadu Wojskowego) szczególną uwagę przywiązują do podatności na zagrożenia oraz określenie standardów bezpieczeństwa dla danej sieci, jeśli jej użycie ma charakter niejawny. W przypadku podatności na przewidywane groźby wciąż poszukuje się oraz określa czynniki i zjawiska mające wpływ na zagrożenie ochrony informacji.

K. Liderman wskazuje, że zagrożenia które mogą być identyfikowane w związku z funkcjonowaniem sieci komputerowej, chociaż nie rzadko występują pod różnym nazewnictwem, są znane ich użytkownikom, a do podstawowych klas zagrożeń bezpieczeństwa informacji powinno się zaliczać[18]:

1. ***„Siły wyższe*** *(np. klęski żywiołowe, katastrofy finansowe, zmiany prawa)”.*
2. ***„Działania przestępcze (Nieuprawnione i przestępcze działania ludzi)”.***
3. ***„Błędy personelu*** *obsługującego system komputerowy”.*
4. ***„Skutki złej organizacji pracy*** *- np. brak jasno sprecyzowanych zakresów odpowiedzialności, nieprzestrzeganie i/lub brak odpowiednich przepisów itd. (zagrożenia związane z błędami ochronie fizycznej, możliwość utraty dostępności, integralności i poufności)”.*
5. ***„Awarie sprzętu i wady oprogramowania (Awarie i uszkodzenia sprzętu oraz wady oprogramowania)”.***

Należy podkreślić, że przedstawione obszary zagrożeń powinno się traktować jako ogólne wskazówki, natomiast ich rozpatrywanie w kontekście konkretnej sieci informatycznej jest równoznaczne z identyfikacją pojedynczych lub też całych grup potencjalnych i realnych gróźb. Minimalne standardy bezpieczeństwa osiąga się poprzez realizację założeń przedstawionych w dokumentach prawnych (ustawy, rozporządzenia) oraz innych, takich jak instrukcje, wytyczne oraz rozkazy (np. policja, wojsko), w których przyjęto określone wymagania dla zapewnienia oczekiwanego poziomu bezpieczeństwa systemu lub sieci. Są one coraz częściej są wdrażane nie tylko w resortach związanych z obronnością, ale także w różnego rodzaju państwowych i prywatnych podmiotach gospodarczych.

Analiza dostępnej literatury pozwala autorowi na refleksję, iż rozpatrując kwestię zagrożeń dla informacji kluczowych dla niezakłóconego funkcjonowania logistyki, nie można ogólnie nie odnieść się do niebezpieczeństw wynikających z powszechnego użytkowania różnorodnych urządzeń przeznaczonych do komunikacji mobilnej. Wśród najbardziej znanych wymienia się przekazywanie wiadomości przy pomocy radia CB (*ang. Citizen Band*), wcześniej wspominanego systemu telefonii komórkowej GSM, rzadziej telefonów satelitarnych, a także korzystanie z odbiorników GPS:

1. **Radia CB** - zasadniczo są przeznaczone do wzajemnego komunikowania się pomiędzy kierowcami wszelkich pojazdów, którzy posiadają urządzenia nadawczo-odbiorcze. Średni zasięg wynosi od 3-7 km. Najczęściej na ogólnodostępnym w Polsce kanale nr 19 przekazywane są ostrzeżenia o sytuacji na drodze, różnorodne komunikaty oraz prośby o pomoc. W logistyce używane przede wszystkim przez kierowców różnych pojazdów dostawczych oraz ciężarowych.
2. **Telefonia GSM** - najbardziej rozpowszechniony system mobilnej komunikacji telefonicznej, który umożliwia łączność ze wszystkimi posiadaczami urządzeń końcowych. W logistyce służy głównie do prowadzenia rozmów pomiędzy menadżerami różnych szczebli, jak również do komunikacji z wszelkimi innymi osobami mogącymi decydować o realizacji usług logistycznych.

[18] Por. K. Liderman, *Podręcznik administratora...,* op. cit., s. 179-180, K. Liderman, *Analiza ryzyka...*, op. cit., s. 42.

3. **Łączność satelitarna** - podobnie jak systemy GSM, służy do zapewnienia łączności z osobami, które nie posiadają dostępu do telefonii komórkowej. Ze względu duże koszty połączeń jest rzadko stosowana w transporcie kołowym, ale za to powszechna dla transportu lotniczego i morskiego.
4. **Odbiorniki GPS** - pozwalają na ustalenie położenia środków transportu, powszechnie użytkowane w transporcie kołowym. Pozwalają także na odnalezienie punktu docelowego podróży, dodatkowo wskazują na prędkość przemieszczania się danego pojazdu.

W opinii autora, możliwość niezakłóconego zakupu oraz eksploatacji ww. środków przez osoby prywatne oraz różne organizacje, powoduje brak poczucia zagrożeń dla ich funkcjonowania. Warto jednak pochylić się nad problemem, który znalazłby swoje odzwierciedlenie w realizacji zadań logistycznych w przypadku braku możliwości korzystania z urządzeń telekomunikacyjnych ze względu na ich destrukcję, czy co gorsza - wprowadzenie zmian w ich oprogramowaniu mogącym skutkować licznymi katastrofami w ruchu lądowym, morskim i powietrznym, a także brakiem technicznych zdolności do porozumiewania się. Wbrew różnym opiniom, jest to scenariusz, który może mieć miejsce, natomiast prawdopodobieństwo jego wystąpienia wydaje się być mniejsze niż konieczność dbałości o zasoby informacji zgromadzone w systemach komputerowych. Stąd też, według autora, istotnym jest wskazanie na podstawowe organizacyjno-techniczne środki ochrony informacji dla potrzeb logistyki.

2. ORGANIZACYJNE ŚRODKI OCHRONY INFORMACJI W LOGISTYCE

Organizacyjne środki ochrony informacji dla sieci teleinformatycznej są czynnościami wykonywanymi w celu zmniejszania mogących mieć miejsce różnorodnych zagrożeń Ich realizacja bezpośrednio wpływa na funkcjonowanie nie tylko pojedynczych stanowisk pracy, ale całości systemu logistycznego. Są obok przedsięwzięć ochrony technicznej jednym z fundamentów systemu bezpieczeństwa. Środki te mają na celu wzmocnić istniejący stan bezpieczeństwa gromadzonych, przetwarzanych i przekazywanych informacji wynikający z przewidywanych zagrożeń oraz zdolności i możliwości technicznych eksploatowanych urządzeń i środków. Ich zastosowanie nabiera szczególnego znaczenia w aspekcie spełnienia oczekiwań ochrony wiadomości i danych klasyfikowanych w myśl *Ustawy o ochronie informacji niejawnych* lub decydujących o rozwoju danego przedsiębiorstwa (firmy). Organizacyjne środki ochrony informacji powinny być ważnym ogniwem stworzonego systemu bezpieczeństwa. Ich zaplanowanie oraz wdrożenie do realizacji powinno gwarantować wymagany poziom ochrony wszystkich wiadomości, które mogą być istotne dla logistyki.

Do kompletu przedsięwzięć, których realizacja pozwoli na odpowiednią do potrzeb ochronę przede wszystkim sieci informatycznych powinno się zaliczać:

a) zapewnienie, stosownego do wymagań oraz potrzeb szefa (dyrektora, kierownika jednostki administracyjnej) administratora i użytkowników - **bezpieczeństwa osobowego;**
b) **ochronę źródeł informacji** związanych z pracą danego systemu informatycznego;
c) **kontrole dostępu** do wiadomości niejawnych (a także patentów, receptur, projektów, baz danych);
d) **zarządzanie ochroną sieci lub systemu informatycznego**;
e) **kontrolę ochrony wymiany informacji**.

W świetle obowiązujących dokumentów normatywnych, za gromadzenie, wytwarzanie, przetwarzanie i przekazywanie oraz za ochronę informacji niejawnych odpowiada kierownik jednostki organizacyjnej[19], w której to następuje. Odnosi się to także do bezpieczeństwa wymiany informacji przy udziale sieci teleinformatycznych (w tym komputerowych). Analiza sposobu spełniania tego wymagania wskazuje, że każdy kierownik jednostki organizacyjnej chcąc realizować ten wymóg powinien:

a) w zakresie ogólnej ochrony informacji klasyfikowanych - wyznaczyć lub zatrudnić pełnomocnika ds. ochrony informacji niejawnych (personel kancelarii tajnej);
b) wyznaczyć lub zatrudnić osoby odpowiedzialne za organizację bezpieczeństwa wymiany informacji w sieci komputerowej.

[19] *Ustawa o ochronie informacji niejawnych...*, op. cit., Rozdział III, art. 14.

Pełnomocnik ds. ochrony informacji niejawnej odpowiada m.in. za zorganizowanie systemu ochrony danego obiektu (lokalizacji), wyznaczenie stref ochronnych, systemu dostępu do informacji, jak również zorganizowanie ochrony fizycznej.

2.1. Bezpieczeństwo osobowe

Bezpieczeństwo osobowe nazywane jest często bezpieczeństwem personalnym. Jego istotą jest ochrona informacji poprzez uniemożliwienie dostępu do zasobów sieci informatycznej osobom, które z różnych przyczyn gotowe będą do ujawnienia gromadzonych, przetwarzanych wiadomości (w tym klasyfikowanych). Znajomość personelu przez osoby funkcyjne na stanowiskach kierowniczych powinna skutecznie eliminować sytuacje, w których nie można by było zidentyfikować, kto posiada dostęp do kluczowych elementów systemu komputerowego. Jednym z podstawowych warunków do spełnienia jest przeprowadzenie weryfikacji w stosunku do wszystkich osób mogących mieć styczność z informacjami uznawanymi za niejawne. Należy jednakże pamiętać, że wszelkie czynności dotyczące bezpieczeństwa personalnego powinny być realizowane w sposób dyskretny i nie naruszający przyjętych norm międzyludzkich. Może się także zdarzyć, że zaistnieje konieczność dokonania sprawdzenia wielu osób mogących mieć nawet pośredni dostęp do ważnych danych. Najczęściej zalicza się do nich personel pomocniczy (np. sprzątacze), jak również serwis naprawiający lub konserwujący różne urządzenia. Takie osoby także powinny zostać obowiązkowo przeszkolone z zakresu przestrzegania tajemnicy i obowiązujących przepisów.

2.2. Ochrona źródeł informacji

Pod pojęciem „źródło informacji" trzeba rozumieć wszelkie wiadomości gromadzone i przetwarzane w urządzeniach technicznych oraz zapisane przy pomocy umownych znaków (np. rysunków, obrazów, dźwięków, liczb lub przedstawione wskazania przyrządów pomiarowych) oraz wydrukowane dokumenty. Okazuje się, że nie muszą być one przetwarzane w postaci baz danych, jednakże ich treść może zawierać wiadomości, których ujawnienie może spowodować wzrost zagrożeń dla bezpieczeństwa wymiany informacji. Ochrona źródeł informacji o charakterze niejawnym wymusza konieczność zorganizowania systemu ich rejestrowania, ewidencji dostępu osób i kontroli zapobiegających ich uzyskaniu przez osoby nieuprawnione, czy też modyfikowaniu ich treści. Wiadomości zawarte w źródłach informacji (w tym w dokumentach niejawnych) muszą być zabezpieczone od chwili ich powstania, aż do zmiany klauzuli źródła informacji na „JAWNE", bądź ich zniszczenia zgodnie z obowiązującymi przepisami.

Najlepszym sposobem ochrony źródeł informacji jest wydzielenie i przygotowanie specjalnych do tego celu pomieszczeń (tzw. kancelarie tajne), w których można gromadzić źródła informacji (dokumenty) zawierające ważne wiadomości w różnej formie (notatki, rysunki, grafika, nośniki elektromagnetyczne, fotografie, taśmy video i magnetofonowe, filmy, obrazy itd.). Z kolei w systemach informatycznych standardem postępowania powinno być gromadzenie i archiwizowanie informacji w formie elektronicznej. Jest to prostsze niż przechowywanie dokumentów drukowanych, jednakże wymaga zastosowania odpowiednich urządzeń. Rozwiązanie takie powoduje konieczność stosowania barier utrudniających uzyskanie informacji z terminali końcowych oraz serwerów, co powinno pozwolić na ścisłą ewidencję stanu ilościowego dokumentu oraz kto był i jest aktualnie jego użytkownikiem. Ochronę źródeł informacji dla eksploatowanych sieci informatycznych zapewnia się poprzez realizację następujących czynności:

a) nadanie klauzuli tajności i odpowiedniego priorytetu ochrony dla źródła informacji (dokumentu), w którym zawarte są informacje o funkcjonowaniu sieci teleinformatycznej;
b) zabezpieczenie przed utratą dokumentu lub ujawnieniem treści źródła informacji dla osób nieuprawnionych - wydruki niejawne wyprowadzane na drukarki przekazuje się możliwie najszybciej pod formalną kontrolę kancelarii;
c) wskazanie imienne osób, które mogą korzystać z danego źródła informacji;
d) każdorazowe potwierdzenie otrzymania źródła informacji przez osobę użytkującą oraz zwrotu w wyznaczonym terminie.

Niszczenie źródeł informacji (dokumentów) odbywa się w sposób uniemożliwiający jakiekolwiek ich odtworzenie (np. poprzez deklasyfikację nośników elektromagnetycznych lub ich fizyczną destrukcję), komisyjnie, po sprawdzeniu ich zgodności z wykazem protokołów zniszczenia.

2.3. Kontrola dostępu

Kontrola dostępu do zasobów w systemach informatycznych skupia się na przyznawaniu uprawnień ich użytkownikom oraz opracowywaniu metod do sprawdzania, kto, kiedy i z jakich zasobów korzystał[20]. W tym celu wyznacza się strefy ochronne, a także warunki ochrony przed niewłaściwym działaniem personelu i użytkowników[21]. Kontrola taka połączona jest z identyfikacją, wiarygodnością oraz upoważnieniami dostępu do informacji. Aby właściwie chronić zasoby wiadomości, które są przechowywane w sieci komputerowej dla potrzeb logistyki właściwym jest zaangażowanie administratora systemu, a także jego wszystkich użytkowników. Jeśli okoliczności eksploatacji sieci tego wymagają, to dana instytucja może posiadać wyspecjalizowane komórki podległe Pełnomocnikowi ds. ochrony informacji niejawnych oraz personel bezpieczeństwa, który powinien mieć precyzyjnie sformułowany zakres kompetencji oraz zadania mogące mieć wpływ na ochronę informacji.

2.4. Zarządzanie ochroną sieci lub systemu informatycznego

Jednym z warunków realizacji celów działania każdej współczesnej instytucji korzystającej z dobrodziejstw rozwoju technicznego, a także przetwarzającej lub posiadającej w zasobach informacje niejawne jest zarządzanie funkcjonującą dla jej potrzeb ochroną sieci informatycznej. Wydaje się, że codziennie liczne grono szefów, kierowników, czy też dyrektorów komórek organizacyjnych, jak również personelu ochrony poszukuje odpowiedzi na poniższe pytania:

1. W jaki sposób powinno się to realizować?
2. Jakie elementy systemu ochrony uznać za krytyczne?

Zaistniała sytuacja problemowa powoduje, że ochrona informacji winna być rozpatrywana w aspekcie prawnym, organizacyjnym oraz technicznym. Powstał obszar działalności, w którym łączona jest wiedza teoretyczna oraz praktyka będąca wynikiem nabytych doświadczeń. Oznacza to, że zarządzanie ochroną czynnie wspiera również zapewnianie i utrzymanie pożądanego jej poziomu. Wiąże się to z zachowaniem gwarantowanego poziomu jakości informacji, które muszą być aktualne, nie mogą ulec celowej modyfikacji lub uszkodzeniu oraz być dostępne dla uprawnionych użytkowników.

Zarządzanie siecią komputerową powinno być rozumiane jako zespół środków organizacyjnych, programowych i sprzętowych umożliwiający administrowanie, sterowanie jej zasobami poprzez ustalanie zmian w jej topologii oraz zdolność do utrzymania wymaganego stanu pracy (np. określona ilość jednocześnie pracujących terminali i serwerów). Zarządzanie ochroną informacji stanowi połączenie elementów organizacji i zarządzania oraz informatyki, a także środków technicznych. Jest to proces ustawiczny zachodzący w zmieniających się warunkach otoczenia i funkcjonowania systemu lub sieci, który powinien być dostosowany do zmieniających się zagrożeń. W zarządzaniu ochroną dąży się do identyfikacji zagrożeń i eliminowania ich poprzez utrzymanie ustalonego poziomu ich bezpieczeństwa. Przyjmuje się, że im wyższy jest stopień niejawności wiadomości (danych), tym większa powinna być ilość zadań zapewniających jej bezpieczeństwo. Zarządzanie ochroną sieci lub systemu informatycznego jest często kojarzone z zarządzaniem informacją i posiada następujące cechy:

a) jest realizowane przez jej administratora oraz wykwalifikowany personel;
b) istnieje stała kontrola elementów podlegających ochronie oraz monitoring zagrożeń;
c) przestrzegane są zasady obiegu informacji, ich wytwarzania, przechowywania i niszczenia;
d) realizowanie zabezpieczenia organizacyjnego oraz technicznego;

[20] M. Szaliłow, *Organizacyjno-prawne aspekty ochrony systemów łączności i informacji w nich przesyłanej*, AON Warszawa 2001, s. 35.
[21] T. Goban-Klaus, P. Sienkiewicz, *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999, s. 66.

e) następuje alarmowanie o wszelkich naruszeniach bezpieczeństwa personelu związanego z bezpieczeństwem systemu lub sieci.

2.5. Kontrola ochrony wymiany informacji

Kontrola ochrony wymiany informacji pozwala na dokonanie porównywania stanu pożądanego z faktyczną realizacją zleconych środków bezpieczeństwa. Powinna umożliwiać obiektywną ocenę wysiłków podejmowanych działań zmierzających do utrudnienia i stworzenia barier przed jakąkolwiek utratą informacji o szczególnym znaczeniu. W tym celu przyjmuje się, że w każdej jednostce organizacyjnej (firmie) jej szef powinien wdrożyć system kontroli dający rzeczywisty obraz stanu faktycznego poziomu zagrożeń i bezpieczeństwa. Jednocześnie prowadzone kontrole nie mogą stanowić czynnika, który negatywnie wpływa na użytkowników sieci komputerowej, ale uświadomić im dodatkową formę nadzoru mającą wpływ na ochronę informacji klasyfikowanych (ważnych dla rozwoju oraz funkcjonowania przedsiębiorstwa). Zasadnicze cele kontroli to:

1. Ocena faktycznej ochrony informacji.
2. Porównanie stanu ewidencyjnego ze stanem faktycznym urządzeń, nośników oraz dokumentów.
3. Określenie czy sposób destrukcji nośników informacji, urządzeń i dokumentów oraz ich wyznaczenie do zniszczenia jest zgodne z przyjętymi procedurami.
4. Zebranie wniosków mogących służyć polepszeniu stanu bezpieczeństwa informacji.
5. Wyciągnięcie wniosków dyscyplinarnych w stosunku do winnych zaniedbań i naruszeń przyjętego systemu ochrony.

Wybór sposobu i częstotliwości kontroli zależał będzie przede wszystkim od przestrzegania obowiązujących przepisów w zakresie ochrony informacji, a także skuteczności wdrożonych środków bezpieczeństwa. Ponadto realizuje się stałe przedsięwzięcia podczas bieżącej eksploatacji systemu lub sieci, które mogą wpłynąć na poprawę bezpieczeństwa wymiany informacji. Coraz częściej w tym celu angażowane są wyspecjalizowane firmy zewnętrzne.

3. TECHNICZNE ŚRODKI OCHRONY INFORMACJI W LOGISTYCE

Warunkiem funkcjonowania sieci informatycznych dedykowanych dla logistyki jest zastosowanie urządzeń, które mogą zapewniać ich bezpieczeństwo, także wówczas gdy zachodzi uzasadniona potrzeba współdzielenia zasobów oraz wymiany informacji pomiędzy wskazanymi osobami funkcyjnymi. Terminale oraz inne urządzenia końcowe, powinny spełniać sprecyzowane odpowiednio wcześniej wymagania w aspekcie zabezpieczenia gromadzonych i przekazywanych za ich pomocą danych. Jednocześnie, w celu zwiększania stopnia ich ochrony oraz minimalizowania błędów użytkowników czy też dostępu do zasobów, stosowane są narzędzia pozwalające na automatyczne rejestrowanie pracy na pojedynczych terminalach oraz całości systemu lub sieci. Przestrzeganie procedur bezpieczeństwa wymiany informacji, identyfikacji urządzeń i połączeń, jak również stosowanie ochrony technicznej powinno tworzyć efektywne bariery dla osób postronnych. Tym niemniej należy zauważyć, że trudno jest objąć technicznymi środkami ochrony całość rozwiniętego w wielu różnych lokalizacjach systemu lub sieci informatycznej, a zwłaszcza ich wzajemnych połączeń poprzez środki transmisyjne na dużych odległościach.

Organa bezpieczeństwa teleinformatycznego zalecają, że aby poziom bezpieczeństwa ochrony informacji był odpowiedni do kategorii przekazywanych wiadomości, powinno się stosować środki ochrony zapewniające jej bezpieczeństwo przed możliwością narażenia jej na zidentyfikowane zagrożenia, a w szczególności nieuprawnione ujawnienie. Do głównych technicznych środków ochrony informacji zalicza się:

1. Ochronę sprzętową.
2. Wpływ oprogramowania na ochronę informacji.
3. Ochronę fizyczną (odpowiednik kontroli dostępu).
4. Ochronę kryptograficzną[22].

[22] Ze względu na jawny charakter opracowanie zostanie ona przedstawiona w sposób ogólny, który nie naruszy zasad ochrony informacji klasyfikowanych.

3.1. Ochrona sprzętowa

Prowadzone obserwacje wskazują, że współczesne urządzenia techniczne pracujące w sieciach komputerowych w ograniczony sposób zapewniają trwałość i ciągłość pracy oraz pożądany poziom ochrony informacji. Niedociągnięcia w tym zakresie odnoszą się do zapewnienia ochrony technicznej. Zazwyczaj wynika to z niskiej świadomości użytkowników w aspekcie konieczności dbałości o bezpieczeństwo informacji. Stąd można wyróżnić następujące czynniki ochrony sprzętowej:

1. Brak możliwości kradzieży urządzeń przetwarzających informacje oraz wykluczenie możliwości ich podmiany na inne bez naruszenia zabezpieczeń.
2. Maksymalne wykorzystanie zewnętrznych wejść-wyjść do danego urządzenia - niewykorzystane wejścia-wyjścia należy zaślepić (zatkać, oplombować) w sposób, w którym nie będzie możliwości ominięcia tak wykonanych zabezpieczeń.
3. Utrzymanie stałego zasilania pracy urządzeń przekazujących informacje, jak również przestrzeganie wymogów bezpieczeństwa określonych w instrukcjach obsługi urządzeń czy też przeciwpożarowych.
4. Bezpieczeństwo transmisji, które osiąga się poprzez zastosowanie metod i środków, innych niż fizyczne i kryptograficzne, mających na celu ochronę przekazywanych informacji przed podsłuchem, analizą ruchu itp.

3.2. Wpływ oprogramowania na ochronę informacji

Oprogramowanie umożliwia działanie urządzeń wykorzystując ustalone mechanizmy zarządzania oraz kolejność realizacji poszczególnych zadań. Dzięki niemu sprzęt wykonuje określone czynności, do czego w szczególności przyczynia się oprogramowanie systemowe kontrolujące pracę urządzeń (systemy operacyjne i programy użytkowe) i pozwalające na eksploatację sieci komputerowej. Wykorzystuje się również zaprogramowane mechanizmy sterowania oraz bezpieczeństwa. Określa się wymagania do oprogramowania w zależności od jego przeznaczenia oraz użytkowników, warunkujące bezpieczeństwo informacji, które zawiera mechanizmy umożliwiające gromadzenie, przetwarzanie i wymianę informacji, pochodzi z legalnego i sprawdzonego źródła oraz jest certyfikowane. Każdorazowo dokonuje się badań jego przydatności do skutecznego zapewnienia ochrony informacji (przede wszystkim niejawnych) oraz przeprowadza się kontrole mogące ujawnić jego wady. Oprogramowanie stosowane w systemach lub sieci informatycznej logistyki powinno umożliwiać:

a) realizację połączeń pomiędzy użytkownikami (stanowiskami pracy);
b) kontrolę dostępu do przetwarzanych informacji poprzez logowanie osób funkcyjnych oraz dedykowane im hasła dostępu (identyfikacja „swój-obcy”);
c) stworzenie mechanizmów utrudniających celowe lub nieumyślne wprowadzenie zainfekowanego oprogramowania - mogącego mieć trwałe skutki w postaci niesprawności terminali oraz sieci komputerowej;
d) zmianę kodów dostępu przez osoby uprawnione - zdalne sterowanie sieciami;
e) identyfikację oprogramowania, profesjonalnej pomocy serwisowej, dostosowywanie do nowych oczekiwań;
f) spełnienie przyjętych norm bezpieczeństwa (barierę powyżej której dostęp do oprogramowania nie występuje), a jednocześnie pozwalają na prace przy nim w zakresie jego modernizacji, kontroli, sporządzania sprawozdań z pracy;
g) monitoring informacji wymienianych za pomocą sieci komputerowej, włącznie z określeniem czasu przekazania wiadomości, adresatów oraz sposobu odebrania wiadomości (przez kogo oraz kiedy).

Warto zauważyć, że oprogramowanie nie będzie spełniać swojej roli bez powiązania go z innymi elementami ochrony technicznej, natomiast wzrost poziomu bezpieczeństwa informacji w sieciach oraz minimalizacja (wykluczanie) dużej ilości błędów podczas eksploatacji jest ściśle związany z sprawdzonym oprogramowaniem.

3.3. Ochrona fizyczna

W literaturze przedmiotu stwierdza się, że „*ochronę fizyczną sieci teleinformatycznej zapewnia się poprzez umieszczenie urządzeń sieci teleinformatycznej w strefach bezpieczeństwa w zależności od klauzuli tajności informacji niejawnych, ilości informacji niejawnych, zagrożeń w zakresie ujawnienia, utraty, modyfikacji przez osobę nieuprawnioną oraz poprzez instalację środków zabezpieczających pomieszczenia, w których znajdują się urządzenia (...) sieci teleinformatycznej, a w szczególności przed nieuprawnionym dostępem, podglądem, podsłuchem*”[23]. Zatem uznaje się, że realizacja ochrony fizycznej sieci komputerowej skupiona jest przede wszystkim w ściśle określonych miejscach (teren firmy, obiekt, biuro, ale także rejon rozwinięcia tymczasowych miejsc pracy).

Ochrona fizyczna często jest błędnie przypisywana do czynności organizacyjnych ochrony informacji (zwłaszcza do kontroli dostępu). Różnica wynika z stosowania i wsparcia jej przez różne urządzenia techniczne (np. czytniki elektroniczne i biometryczne, monitoring, systemy alarmowe, czujniki). Może być zapewniona w wyniku zabezpieczenia pomieszczeń (zgodnie z obowiązującymi przepisami), z których mogą być przekazywane informacje klasyfikowane (np. kancelaria tajna, archiwum, pomieszczenia, w których rozlokowano centrale, terminale i punkty informatyczne). Wyznacza się i trwale oddziela strefy z ograniczeniem możliwości wejścia i wyjścia w zależności od klauzuli ważności informacji, a także charakteru zagrożeń w zakresie ich ujawnienia. Ma to zapewnić ochronę tych wiadomości z jednoczesnym pozwoleniem na korzystanie z ich zasobów przez osoby uprawnione. Może być stosowany system przepustek oraz dostępu uprawniający do pracy w ściśle określonych miejscach. Sposób realizacji ochrony fizycznej zależy od miejsca lokalizacji oraz wymagań w aspekcie ochrony informacji. Stosowane są przedsięwzięcia, które pozwalają na szybkie wykrywanie wszelkiego rodzaju naruszeń bezpieczeństwa, wykrywają nieprawidłowości w pracy systemów i sieciach oraz zapewniają ochronę w sytuacjach awaryjnych.

3.4. Ochrona kryptograficzna

Kryptografia, to „*sztuka przekształcania tekstu pisanego, zrozumiałego dla wszystkich w tekst zaszyfrowany zrozumiały tylko dla wtajemniczonych, znających dany szyfr*”[24]. Słowo to pochodzi z języka greckiego, z połączenia słów „kryptos” (oznacza „ukryty”) oraz „gráphein” (oznacza „pisać”). Kryptografia jest nauką zajmująca się poufnością przekazywanych informacji. Pod tym pojęciem należy rozumieć też *sztukę zabezpieczania wiadomości*[25]. Współcześnie kryptografia definiowana jest także jako „*element informatyki, umożliwiający za pomocą różnych metod (...) zabezpieczenie informacji tworzonej, przesyłanej lub przetwarzanej w postaci cyfrowej. Stanowi narzędzie do zabezpieczenia usług przebiegających on-line (transmisja) lub off-line (poczta elektroniczna), w sposób czysto programowy, sprzętowy lub mieszany*”[26].

Ochrona kryptograficzna sieci informatycznej polega na:

a) stosowaniu metod i środków zabezpieczających informacje niejawne przez ich szyfrowanie oraz stosowanie innych mechanizmów kryptograficznych gwarantujących integralność i zabezpieczenie przed nieuprawnionym ujawnieniem tych informacji lub uwierzytelnienie podmiotów oraz informacji;
b) zastosowaniu mechanizmów gwarantujących ich poufność, integralność oraz uwierzytelnienie.

Ochronę kryptograficzną stosuje się przy przekazywaniu informacji w formie transmisji poza obszar kontrolowanego dostępu, a dla sieci informatycznej powinna gwarantować następujące usługi:

a) **poufności** - właściwość przypisana do danych określająca, do jakiego stopnia dane te nie mogą zostać udostępnione lub ujawnione nieuprawnionym osobom, podmiotom lub procesom;
b) **integralności** - zabezpieczenie przed nieautoryzowaną modyfikacją danych;
c) **uwierzytelniania** - akt weryfikacji deklarowanej tożsamości podmiotu;
d) **niezaprzeczalności** - brak możliwości wyparcia się swego uczestnictwa w całości lub części wymiany danych przez jeden z podmiotów w tej wymianie.

[23] *Metodyka opracowywania szczególnych wymagań bezpieczeństwa dla systemów lub sieci teleinformatycznych*, SG WP, GZDiŁ, Warszawa 2000, Łączn. wew. 51/2000, s. 31-32.
[24] M. Szymczak (red. naukowa), S*łownik języka...,* op. cit., tom I, s. 1063.
[25] B. Schneider, *Kryptografia dla praktyków*, WNT, Warszawa 1995, s. 19.
[26] A. Urbanek, *Ilustrowany leksykon teleinformatyka*, IDG, Warszawa 2001, s. 122.

WNIOSKI

Analiza obecnych rozwiązań w zakresie środków ochrony informacji w sieciach teleinformatycznych logistyki, stanowi zdaniem autora, podstawę do sformułowania następujących wniosków:

I. W zakresie organizacyjnych środków ochrony informacji:

1. Postęp technologiczny oraz wzrost oczekiwań użytkowników wymaga, aby był obsługiwany przez właściwie wyszkolony oraz zweryfikowany personel.
2. Przestrzeganie procedur bezpieczeństwa powinno być normą i nie może być traktowane, jak zło konieczne, ale wynikać z przyjętych zasad postępowania.
3. Kluczowym elementem ochrony zasobów jest kontrola dostępu, której efektem powinna być możliwość sprawdzania, kto, kiedy i z jakich zasobów sieci korzystał, kontrola przestrzegania obowiązujących przepisów oraz systemu ochrony.

II. W odniesieniu do technicznych środków ochrony:

1. Zabezpieczenie sprzętowe posiada fundamentalne znaczenie dla organizacji oraz eksploatacji całości sieci komputerowej.
2. Oprogramowanie decyduje o poprawności działania elementów składowych sieci. Wszelkie zmiany dokonywane bez wiedzy administratora bezpieczeństwa teleinformatycznego oraz ingerencja w zaprogramowane algorytmy funkcjonowania urządzeń elektronicznych mogą mieć negatywne skutki.
3. Ochrona fizyczna, obok przedsięwzięć kontroli dostępu, jest głównym czynnikiem mającym wpływ na ochronę informacji. Prawidłowo zorganizowana ochrona systemów komputerowych oraz wykorzystanie wszelkich dostępnych środków technicznych powinna minimalizować przewidywane zagrożenia oraz ewentualne ich skutki.

Przedstawione sposoby przeciwdziałania zagrożeniom są fundamentem następujących wniosków końcowych:

1. Należy minimalizować możliwość straty, podmiany lub modyfikacji przekazywanych wiadomości.
2. Obowiązujące zasady oraz procedury bezpieczeństwa nie mogą być ujawniane osobom nieuprawnionym.
3. Zapewnienie ochrony informacji następuje przy uwzględnieniu niżej wymienionych warunków:
   a) stosowanie certyfikowanego sprzętu i oprogramowania;
   b) wszyscy użytkownicy sieci odbyli odpowiednie do zajmowanego stanowiska szkolenia;
   c) ochrona źródeł informacji;
   d) właściwe zarządzanie ochroną sieci informatycznej;
   e) ograniczenie dostępu dla osób postronnych;
   f) stworzenie systemu nadzoru i kontroli.
4. Nawet najlepiej zaplanowany system ochrony jest zawodny, jeśli nie stworzy się dla niego odpowiednich warunków do realizacji. Umiejętne połączenie komponentów organizacyjno-technicznych bezpieczeństwa sieci daje poczucie uzyskania oczekiwanych rezultatów, natomiast bardzo trudno jest zapewnić 100% bezpieczeństwa ochrony informacji niejawnych. W tym przypadku wskazane jest minimalizowanie prawdopodobieństwa utraty wiadomości oraz uczynić je nieopłacalnym w wyniku długości czasu, jaki byłby potrzebny do jej zdobycia.

W ocenie autora, nie ulega wątpliwości, że jednym z najważniejszych czynników mogących mieć wpływ na ochronę informacji przekazywanych przez sieci teleinformatyczne dedykowane dla logistyki są cykliczne szkolenia zasad bezpieczeństwa stosowanych w danej sieci informatycznej. Są jednym z fundamentów uświadamiania ich użytkowników w aspekcie istniejących oraz potencjalnych zagrożeń, a także sposobów przeciwdziałania zagrożeniom. Powinny mieć miejsce we wszystkich instytucjach i organizacjach zajmujących się logistyką. Poruszony problem bezpieczeństwa informacji dla potrzeb logistyki nadal będzie przedmiotem kolejnych rozważań autora, który ma świadomość konieczności dalszego prowadzenia badań w tym obszarze.

Streszczenie

Dynamiczny rozwój technologii informacyjnych ma coraz większy wpływ na wszystkie aspekty życia człowieka. Komputer jest urządzeniem, które stało się ogólnie dostępne, a możliwość gromadzenia, przetwarzania oraz przekazywania różnych informacji powoduje, iż wzrasta ilość oferowanych przy jego udziale usług. Ma to również odzwierciedlenie w szeroko rozumianej logistyce.

W artykule poruszono problem identyfikacji czynników, które mają wpływ na ochronę informacji w sieciach teleinformatycznych stosowanych w logistyce. Szczególną uwagę zwrócono na zagrożenia oraz wskazano na atrybuty decydujące o bezpieczeństwie informacji. Zaprezentowano wybrane aspekty ich bezpieczeństwa mające na celu wskazanie ich znaczenia dla codziennej działalności, a także roli wzrostu świadomości użytkowników w zwiększaniu poziomu ochrony informacji ważnych dla prawidłowego funkcjonowania logistyki.

The threats and information security in logistics data teleinformatics networks

Abstract

The dynamic evolution of informational technologies has a more and more greater influence on all aspects of the life of the man. The computer is a device which became general accessible. The possibility of the accumulation, processings and the transfer of the different information causes that increases the quantity offered at his participation of services. There has this also a reflection in the widely understood logistics.

The article moves the problem of the identification of factors which have an influence on the information assurance. One presented chosen aspects of their security targeting indication of their meaning for the daily activity, and also the part of the height of the consciousness of users in enlarging of the level of the information assurance important for the correct kelter of the logistics.

BIBLIOGRAFIA

1. Goban-Klaus T., Sienkiewicz. P., *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999.
2. Janczak J., Świdzikowski G., *Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym*, Warszawa AON, 2004.
3. Lent B. (redakcja naukowa), *Bezpieczeństwo w telekomunikacji i teleinformatyce*, tom 3, Biblioteka Bezpieczeństwa Narodowego, Warszawa 2007.
4. Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008.
5. Liderman K., *Podręcznik administratora bezpieczeństwa teleinformatycznego*, Warszawa 2003.
6. Markowski A., *Nowy Słownik Poprawnej Polszczyzny*, PWN, Warszawa 1999.
7. *Metodyka opracowywania szczególnych wymagań bezpieczeństwa dla systemów lub sieci teleinformatycznych*, SG WP, Warszawa 2000.
8. Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 roku *w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego .(Dz. U. nr 171, poz. 1433)*, art. 7.1.
9. Schneider B., *Kryptografia dla praktyków*, WNT, Warszawa 1995.
10. *Słownik współczesnego Języka Polskiego,* wyd. WILGA, Warszawa 1999.
11. Szaliłow M., *Organizacyjno-prawne aspekty ochrony systemów łączności i informacji w nich przesyłanej*, AON Warszawa 2001.
12. Szymczak M., (red. naukowa), *Słownik języka polskiego*, PWN, Warszawa 1992.
13. *Uniwersalny Słownik Języka Polskiego*, PWN, Warszawa 2003.
14. Urbanek A., *Ilustrowany leksykon teleinformatyka*, IDG, Warszawa 2001.
15. *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z dnia 2 sierpnia 1997 r., Dz.U.97.88.553, sprost.: Dz.U.97.128.840, zm.: Dz.U.99.64.729, zm.: Dz.U.99.83.931, zm.: Dz.U.00.48.548 - 2000.07.15, zm.: Dz.U.00.48.548 - 2000.12.15, zm.: Dz.U.00.93.1027, zm.: Dz.U.00.116.1216).*
16. Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. Dz.U.10.18.1228.
17. Żmigrodzki P., Słownik *synonimów i antonimów*, wyd. EUROPA, Wrocław 2007.