Michał Kozioł

Bezpieczeństwo i ochrona systemów informatycznych

1. Uwagi wstępne

We współczesnym świecie coraz większą rolę odgrywa informacja, a zwłaszcza sprawne i skuteczne posługiwanie się nią. Bez umiejętności tej nie mogłyby funkcjonować instytucje i przedsiębiorstwa. W dużej mierze przyczynia się do tego nieustanny rozwój technologii teleinformatycznej. Dzięki niemu dostęp do informacji stał się łatwiejszy i szybszy, można ją gromadzić, systematyzować i wykorzystywać. Jednocześnie pojawił się problem wyodrębnienia właściwej jakości i ilości informacji dla danej organizacji, jak również jej ochrony i zabezpieczenia. W tym celu firmy i instytucje muszą opracować i wdrożyć odpowiednią politykę bezpieczeństwa, która ma za zadanie zminimalizowanie zagrożeń wewnętrznych i zewnętrznych. Przy jej opracowywaniu — podkreślają to liczni autorzy — należy uwzględnić wielkość przedsiębiorstwa, rodzaj prowadzonej działalności, zakres zastosowania sprzętu teleinformatycznego, a także określić jakie znaczenie dana informacja ma dla firmy i koszty z tym związane.

Celem artykułu jest zaprezentowanie koncepcji polityki bezpieczeństwa i ochrony informacji oraz metodyki jej implementacji w organizacji. W artykule przedstawiono najczęściej spotykane zagrożenia występujące w obszarze ochrony informacji, jak również mechanizmy ich zabezpieczenia. Zwrócono uwagę na czynnik ludzki, odgrywający najważniejszą rolę w tym procesie.

Szczególnie wiele miejsca poświęcono na omówienie etapów budowy polityki bezpieczeństwa i ochrony informacji, które uzupełniono o podanie etapu analizy i oceny sytuacji firmy. W zakończeniu artykułu zawarto ocenę skuteczności i efektywności scharakteryzowanych pokrótce narzędzi (metod, środków, oprogramowania) wykorzystywanych w praktyce ochrony informacji.

Artykuł adresowany jest głównie do specjalistów zajmujących się tym zagadnieniem, a w szczególności zarządzaniem bezpieczeństwem informacji. Nadto może być przydatny studentom kierunku informatyka i ekonometria oraz praktykom zajmującym się tym zagadnieniem.

2. Istota i rodzaje zagrożeń bezpieczeństwa informacji

Bezpieczeństwo informacji rozumiane jest zazwyczaj jako pewność ochrony dostępu do informacji zgromadzonej i pewność ochrony informacji przesłanej [J. Kosiński 2000, s. 482]. Podkreśla się przy tym, że należy przede wszystkim uwzględnić ryzyko związane z jego zagrożeniem. Nadto powinno się wyraźnie odróżnić bezpieczeństwo informacji od bezpieczeństwa systemu informacyjnego, czyli sprzętu i oprogramowania służącego do gromadzenia, przechowywania i przetwarzania informacji. Przy czym głównym źródłem zagrożeń jest konflikt interesów związany z technologiami informatycznymi [J. Kosiński 2000, s. 492]. Podstawowymi źródłami konfliktu są: wymagania i cele organizacji, ograniczenia jej rozwoju, zagrożenia, obowiązujące przepisy prawne [J. Kosiński 2000, s. 492].

Zagrożenia mogą być spowodowane poprzez:

— działania sił przyrody (np. huragany, powodzie, trzęsienia ziemi),
— czynniki ekonomiczne i/lub polityczne,
— działania człowieka (podmiotu odpowiedzialnego za szkodę),
— zaburzenia funkcjonowania systemu.

Człowiek przez niewłaściwe działanie może spowodować szkody. Można je podzielić na działania umyślne, czyli ataki, jak i działania nieumyślne. Dalej wyróżnia się ataki pasywne i aktywne. Atakami pasywnymi jest podsłuchiwanie informacji (*snooping*) znajdujących się w sieci, aktywne zaś to próby uzyskania nieautoryzowanego dostępu do systemu bądź informacji o potencjalnych lukach bezpieczeństwa w systemie [M. Szmit 2003, s. 100]. Ataki mogą nastąpić zarówno z zewnątrz, jak i wewnątrz przedsiębiorstwa. Z kolei do działań nieumyślnych zaliczamy: dążenie do odmiennych celów, zaniedbanie, brak wiedzy. Mogą się one przyczynić do ujawnienia, uszkodzenia, modyfikacji, zablokowania, a nawet do utraty informacji. Następstwem tego są straty finansowe ponoszone przez firmę, utrata znacznych jej udziałów w rynku lub/i wizerunku, co w konsekwencji może doprowadzić do jej upadku.

Specyficznym zagrożeniem dla bezpieczeństwa informacji są świadome działania człowieka związane ze sprzętem teleinformatycznym określanych mianem przestępczości komputerowej. Są to następujące rodzaje tego przestępstwa [J. Kosiński 2000, s. 487—489; M. Szmit 2003, s. 101]:

a) przywłaszczanie sobie autorstwa programu, jego fałszowanie, a także oznaczenie cudzego programu własnym znakiem firmowym,

b) *cracking*, czyli nieuprawnione wejście do programu w celu dokonywania skrótów, adaptacji i przeróbek zmieniających kod programu niezgodnie z intencją autora,

c) *hacking*, czyli nieuprawniony dostęp do systemu komputerowego,

d) przechwytywanie danych m.in. poprzez nieuprawnione wykonywanie dodatkowych kopii programu lub jego preinstalacje na dysku twardym,

e) kradzież czasu polegająca na korzystaniu przez pracownika z systemu komputerowego poza wyznaczonymi godzinami pracy,

f) utrudnienie lub uniemożliwienie przeprowadzenia kontroli legalności korzystania z określonego oprogramowania,

g) paserstwo komputerowe, czyli nielegalne nabywanie i sprzedaż sprzętu i oprogramowania pochodzącego z kradzieży,

h) oszustwa dokonywane z użyciem komputera, a w szczególności:

— oszustwa bankomatowe, polegające głównie na przywłaszczeniu cudzej karty uprawniającej do podjęcia pieniędzy z automatu bankowego,

— fałszowanie urządzeń wejścia lub wyjścia (np. kart magnetycznych lub mikroprocesorowych),

— oszustwa dokonywane na maszynach do gier,

— podanie do wiadomości fałszywych danych identyfikacyjnych,

— oszustwa dokonywane w systemach sprzedaży, np. w kasach fiskalnych,

— niszczenie lub uszkodzenie urządzeń nawigacyjnych służących do przetwarzania danych w komunikacji;

i) phearing, czyli oszustwa w systemach telekomunikacyjnych:

— powielanie programów komputerowych,

— bezprawne kopiowanie topografii półprzewodników,

— włączenie się do urządzenia telekomunikacyjnego w celu uruchomienia na cudzy rachunek impulsów telefonicznych;

j) modyfikacja i niszczenie zasobów danych przy wykorzystaniu wszelkiego rodzaju wirusów, robaków, koni trojańskich oraz bomby logicznej. Często występują w powiązaniu z piractwem komputerowym. Wirusy są to programy wykonywalne lub makrodefinicje, ukrywające się przed użytkownikiem i powielające się w systemie komputerowym przy wykorzystaniu mechanizmów systemu operacyjnego bądź oprogramowania użytkowego. Robaki komputerowe (*I-worms*), to szczególny rodzaj wirusów komputerowych, rozmnażających się w systemie internetowym (np. w nieprawidłowo zabezpieczonej poczcie elektronicznej). Z kolei konie trojańskie są to uruchamiane przez użytkownika programy podejmujące w sposób ukryty przed nim działania w systemie komputerowym, np. udające arkusz kalkulacyjny, edytor tekstów. Wykorzystują one luki w programie lub systemie komputerowym, tzw. „tylne drzwi" (*backdoor*). Często są nosicielami wirusów komputerowych.

k) sabotaż sprzętu i oprogramowania,

l) rozpowszechnianie za pomocą BBS chronionego oprogramowania komputerowego,

m) przechowywanie zabronionych przez prawo zbiorów danych o treściach: obrażających czyjeś uczucia religijne, propagujących faszyzm, rasizm, antysemityzm; pochwalających przemoc; pornograficznych (szczególnie z wykorzystaniem osób niepełnoletnich i zwierząt),

n) przestępstwa dokonywane w witrynach internetowych.

Dokonując klasyfikacji zagrożeń warto pamiętać, że nie jest to sztywny podział, gdyż niektóre z nich nakładają się na siebie. Ponadto należy dokonując podziału uwzględnić wielkość, charakter, formę prawną oraz rodzaj prowadzonej działalności przedsiębiorstwa. Pewne zagrożenia dla bezpieczeństwa informacji mogą wystąpić zarówno dla zbioru danych, jak i systemu teleinformatycznego.

Oprócz wymienionych najczęstszymi działaniami podejmowanymi w celu zniszczenia danych jest fizyczne niszczenie sprzętu komputerowego.

Wśród wielu wymienionych źródeł zagrożeń bezpieczeństwa informacji zwłaszcza tych, które związane są z działalnością człowieka, na szczególną uwagę zasługują zagrożenia wynikłe z niewiedzy, braku fachowości, zaniedbań i innych cech osobowych oraz kultury w dziedzinie ochrony informacji. Stanowią one istotną determinantę polityki bezpieczeństwa informacji, sprowadzającą się nie tyle do wprowadzania dodatkowych urządzeń, czy programów, co raczej do odpowiedniego przeszkolenia pracowników i uświadomienia im wagi tego problemu. Można zatem mówić o kulturowych determinantach ochrony informacji, mniej eksponowanych w licznych już pracach informatyków oraz specjalistów w zakresie zarządzania informacją. Nadto szczególną ochroną należałoby objąć informacje mające strategiczne znaczenie dla konkurencji.

3. Polityka bezpieczeństwa systemu informatycznego

Każda organizacja niezależnie od formy prawnej i charakteru prowadzonej działalności powinna zapewnić bezpieczeństwo zasobów informacyjnych. Dotyczy to zwłaszcza organizacji wykorzystujących szczególnie ważne dane dla kraju lub społeczności międzynarodowych (m.in. przedsiębiorstwa o charakterze militarnym) oraz wykorzystujące nowoczesny sprzęt teleinformatyczny. Konieczne jest więc opracowanie koncepcji bezpieczeństwa. Nosi ona nazwę polityki bezpieczeństwa informacji (*security policy*). Jest to plan lub sposób działania przyjęty w celu zapewnienia bezpieczeństwa systemów i ochrony danych [M. Szmit 2003, s. 104 za: PN-I-02000]. Przed przystąpieniem do jej opracowania należy określić:

— miejsce i sposób gromadzenia i przechowywania informacji,

— potencjalne źródła zagrożeń,

— potencjalne działania mające na celu wyeliminowanie zagrożeń, a przynajmniej ograniczenie ich do akceptowanego minimum.

Nad opracowaniem i wdrożeniem polityki bezpieczeństwa w przedsiębiorstwie powinno czuwać przede wszystkim kierownictwo firmy. Jednakże swój wkład powinni wnosić wszyscy pracownicy, a w szczególności informatycy i administratorzy sprzętu.

Prawidłowo opracowana polityka bezpieczeństwa powinna określać [L. Kiełtyka 2003, s. 27]:

— cele i strategię bezpieczeństwa,

— wymagany poziom bezpieczeństwa,

— klasyfikację informacji,
— role i odpowiedzialności w procesie przetwarzania informacji,
— strategię analizy ryzyka,
— akceptowane ryzyko szczątkowe.

Najważniejszym jej elementem jest ochrona danych oraz sprzętu służącego do ich pozyskiwania, przetwarzania i przechowywania. Musi być opracowana w formie całościowego dokumentu, obejmującego ochronę zarówno informacji gromadzonych, przechowywanych i przetwarzanych za pomocą sprzętu teleinformatycznego, jak i metodami tradycyjnymi. Ponadto należy też uwzględnić ochronę samego systemu, jako nośnika informacji.

Wprawdzie dość powszechnie uważa się, że dla bezpieczeństwa informacji wystarczy, aby była ona wiarygodna, dostępna oraz odznaczała się poufnością, niemniej jednak warto zwrócić uwagę na inne jej desygnaty. Wybrane ważniejsze z nich to [J. Kosiński 2000, s. 482]:

— poufność (*confidentialy*) — zabezpieczająca, że dane zawarte w systemie nie będą udostępniane osobom nieupoważnionym,
— wiarygodność (*integrity*) — zapewniająca, że dane zgromadzone w systemie są integralne, nie ulegają nieupoważnionym modyfikacjom i zniekształceniom,
— dostępność (*availability*) — prowadząca do tego, że dane zawarte w systemie będą dostępne zawsze, gdy tego zażądamy a jesteśmy do tego uprawnieni [...],
— rozliczalność (*accountability*) — umożliwiająca jednoznaczne przypisania działań do określonego użytkownika umożliwiająca określenie i weryfikację odpowiedzialności za realizowane działania,
— autentyczność (*authenticity*) — podkreśla jednoznaczność określania deklarowanej tożsamości użytkownika lub prawdziwości zasobów,
— niezawodność (*reliability*) — to właściwość określająca, że działanie systemu będzie zawsze zgodne z zamierzonym.

Proces tworzenia polityki bezpieczeństwa jest wieloetapowy [P. Lula, J. Wołoszyn 2001, s. 296]. Wyróżniamy tu następujące etapy:

— ewidencję składników systemu informatycznego,
— tworzenie projektu systemu bezpieczeństwa,
— wdrożenie systemu bezpieczeństwa,
— eksploatację systemu bezpieczeństwa.

E w i d e n c j a s k ł a d n i k ó w s y s t e m u i n f o r m a t y c z n e g o jest pierwszym etapem tworzenia systemu bezpieczeństwa w przedsiębiorstwie. Polega na sporządzeniu szczegółowego wykazu zarówno elementów sprzętowych (sprzęt komputerowy, urządzenia telekomunikacyjne, urządzenia zewnętrzne), jak i oprogramowania (programy komputerowe, dane systemowe, dane użytkowe). Ponadto przeprowadza się szczegółowe badania i opis zarówno struktury fizycznej, jak i struktury funkcjonalnej systemu teleinformatycznego. Struktura fizyczna określa

sposób połączenia poszczególnych elementów tegoż systemu, zaś struktura funkcjonalna określa funkcje realizowane przez poszczególne składniki systemu [P. Lula, J. Wołoszyn 2001, s. 296].

Na podstawie dokonanej ewidencji składników systemu komputerowego przeprowadza się analizę ryzyka, która sprowadza się do określenia potencjalnego ryzyka, jakie występuje podczas jego eksploatacji. Przede wszystkim należy określić, które składniki są najbardziej wartościowe i dokonać prawidłowego ich zabezpieczenia. Najpierw trzeba zatem dokonać przeglądu i oceny istniejących już zabezpieczeń. Jeżeli okażą się nieodpowiednie, to wówczas należy je zmodyfikować. Ponadto należy określić źródło, stopień ich zagrożenia, ryzyko występowania tych zagrożeń, a także koszty ich eliminacji.

T w o r z e n i e p r o j e k t u s y s t e m u b e z p i e c z e ń s t w a, to wstępny etap opracowywania polityki bezpieczeństwa. Jest on realizowany głównie w oparciu o przeprowadzoną uprzednio analizę ryzyka. Projekt ten powinien uwzględniać wszystkie aspekty ochrony informacji i systemu informatycznego. Warto przy tym zwrócić uwagę na źródło i rodzaj zagrożeń, stopień informatyzacji przedsiębiorstwa, a także rodzaj prowadzonej działalności gospodarczej, jego formę prawną i organizacyjną. W celu zmniejszenia kosztów należy wykorzystać istniejące

W etapie w d r o ż e n i a s y s t e m u b e z p i e c z e ń s t w a wprowadza się wszystkie planowane zabezpieczenia, poczynając od instalacji mechanizmów programowych i sprzętowych, a na rozwiązaniach administracyjnych i prawnych kończąc. Ważnym elementem wdrażania systemu bezpieczeństwa jest jego testowanie. Polega ono na wywoływaniu zagrożenia, a następnie jego likwidacji. Do testowania powinno się wybrać pracowników, którzy nie brali udziału w pracach projektowych. Ponadto należy wykorzystać specjalistyczne narzędzia komputerowe stosowane w takich przypadkach. Jeżeli system ochrony okaże się niesprawny, to należy go zmodyfikować, lub poprawić.

Ważnym elementem wdrażania systemu bezpieczeństwa jest dobór odpowiedniego personelu. Warto przy tym podkreślić, że wszyscy pracownicy powinni być zaznajomieni z obowiązującą polityką bezpieczeństwa firmy, m.in. przez specjalne szkolenia. Przede wszystkim muszą oni zachować dyskrecję w tej sprawie. Ważne jest tu także właściwe podejście pracowników do wdrażanego systemu. Jest to ważny element polityki bezpieczeństwa wielu firm i instytucji krajów zachodnich. Jednakże wśród pracowników wielu polskich firm istnieje pogląd, iż niepotrzebny jest jakikolwiek system zabezpieczenia informacji. Ich nastawienie zmienia się dopiero po wystąpieniu realnego zagrożenia, np. kradzieży danych, zniszczenia sprzętu komputerowego itp.

E k s p l o a t a c j a s y s t e m u o c h r o n y, to ostatni etap polityki bezpieczeństwa. Polega on na ciągłym administrowaniu systemu przez wydzielone komórki. W razie wystąpienia jakichkolwiek niesprawności, usterek, bądź pojawienia się nowych zagrożeń należy dokonać jego usprawnienia lub modyfikacji. Warto rów-

nież przeprowadzać okresowe audyty dotyczące funkcjonowania systemu przez wiarygodnego specjalistę zatrudnionego z zewnątrz.

Należy pamiętać, że polityka bezpieczeństwa nie powinna zawierać szczegółowych zabezpieczeń technicznych, gdyż są one uregulowane odrębnymi przepisami i zasadami.

Wśród wymienionych etapów procesu tworzenia polityki bezpieczeństwa informacji szczególną wagę przywiązuje się do projektowania tego systemu. Mniej uwagi poświęca się etapowi wdrożenia, a zwłaszcza zagrożenia implementacji systemu wynikających z działalności człowieka.

Sumując przedstawiony wątek analizy warto zwrócić uwagę na jeszcze jedną kwestię. Otóż, wśród podanych etapów tworzenia polityki ochrony informacji pominięto etap p r e p a r a c j i, który można by nazwać etapem identyfikacji i analizy sytuacji firmy. Efektem pracy wykonanej w ramach tego etapu byłoby określenie potrzeb organizacji w zakresie wspomnianej polityki. W etapie tym w szczególności należałoby zwrócić uwagę na takie determinanty praktyki ochrony informacji, jak: wielkość firmy, jej osobowość prawna, rodzaj prowadzonej działalności, sposób zarządzania oraz przede wszystkim kulturę organizacji i strategię ochrony informacji.

4. Metody ochrony informacji

W literaturze przedmiotu znaleźć można wiele różnych klasyfikacji zabezpieczeń informacji i systemu informatycznego. Jedną z częściej podawanych jest klasyfikacja „rodzajowa" wskazująca na następujące zabezpieczenia [P. Lula, J. Wołoszyn 2001, s. 295—296]:

— zabezpieczenia fizyczne, np. fizyczne zabezpieczenia sprzętu, pomieszczeń, w których się znajdują,

— zabezpieczenia informatyczne, w tym przypadku wykorzystywane są metody i środki informatyczne, np. alarmy, czytniki telewizji przemysłowej itp., zabezpieczają one zarówno sprzęt (*hardware*), jak i oprogramowanie (*software*),

— zabezpieczenia organizacyjne polegają na przeprowadzeniu zmian organizacyjnych mających na celu zwiększenie poziomu bezpieczeństwa systemu,

— zabezpieczenia administracyjne są to wszelkiego rodzaju certyfikaty gwarantujące, że system informacyjny jest bezpieczny. Certyfikacji podlega zarówno oprogramowanie, sprzęt teleinformatyczny, wykorzystywane technologie, a także personel firmy. Najważniejszym elementem tego rodzaju zabezpieczeń jest prawidłowa administracja. Odpowiada za nią administrator. Jest to osoba powołana przez kierownictwo firmy. Posiada on wiedzę w zakresie obsługi systemu teleinformatycznego oraz odpowiednie przeszkolenie w zakresie bezpieczeństwa i ochrony tegoż systemu. Do zadań administratora należy: tworzenie kont użytkowników, określanie ich uprawnień, przeprowadzenie archiwizacji systemu i danych użytkowników, przeprowadzenie kontroli stanu systemu, instalacje mechani-

zmów zabezpieczających system komputerowy przed atakiem za pośrednictwem sieci globalnej,

— zabezpieczenia prawne to szereg uregulowań prawnych, których zadaniem jest ochrona i bezpieczeństwo systemów komputerowych. Należą do nich ustawy, uchwały, dyrektywy, normy prawne (np. ISO/IE C TR 13335 PN-I-13335), rozporządzenia, regulaminy, przepisy BHP itp. W polskim prawodawstwie podstawowymi aktami prawnymi regulującymi te kwestie są:

— Ustawa z 22 stycznia 1999 roku o ochronie informacji niejawnych — określa, które informacje są objęte klauzurą tajności lub niejawności,

— Ustawa z 29 sierpnia 1997 roku o ochronie danych osobowych — określa zasady dostępu i wykorzystania danych osobowych. Jako pierwsza wprowadziła do polskiego prawodawstwa pojęcia polityki bezpieczeństwa, ochrony systemów informatycznych i administratora bezpieczeństwa informacji [J. Kosiński 2000, s. 490],

— Ustawa z 30 października 1992 roku o ochronie topografii układów scalonych,

— Ustawa z 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych,

— Ustawa z 6 czerwca 1997 roku Kodeks karny — reguluje takie zagadnienia, jak: bezprawny dostęp do systemów komputerowych, jego manipulacja, oszustwo komputerowe, sabotaż informacyjny, ataki na system komputerowy instytucji publicznych, które odgrywają szczególną rolę dla bezpieczeństwa Polski i nie tylko (instytucje rządowe, szpitale, obiekty wojskowe itp.),

— Ustawa z 29 września 1994 roku o rachunkowości (rozdział 8 art. 71—76) — reguluje zagadnienia związane z ochroną danych znajdujących się w księgach rachunkowych. Są to głównie dane finansowe.

Środki teleinformatyczne są jedną z metod ochrony i bezpieczeństwa zarówno informacji, jak również systemu informacyjnego. Są to głównie środki techniczne stanowiące uzupełnienie technicznych metod i środków fizycznej ochrony danych i systemów teleinformacyjnych. Wyróżnia się tu rozwiązania sprzętowe, takie jak:

— wprowadzenie redundantnych elementów do systemów komputerowych,
— kryptograficzna ochrona informacji,
— identyfikacja i uwierzytelnienie osób,
— zapewnienie bezpieczeństwa transmisji,
— monitorowanie dostępu do systemu i realizacji zadań,
— przystosowanie systemu operacyjnego,
— ochrona elektromagnetyczna,
— ochrona programowa,
— archiwizacja danych,
— ochrona antywirusowa,
— zabezpieczenie systemu poprzez tzw. ściany przeciwogniowe,
— zabezpieczenie usług internetowych.

W p r o w a d z e n i e r e d u n d a n t n y c h e l e m e n t ó w d o s y s t e m ó w k o m p u t e r o w y c h, to najczęściej stosowana metoda zwiększająca bezpieczeństwo systemów teleinformatycznych. Dokonuje się tu przede wszystkim dublowania źródeł zasilania, instalowania zasilania awaryjnego, które jest automatycznie uruchamiane w przypadku awarii zasilania podstawowego. Ponadto dublowane są urządzenia pamięci masowej [P. Lula, J. Wołoszyn 2001, s. 299]. Najczęściej instaluje się w komputerach dwa lub więcej dysków magnetycznych, bądź optycznych, na których zapisuje się jednocześnie te same informacje. Niekiedy w sieci komputerowej funkcjonującej w przedsiębiorstwie instaluje się — obok serwera podstawowego — kilka serwerów dodatkowych, jak również dodatkowe dyski (tzw. matryce dyskowe), a nawet dodatkowe łącza transmisyjne. Zabezpieczenia te służą przede wszystkim zapewnieniu integralności danych [P. Lula, J. Wołoszyn 2001, s. 299]. Zmniejszają zniekształcenia informacji przerwaniem dopływu źródła zasilania (np. prądu), a nawet zmniejszają ryzyko ich utraty.

K r y p t o g r a f i c z n a o c h r o n a i n f o r m a c j i, to najstarsze metody ochrony informacji. Już w starożytności posługiwano się prostymi szyframi (np. szyfr Cezara, który stworzył Juliusz Cezar). Jednakże z biegiem lat były one modyfikowane i udoskonalane (np. szyfr Thitemiusa jest zmodyfikowanym szyfrem Cezara). Dużą rolę odgrywa tu nieustanny postęp w dziedzinie teleinformatycznej. Są wykorzystywane głównie w celu zapewnienia poufności i integralności informacji. Jego działanie polega na przekształceniu informacji jawnej w jej zaszyfrowaną postać (szyfrogram). Podstawowymi szyframi są:

— Szyfry podstawieniowe, to takie, których bity, znaki lub bloki znaków są zastępowane ich utajnionymi odpowiednikami. Najczęściej stosowanymi szyframi podstawieniowymi są szyfry: monoalfabetyczne (każdej literze alfabetu tekstu jawnego odpowiada jedna litera alfabetu zaszyfrowanego), homofoniczne (każdej literze tekstu jawnego odpowiada kilka liter (tzw. homofon) alfabetu szyfrogramu), poligramowe (szyfrowane są tu grupy liter tekstu jawnego). Najprostszym tego typu szyfrem jest wspomniany już szyfr Cezara.

— Szyfry polialfabetyczne, są połączeniem kilku prostych szyfrów podstawieniowych. Każda litera tekstu jawnego jest zaszyfrowana za pomocą litery z innego alfabetu. Określa się tu jego okresowość poprzez ilość wykorzystywanych alfabetów. Podstawowym szyfrem polialfabetycznym jest szyfr opracowany przez średniowiecznego dominikanina zwany szyfrem Thitemiusa (jako kombinacja szyfru Cezara).

Aby odczytać treść faktyczną zaszyfrowanej informacji należy dokonać jej deszyfracji. Odbywa się ona za pomocą klucza. Jest to zbiór parametrów opisujących konkretne przekształcenie. W praktyce wykorzystuje się dwie metody szyfrowana: symetryczne i asymetryczne.

Metoda asymetryczna to taka, w której do szyfrowania, jak i deszyfrowania informacji tylko jednego, poufnego klucza. Wyróżniamy tu klucze strumieniowe (informacja szyfrowana jest za pomocą strumienia danych, które nie powinny być

krótsze niż zaszyfrowane informacje) oraz klucze blokowe (określonym blokom tekstu jawnego odpowiadają bloki tekstu zaszyfrowanego). Zaletą metody symetrycznej jest stosunkowo niski nakład obliczeń ponoszonych na szyfrowanie i rozkodowanie nawet dużych plików [L. Kiełtyka 2002, s. 528]. Główną wadą jest konieczność dostarczenia klucza odbiorcy informacji. Może on zostać przechwycony w przypadku dostarczania go siecią publiczną. Z kolei w metodach asymetrycznych stosuje się dwa rodzaje kluczy: klucz publiczny nadawcy służący do zaszyfrowania informacji oraz klucz prywatny odbiorcy służący do jej rozszyfrowania. Zaletą tego rodzaju metod szyfrowania jest zagwarantowanie prywatności zarówno osobie przesyłającej, jak i odbierającej wiadomość. Natomiast podstawową wadą jest brak wyraźnego zagwarantowania autentyczności przesłanej informacji. Odbiorca przesyłki nie jest do końca pewien, czy obiekt jest tym za kogo się podaje. Sytuacja taka może prowadzić do różnego typu ataków znanych jako *Man in the Middle* („człowiek w środku"). Aby uniknąć tego typu sytuacji algorytm klucza publicznego stosowany jest wraz z podpisem elektronicznym nadawcy.

Podpis elektroniczny (cyfrowy) jest to zaszyfrowana kombinacja danych personalnych nadawcy opartych o technikę elektroniczną. Charakteryzuje się on następującymi cechami:

— stanowi ciąg znaków (cyfr, liter i innych występujących na klawiaturze komputera), jednoznacznie wiążący dokument podpisany z osobą podpisującą go,

— wymaga podstawowej wiedzy i umiejętności z zakresu informatyki,

— istnieje tylko w środowisku elektronicznym,

— jest zależny od sprzętu komputerowego, jego zasilania i oprogramowania,

— budowany jest na bazie techniki szyfrowania w systemie klucza publicznego,

— może być złożony tylko na dokumencie zakończonym. Osoba podpisująca nie może dokonywać żadnych zmian w dokumencie po jego złożeniu. Spowoduje to spadek podpisu cyfrowego,

— jest tworzony na polecenie podpisującego,

— jednoznacznie wskazuje osobę podpisującą (zawiera jej najważniejsze dane),

— posiada określoną ważność, która jest potwierdzona wydanym w tym celu specjalnym certyfikatem,

— zakres jego stosowania określają obowiązujące przepisy prawne,

— posiadanie podpisu jest kosztowne.

I d e n t y f i k a c j a i u w i e r z y t e l n i e n i e o s ó b, polega ona na sprawdzeniu, czy dana osoba jest rzeczywiście tą, za którą się podaje. W tym celu musi podać poprawne dane przydzielone jej przez administratora sprzętu. Są to identyfikator i hasło użytkownika, a także przydzielony jej sprzętowy element zabezpieczający w postaci karty magnetycznej lub procesorowej. W celu zwiększenia wiarygodności dotyczącej tożsamości danej osoby sprawdza się niekiedy jej

cechy biometryczne, np. linie papilarne. Tego typu zabezpieczenia są stosowane w bankach.

Zapewnienie bezpieczeństwa transmisji, są to środki gwarantujące bezpieczne przesyłanie informacji w systemie informatycznym (zarówno wewnątrz, jak i na zewnątrz przedsiębiorstwa). Stosuje się tu środki bezpieczeństwa takie, jak: mechanizm chroniący przed ujawnieniem informacji o strukturze sieci, kontrola dostępu do sieci, stosowanie systemów zaporowych (tzw. ściany przeciwogniowe itp.).

Monitorowanie dostępu do systemu i realizacji zadań, to środki ochrony mające na celu wykrycie niewłaściwego zachowania użytkowników. Stosuje się tu stały nadzór nad dostępem do informacji szczególnie ważnych dla przedsiębiorstwa, jak również nad osobami mającymi prawo dostępu do nich.

Przystosowanie systemu operacyjnego, polega głównie na: konfiguracji sprzętu, kontroli przepływu informacji, akredytacji, uodpornianiu sprzętu (*hardening*) itp.

Ochrona elektromagnetyczna, to: ochrona urządzeń o niskiej emisji, stosowanie wszelkiego rodzaju osłon instalacji zasilających sprzęt, filtrowanie zasilania itp.

Ochrona programowa, są to wszelkie rozwiązania zabezpieczające zarówno sprzęt, jak i oprogramowanie. Wykorzystuje się tu następujące środki:

— dzienniki systemowe, które pozwalają na późniejszą identyfikację działalności użytkowników,
— programy śledzące,
— mechanizmy rozliczania,
— mechanizmy wspomagające pracę administratorów,
— wirtualne sieci prywatne.

Archiwizacja danych polega na tworzeniu dodatkowych kopii systemu, a także przechowywanych w nim danych. Ma to na celu zapobieżenie ich utracie na skutek awarii. Powinna być przeprowadzana regularnie. Do tego celu wykorzystuje się takie nośniki, jak: dyskietki, płyty magnetyczne, dyski magnetyczne, dyski optyczne itp. Aby zwiększyć bezpieczeństwo danych należy wybrać taki nośnik, który odznacza się największą trwałością i jest najmniej podatny na zniszczenie. Nie powinien być zainstalowany w zabezpieczonym sprzęcie. Powinny być przechowywane w osobnym pomieszczeniu i mieć dodatkowe zabezpieczenia, np. być przechowywane w sejfie. Należy także uwzględnić wielkość przedsiębiorstwa oraz rodzaj prowadzonej działalności. Jeżeli przedsiębiorstwo przechowuje dużą ilość danych (zazwyczaj duże), to zaleca się przeprowadzenie archiwizacji całościowej. W przypadku, gdy ochronie podlegają tylko niektóre dane, to wystarczy przeprowadzić archiwizację częściową (głównie w małych i średnich przedsiębiorstwach). Powinno się je co jakiś czas modyfikować.

Archiwizacje danych przeprowadza powołana przez kierownictwo osoba, która odznacza się odpowiednią wiedzą w tym zakresie, postępująca zgodnie z odpo-

wiednimi przepisami. Niekiedy musi odbyć niezbędne szkolenia. Do obowiązków jej należy sprawdzanie integralności tych nośników oraz testowanie procedury odzyskiwania danych z tych nośników.

Ochrona antywirusowa, to instalacja programów zwalczających wirusy, robaki i konie trojańskie. Instaluje się je w całym systemie informatycznym firmy lub na poszczególnych stanowiskach komputerowych. Mogą być uruchomione przez cały czas, lub na żądanie użytkownika. Z uwagi na możliwość błyskawicznego rozprzestrzeniania się wirusów w skali całego globu skuteczność programów antywirusowych jest uzależniona od regularnej aktualizacji bazy wzorców wykorzystywanej w trakcie monitorowania systemu komputerowego [P. Lula, J. Wołoszyn 2001, s. 303]. Popularnym programem antywirusowym używanym przez firmy i użytkowników indywidualnych jest program o nazwie MksVir.

Zabezpieczenie systemu przez ściany przeciwogniowe (*firewall*), są to wszelkiego rodzaju zabezpieczenia sprzętowo-programowe. Polegają na zainstalowaniu w wybranym komputerze oprogramowania, którego celem jest zarządzanie komunikacją pomiędzy sieciami (zarówno wewnętrzną, jak i zewnętrzną). W celu nieprzedostania się pewnych informacji na zewnątrz organizacji instaluje się takie ściany ogniowe, które ograniczają komunikację pomiędzy sieciami wewnętrzną przedsiębiorstwa i zewnętrznymi. W skrajnym przypadku może być to komunikacja jednokierunkowa — z sieci lokalnej do globalnej [P. Lula, J. Wołoszyn 2001, s. 303]. Można również zablokować przepływ informacji.

Zabezpieczenie usług internetowych, to szereg metod i technik zabezpieczenia informacji znajdujących się w sieci Internet. Do najczęściej wykorzystywanych usług internetowych zaliczamy pocztę elektroniczną oraz strony internetowe (strony world wwide web — www).

Poczta elektroniczna jest cyfrowym odpowiednikiem zwykłej poczty funkcjonującej od dawna. Polega ona na przesyłaniu informacji tekstowych pomiędzy serwerami pocztowymi, jak również dodatkowych załączników w postaci plików, zdjęć, rysunków, grafiki komputerowej itp. Odbywa się to za pomocą specjalnego protokołu SMTP (*Simple Mail Transfer Protocol*). Najczęściej stosowanym zabezpieczeniem przesyłanych informacji jest stosowanie hasła dostępu. Jest to tylko zabezpieczenie częściowe. Aby przekaz informacji był w pełni zabezpieczony należy stosować programy pocztowe zawierające podpis elektroniczny oraz programy szyfrujące je. Programy te mogą także przeprowadzić kompresję przesyłanych wiadomości, które skracają czas ich transferu. Należy pamiętać także o niebezpieczeństwach wynikających z dołączanych przesyłek. Mogą one zawierać m.in. wirusy i robaki komputerowe uaktywniające się po ich otwarciu.

Strony www są — obok poczty elektronicznej — powszechnie stosowaną usługą sieci Internet. Są tworzone zarówno przez firmy, organizacje, a także przez osoby indywidualne. Dostęp do nich odbywa się za pomocą protokołu transferu hipertekstu HTTP (*Hiper Text Transfer Protocol*), lub protokołu transfe-

ru plików FTP (*File Transfer Protocol*). Wykorzystuje się w tym celu odpowiednie przeglądarki, w których wpisuje się odpowiednie adresy stron. Twórca witryn internetowych powinien zatroszczyć się o bezpieczeństwo prezentowanych informacji (ochrona antywirusowa, szyfrowanie ważnych informacji, ograniczanie dostępu do sieci itp.). Bezpieczniejszą odmiana protokołu HTTP jest protokół SHTTP. Wiele przedsiębiorstw, a zwłaszcza banki stosują dodatkowy protokół zabezpieczający informacje zamieszczone na stronach internetowych SSL (*Secure Sockets Loyers*). Zapewnia bezpieczną i wiarygodną komunikację w sieci, głównie w tzw. bankowości internetowej (*i-bankingu*). Gwarantuje on większą prywatność klientom banku poprzez szyfrowanie przesyłanych informacji. Ponadto klient, jak i serwer dokonują autoryzacji przesyłanych danych poprzez określenie swojej tożsamości. Zapewniona jest także integralność przesyłanych informacji (zastosowanie sum kontrolnych).

Ważną sprawą jest bezpieczeństwo transferów internetowych. Są to: przelewy bankowe, zakupy itp., klient nie powinien dopuścić do tego, aby sprzedawca zdobył numer identyfikacyjny jego karty płatniczej. W tym celu powinien dokonywać zakupów za pomocą banku, albo posłużyć się przydzielonym mu kodem certyfikacyjnym, który potwierdza się w urzędzie certyfikacyjnym, który go wydał. Aby sprzedający miał pewność, że transakcja została zawarta z właściwą osobą powinien zażądać od kupującego potwierdzenia jej poprzez użycie podpisu cyfrowego.

Wśród wymienionych i pokrótce scharakteryzowanych metod i technik ochrony informacji na szczególną uwagę zasługują te z nich, które odznaczają się dużą skutecznością i relatywnie wysoką efektywnością ekonomiczną. Należą do nich m.in. metody kryptograficzne, identyfikacja i uwierzytelnienie osób, archiwizacja danych, ochrona programowa, ochrona antywirusowa. Właśnie te techniki należałoby rekomendować firmom, zwłaszcza małym i średnim, a przede wszystkim uświadomienie zagrożenia bezpieczeństwa informacji. Niektórzy właściciele nie odczuwają potrzeby ochrony zgromadzonych danych.

Zakończenie

Jak można zauważyć tematyka bezpieczeństwa i ochrony systemu informacyjnego nie została do końca wyczerpana. Wynika to głównie z jej rozległości i wielowątkowości, jak również wiąże się z nieustannym postępem w dziedzinie informatyki (sprzętu i oprogramowania). Warto przy tym dodać, że pojawiają się nowe zagrożenia, którym należy przeciwdziałać. Wobec powyższego problem stworzenia bezpiecznego systemu komputerowego jest nadal otwarty. Jego rozwiązanie wymaga jednak opracowania kompleksowej i wewnętrznie spójnej metodyki budowy systemu ochrony informacji w organizacji, zwłaszcza w firmie. Proces ten powinien obejmować zarówno etapy, jak i narzędzia badawcze umożli-

wiające ich realizację. Proponuje się więc wyróżnić etapy tworzenia polityki bezpieczeństwa informacji takie, jak:

— analiza i ocena bieżącej sytuacji firmy,
— ewidencja składników systemu informatycznego,
— tworzenie projektu systemu bezpieczeństwa,
— wdrożenie systemu bezpieczeństwa,
— eksploatacja i audyt systemu bezpieczeństwa.

Wśród licznych metod i technik badawczych wykorzystywanych w poszczególnych etapach tworzenia polityki bezpieczeństwa informacji powinna znaleźć się procedura diagnozowania społecznych uwarunkowań tej polityki, ze zwróceniem szczególnej uwagi na proces diagnozowania struktury organizacyjnej firmy.

Bibliografia

Bezpieczeństwo informatyczne — zabezpieczenie dostępu logistycznego, „Rachunkowość", nr 6 z 2004.

Bezpieczeństwo informatyczne — zabezpieczenia mechaniczne, „Rachunkowość", nr 1 z 2004.

Kiełtyka L., *Komunikacja w zarządzaniu*, Agencja Wydawnicza Placet, Warszawa 2002.

Kiełtyka L., *Zarządzanie bezpieczeństwem informacji*, „Współczesne Zarządzanie" nr 3/2003.

Kosiński J., *Bezpieczeństwo danych i systemów teleinformatycznych* [w:] *Zarządzanie bezpieczeństwem*, pod red. P. Tyrały, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 2000.

Lula P., Wołoszyn J., *Informatyczne metody i środki ochrony zasobów informatycznych przedsiębiorstwa* [w:] *System informacji strategicznej. Wywiad gospodarczy a konkurencyjność przedsiębiorstwa*, pod red. R. Borowieckiego i M. Romanowskiej, Diffin, Warszawa 2001.

Madej J., *Polityka bezpieczeństwa i system ochrony informacji w przedsiębiorstwie*, Zeszyty Naukowe Akademii Ekonomicznej w Krakowie, Zeszyt nr 604, Kraków 2002.

Mascha M. F., *Stop E-Mail Snoops*, „Journal of Accounting", nr 7, sierpień 2002.

Martinet B., Marti Y. M., *Wywiad gospodarczy. Pozyskiwanie i ochrona informacji*, PWE, Warszawa 1999.

Sieja M., Wach K., *Rola bezpieczeństwa danych w budowie i utrzymaniu przewagi konkurencyjnej banków internetowych* [w:] *Informacja i wiedza w zintegrowanym systemie zarządzania*, pod red. R. Borowieckiego i M. Kwiecińskiego, Zakopane — Kraków 2004.

Szmit M., *Informatyka w zarządzaniu*, Diffin, Warszawa 2003.

Wołoszyn J., Lula P., *Informatyczne metody i środki ochrony zasobów informacyjnych przedsiębiorstwa* [w:] *Zarządzanie informacją i komunikacją*, pod red. Z. Martyniaka, Wydawnictwo Akademii Ekonomicznej w Krakowie, Kraków 2000.