Zeszyty Naukowe nr 770 2009
Uniwersytetu Ekonomicznego w Krakowie

Jan Madej
Katedra Informatyki
Katarzyna Szymczyk-Madej
Katedra Informatyki

Prawne wymogi bezpieczeństwa systemów informatycznych w polskich przedsiębiorstwach według kodeksu karnego, ustawy o rachunkowości i ustawy o ochronie danych osobowych

Streszczenie. Artykuł poświęcony jest wymogom bezpieczeństwa systemów informatycznych, jakie nakładają na polskie przedsiębiorstwa obowiązujące przepisy prawa. Przedstawiono w nim najważniejsze akty prawne, które kształtują sytuację w zakresie bezpieczeństwa SI w Polsce. Wynikające z przepisów wymogi prawne zostały scharakteryzowane i poddane analizie, co pozwoliło na wyciągnięcie ogólnego wniosku dotyczącego obowiązku zapewnienia kompleksowej ochrony systemom informatycznym w polskich przedsiębiorstwach.

Słowa kluczowe: bezpieczeństwo systemów informatycznych, ochrona informacji, kodeks karny, ustawa o rachunkowości, ustawa o ochronie danych osobowych.

1. Wstęp

We współczesnej gospodarce troska przedsiębiorstw o bezpieczeństwo swoich systemów informatycznych (SI) nie jest dobrowolną praktyką, lecz koniecznością i obowiązkiem. Obowiązek ten nakładają na nie m.in. odpowiednie przepisy

prawne, które obligują przedsiębiorstwa do zapewnienia ochrony zgromadzonym w systemach danym oraz przewidują odpowiedzialność karną za ich nieprzestrzeganie. Do podstawowych aktów prawnych, które mają wpływ na bezpieczeństwo i ochronę danych w systemach informatycznych polskich przedsiębiorstw należą ustawy: Kodeks karny [k.k. 1997], o rachunkowości [1994], o ochronie danych osobowych [ustawa ODO 1997][1].

Celem niniejszego artykułu jest pokazanie, w jaki sposób ustawy te nakładają na polskie przedsiębiorstwa obowiązek ochrony systemów informatycznych i kształtują sytuację prawną w tym zakresie.

2. Kodeks karny

Podstawowym aktem prawnym w zakresie prawa karnego jest ustawa Kodeks karny [k.k. 1997]. Ustawa ta[2], chroniąc polskie przedsiębiorstwa przed tzw. przestępstwami komputerowymi naruszającymi bezpieczeństwo systemów informatycznych, wymaga zarazem spełnienia określonych warunków, dzięki którym przedsiębiorstwom przysługuje ochrona.

Ujawnienie informacji wbrew zobowiązaniu

Zgodnie z Kodeksem karnym (art. 266 §1) każda osoba, która „wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu ujawnia lub wykorzystuje informację, z którą zapoznała się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2". Oznacza to, że jeżeli informacja nie jest chroniona z mocy ustawy, to ochrona prawna przysługuje jej tylko wtedy, kiedy pracownik zobowiąże się jej nie ujawniać. Wynika z tego ważny wniosek: jeżeli w przedsiębiorstwie konieczne jest zachowanie poufności informacji, które nie są chronione ustawowo, to należy wymagać od pracowników zobowiązania (najlepiej pisemnego), że nie będą ich ujawniać lub wykorzystywać.

[1] Oprócz nich istnieją także akty prawne, które, choć w mniejszym stopniu, również wpływają na sytuację w tym zakresie. Są to ustawy o ochronie informacji niejawnych [ustawa OIN 1999], o prawie autorskim i prawach pokrewnych [ustawa PAiPP 1994], o systemie ubezpieczeń społecznych [ustawa SUS 1998], o podpisie elektronicznym [ustawa PE 2001], o zwalczaniu nieuczciwej konkurencji [ustawa ZNK 1993]. Zostały one omówione w kolejnym artykule zamieszczonym na str. 109.

[2] Wprowadzenie przez Kodeks prawnej ochrony informacji stało się tematem wielu publikacji: (np. [Fischer 1997b, 1997a, 1997c, 2000], [Adamski 1998a, 1998b], [Wójcik 1998, 1999], [Jakubski 1999]).

Niszczenie i fałszerstwo dokumentów

Kodeks karny przyjął ważną, w celu ochrony i funkcjonowania systemów informatycznych, definicję dokumentu. Zgodnie z nią (art. 115 §14) „dokumentem jest każdy przedmiot lub zapis na komputerowym nośniku informacji, z którym jest związane określone prawo albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne". Dokumenty mogą mieć więc także postać elektroniczną, a kodeks przewiduje wysokie kary za ich fałszowanie[3] oraz niszczenie, ukrywanie i usuwanie[4].

Nieuprawnione uzyskanie i podsłuch informacji

Podstawowe dla bezpieczeństwa systemów informatycznych przepisy znajdują się w kodeksie w rozdz. XXXIII pt. „Przestępstwa przeciwko ochronie informacji". Zgodnie z art. 267 karalne jest nieuprawnione pozyskiwanie informacji[5], podsłuch informacji[6] oraz ujawnianie nielegalnie zdobytych informacji[7].

Należy jednak zauważyć, że z treści art. 267 §1 wynika (zob. przypis 4), że chroni on poufność danych zawartych w systemach informatycznych, ale ochrona ta uzależniona jest od „przełamania" przez sprawcę zabezpieczeń. Wynika stąd ważny wniosek: aby móc korzystać z prawnej ochrony poufności, informacje muszą zostać najpierw odpowiednio zabezpieczone[8]. Wymóg ten, zgodnie z art. 267 §2, nie dotyczy sytuacji, w której osoba nieuprawniona wykorzystuje podsłuch.

Sabotaż komputerowy

Kodeks karny chroni także system informatyczny i zawarte w nim dane przed aktami tzw. sabotażu komputerowego, którego celem jest zniszczenie bądź uszko-

---

[3] Art. 270 §1: „Kto, w celu użycia za autentyczny, podrabia lub przerabia dokument lub taki dokument jako autentyczny używa, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności od 3 miesięcy do lat 5".

[4] Art. 276: „Kto niszczy, uszkadza, czyni bezużytecznym, ukrywa lub usuwa dokument, którym nie ma prawa wyłącznie rozporządzać, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2".

[5] Art. 267 §1: „Kto bez uprawnienia uzyskuje informację dla niego nieprzeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2".

[6] Art. 267 §2: „Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym".

[7] Art. 267 §3: „Tej samej karze podlega, kto informację uzyskaną w sposób określony w §1 lub 2 ujawnia innej osobie".

[8] Ponieważ przepis mówi o przełamywaniu zabezpieczeń, dlatego zabezpieczenia te powinny stanowić realną, a nie symboliczną przeszkodę, mającą uniemożliwiać osobom nieuprawnionym zapoznanie się z informacjami.

dzenie danych lub urządzeń należących do systemu (art. 269 i 287)[9]. Pomimo że art. 269 ma pewne ograniczenia co do charakteru chronionej informacji i wykorzystywanych urządzeń, przyjmuje się, że chroni on także systemy telekomunikacyjne, a w szczególności lokalne i rozległe sieci komputerowe [Adamski 1998a]. Ponadto sabotaż komputerowy jest karalny także na podstawie art. 287 §1, w którym nie ma już żadnych ograniczeń co do charakteru informacji.

Niszczenie lub zmiana istotnej informacji

Zniszczenie, uszkodzenie lub zmiana informacji w myśl art. 268 §1 Kodeksu karnego traktowane jest jako czyn niedozwolony i podlega karze[10]. Na szczególną uwagę zasługuje §2 tego artykułu[11], który przewiduje większą karę za zniszczenie informacji zapisanej elektronicznie niż na papierze. Jest to wyraz uznania przez ustawodawcę roli, jaką odgrywa w obecnych czasach ta forma danych.

Bez względu na motywy każdy z tych czynów podlega karze pod warunkiem, że informacja jest istotna. W kodeksie brakuje definicji takiej informacji, co oznacza, że rozstrzygnięcie tej kwestii pozostawione zostało sądom. Ponadto w wypadku tego rodzaju przestępstw ma także zastosowanie art. 287 §1.

Nielegalne uzyskanie i paserstwo programów komputerowych

Zgodnie z art. 278 i 293 (rozdz. XXXV pt. „Przestępstwa przeciwko mieniu"), karalne jest nielegalne uzyskanie i paserstwo programów komputerowych. Potocznie czyny te utożsamiane są z tzw. piractwem komputerowym. Zgodnie z art. 278 §1, osoba, która „zabiera w celu przywłaszczenia cudzą rzecz ruchomą, podlega karze pozbawienia wolności od 3 miesięcy do lat 5". Zgodnie z §2 „tej samej karze podlega, kto bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy w celu osiągnięcia korzyści majątkowych".

[9] Art. 269 §1: „Kto na komputerowym nośniku informacji, niszczy, uszkadza, usuwa lub zmienia zapis o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji lub funkcjonowania administracji rządowej […] albo zakłóca lub uniemożliwia automatyczne gromadzenie lub przekazywanie takich informacji podlega karze pozbawienia wolności od 6 miesięcy do lat 8".

Art. 269 §1: „Tej samej karze podlega, kto dopuszcza się czynu określonego w §1, niszcząc albo wymieniając nośnik informacji lub niszcząc albo uszkadzając urządzenie służące automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji".

Art. 287 §1: „Kto w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji lub zmienia, usuwa albo wprowadza nowy zapis na komputerowym nośniku informacji, podlega karze pozbawienia wolności od 3 miesięcy do lat 5".

[10] Art. 268 §1: „Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2".

[11] Art. 268 §2: „Jeżeli czyn określony w §1 dotyczy zapisu na komputerowym nośniku informacji, sprawca podlega karze pozbawienia wolności do lat 3".

Ponadto art. 293 §1 informuje, że zastosowanie do programu komputerowego mają przepisy art. 291 i 292. Grożą one karą pozbawienia wolności od 3 miesięcy do lat 5 osobie, która nabywa, pomaga w zbyciu albo przyjmuje rzecz „uzyskaną za pomocą czynu zabronionego" (art. 291 §1) oraz grzywną, karą ograniczenia albo pozbawienia wolności do lat 2 osobie, która nabywa, pomaga w zbyciu lub przyjmuje rzecz „o której na podstawie towarzyszących okoliczności powinna i może przypuszczać, że została uzyskana za pomocą czynu zabronionego" (art. 292 §1).

Oszustwo komputerowe i telekomunikacyjne

Nieuprawnione oddziaływanie na system informatyczny i zawarte w nim dane celem osiągnięcia korzyści majątkowych lub wyrządzenia innej osobie szkody traktowane jest jako tzw. oszustwo komputerowe i zgodnie z art. 287 §1 Kodeksu podlega karze pozbawienia wolności od 3 miesięcy do 5 lat (zob. przypis 9). Przepis ten kładzie nacisk na motywy sprawcy (np. osiągnięcie korzyści majątkowych), a nie na sposób popełnienia czynu, dlatego może mieć zastosowanie do różnych rodzajów przestępstw komputerowych. Dodatkowo zagrożenie karą jest większe (od roku do lat 10) przez art. 294 §1, jeżeli szkoda lub osiągnięte korzyści majątkowe są znacznej wartości.

Karę pozbawienia wolności do lat 3 przewiduje art. 285 §1 za tzw. oszustwo telekomunikacyjne – tzn. wykorzystywanie impulsów telefonicznych na cudzy rachunek[12].

Zagrożenie zdrowia, życia lub mienia o znacznej wartości oraz szpiegostwo komputerowe

W rozdz. XX Kodeksu karnego pt. „Przestępstwa przeciwko bezpieczeństwu powszechnemu" karą pozbawienia wolności zagrożone jest sprowadzanie niebezpieczeństwa dla życia lub zdrowia wielu osób albo mienia o znacznej wartości poprzez oddziaływanie na system informatyczny (art. 165 §1 pkt 4)[13]. Dla karalności tego czynu nie są ważne motywy sprawcy, ale za czyn nieumyślny grozi niższa kara – pozbawienie wolności do lat 3 (art. 165 §2).

Czynem karalnym, zaliczanym również do przestępstw komputerowych, jest szpiegostwo. Obecnie technologia informatyczna dostarcza metod i narzędzi zarówno do uzyskiwania, jak i przekazywania informacji, którymi może być zainteresowany obcy wywiad. W rozdz. XVII Kodeksu pt. „Przestępstwa przeciwko

[12] Art. 285 §1: „Kto, włączając się do urządzenia telekomunikacyjnego, uruchamia na cudzy rachunek impulsy telefoniczne, podlega karze pozbawienia wolności do lat 3".

[13] Art. 165 §1 pkt 4: „Kto sprowadza niebezpieczeństwo dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach […] zakłócając, uniemożliwiając lub w inny sposób wpływając na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji, podlega karze pozbawienia wolności od 6 miesięcy do lat 8".

Rzeczypospolitej Polskiej" za taki czyn, zgodnie zart. 130 §3, przewidziana jest kara pozbawienia wolności[14].

Tabela 1. Zagrożenie karą czynów naruszających bezpieczeństwo systemu informatycznego

Czyn podlegający karze	Podstawa prawna	Zagrożenie karą
Ujawnienie informacji wbrew zobowiązaniu	art. 266 §1	grzywna, ograniczenie lub pozbawienie wolności do lat 2
Niszczenie dokumentów	art. 276	grzywna, ograniczenie lub pozbawienie wolności do lat 2
Fałszerstwo dokumentów	art. 270 §1	grzywna, ograniczenie lub pozbawienie wolności od 3 miesięcy do lat 5
Niszczenie lub zmiana istotnej informacji na nośniku papierowym	art. 268 §1	grzywna, ograniczenie lub pozbawienie wolności do lat 2
– wyrządzenie tym znacznej szkody	art. 268 §3	pozbawienie wolności od 3 miesięcy do lat 5
Niszczenie lub zmiana istotnej informacji na nośniku komputerowym	art. 268 §2	pozbawienie wolności do lat 3
– wyrządzenie tym znacznej szkody	art. 268 §3	pozbawienie wolności od 3 miesięcy do lat 5
– w celu osiągnięcia korzyści majątkowych lub wyrządzenia szkody	art. 287 §1	pozbawienie wolności od 3 miesięcy do lat 5
– w stosunku do mienia znacznej wartości	art. 294 §1	pozbawienie wolności od roku do lat 10
Nieuprawnione uzyskanie i podsłuch informacji	art. 267 §1–2	grzywna, ograniczenie lub pozbawienie wolności do lat 2
Sabotaż komputerowy		
– skierowany przeciw bezpieczeństwu kraju lub organom władzy	art. 269 §1–2	pozbawienie wolności od 6 miesięcy do lat 8
– w celu osiągnięcia korzyści majątkowych lub wyrządzenia szkody	art. 287 §1	pozbawienie wolności od 3 miesięcy do lat 5
– w przypadku czynu mniejszej wagi	art. 287 §2	grzywna, ograniczenie lub pozbawienie wolności do roku
Nielegalne uzyskanie programów	art. 278 §1–2	pozbawienie wolności od 3 miesięcy do lat 5
– w wypadku czyny mniejszej wagi	art. 278 §3	grzywna, ograniczenie lub pozbawienie wolności do roku

[14] Art. 130 §3: „Kto, w celu udzielenia obcemu wywiadowi wiadomości […] gromadzi je lub przechowuje, włącza się do sieci komputerowej w celu ich uzyskania albo zgłasza gotowość działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności od 6 miesięcy do lat 8".

cd. tabeli 1

Czyn podlegający karze	Podstawa prawna	Zagrożenie karą
Paserstwo programów	art. 291 §1	pozbawienie wolności od 3 miesięcy do lat 5
– w wypadku czynu mniejszej wagi	art. 291 §2	grzywna, ograniczenie lub pozbawienie wolności do roku
– gdy powinno się i można przypuszczać, że uzyskano je w sposób zabroniony	art. 292 §1	grzywna, ograniczenie lub pozbawienie wolności do lat 2
w wypadku ich znacznej wartości	art. 292 §2	pozbawienie wolności od 3 miesięcy do lat 5
Oszustwo komputerowe	art. 287 §1	pozbawienie wolności od 3 miesięcy do lat 5
– w przypadku czynu mniejszej wagi	art. 287 §2	grzywna, ograniczenie lub pozbawienie wolności do roku
– w stosunku do mienia znacznej wartości	art. 294 §1	pozbawienie wolności od roku do lat 10
Oszustwo telekomunikacyjne	art. 285 §1	pozbawienie wolności do lat 3
Zagrożenie zdrowia, życia lub mienia znacznej wartości	art. 165 §1	pozbawienie wolności od 6 miesięcy do lat
– spowodowanie śmierci (ciężkiego uszczerbku zdrowia wielu osób)	art. 165 §3	pozbawienie wolności od lat 2 do 12
– gdy jest to działanie nieumyślne	art. 165 §2	pozbawienie wolności do lat 3
– gdy spowodowano śmierć (ciężki uszczerbek zdrowia wielu osób)	art. 165 §4	pozbawienie wolności od 6 miesięcy do lat 8
Szpiegostwo przy użyciu komputera	art. 130 §3	pozbawienie wolności od 6 miesięcy do lat 8

Źródło: opracowanie własne na podstawie [k.k. 1997].

Analiza przepisów Kodeksu karnego wykazała, że obejmuje on swoim zakresem wiele czynów, których popełnienie narusza bezpieczeństwo systemu informatycznego i przewiduje za nie dotkliwe kary (tabela 1). Jednak na problem ten nie można patrzeć tylko przez pryzmat aktów prawnych i przyjąć, że skoro czyny zagrażające bezpieczeństwu SI są karalne, to sytuacja jest zadowalająca. W rzeczywistości istotniejsza jest skuteczność wymiaru sprawiedliwości w tym zakresie, a na to mają wpływ także inne czynniki, takie jak np.: zgłaszanie organom ścigania popełnionych przestępstw komputerowych, ich wykrywalność oraz orzekanie przez sądy o ich karalności.

Tymczasem przykładowo liczba wykrytych przez policję podstawowych przestępstw komputerowych wyniosła w 2002 r. 816, a w 2003 r. 540 (zob. tabela 2). Ponieważ wykrywalność tych przestępstw sięga około 70% [KGP www], wynika z tego, że w 2003 r. tylko w sprawie około 800 przestępstw wszczęto postępowania. Brakuje danych o tym, ile wniosków o wszczęciu postępowania zostało odrzuco-

nych. Nie ma też dokładnych informacji danych, ile przestępstw komputerowych nie zostało w ogóle zgłoszonych do organów ścigania[15].

Niewielką liczbę zgłaszanych przypadków naruszenia bezpieczeństwa – nie tylko policji, ale i prokuraturze – potwierdza wielu autorów oraz raporty różnych organizacji (por. np.: [*Przypadki*…, 2000], [Jakubski 1999], [Fischer 2000], Adamski 2001]).

Tabela 2. Liczba wykrytych przez policję przestępstw komputerowych w latach 1999–2008

Rok	Oszustwo komputerowe art. 287 §1–2	Ujawnienie tajemnicy służbowej i zawodowej art. 266 §1–2	Nieuprawnione uzyskanie informacji art. 267 §1–3	Zniszczenie lub zmiana istotnej informacji art. 268 §1–3	Zniszczenie lub zmiana informacji art. 269 §1–2
1999	217	32	113	49	1
2000	323	27	240	48	5
2001	279	48	175	118	5
2002	368	54	215	167	12
2003	168	–	232	138	2
2004	390	–	248	89	0
2005	568	–	260	98	3
2006	444	–	370	136	4
2007	492	–	384	168	0
2008	404	–	505	249	2

Źródło: opracowanie własne na podstawie: [KGP www].

3. Ustawa o rachunkowości

W Polsce podstawowym aktem prawnym w dziedzinie rachunkowości jest ustawa o rachunkowości [1994]. Jej pierwotna treść została poddana późniejszym zmianom, a w 2001 r. nowelizacji. Od 1 stycznia 2002 r. obowiązuje jej znowelizowana postać, często określana mianem nowej ustawy o rachunkowości.

[15] Z badań przeprowadzonych w Stanach Zjednoczonych wynika, że w 1998 r. 64% przedsiębiorstw padło ofiarą nadużyć komputerowych, w Wielkiej Brytanii było to 48%. Specjaliści są zgodni, że co roku liczba ta ulega zwiększeniu [Siłuszek 2000].

Skuteczne realizowanie przez rachunkowość swoich funkcji[16] musi opierać się na wiarygodnych dowodach księgowych, dlatego ustawa o rachunkowości zabiega o to, aby dowody te charakteryzowały się m.in. [Dziedziczak, Stępniewski 1999]:

– bezbłędnością (art. 22 ust. 1), poprawnością (art. 22 ust. 1–3) i prawidłowością (art.20–23, 27, 73),

– dostępnością (art. 11 ust. 3, 4, art. 73 1 i art. 75 ust. 1, 2), dyspozycyjnością (art. 73 ust. 1 i art. 76) i użytecznością (art. 20 ust. 2),

– kompletnością (art. 21, art. 22 ust. 4) i rzetelnością (art. 22 ust. 1),

– koniecznością archiwizowania (art. 74 ust. 2, 3), zapewnieniem bezpieczeństwa i poufności (art. 71 ust. 1),

– systematycznością (art. 20 ust. 2–4 i inne rozporządzenia oraz przepisy),

– niezmiennością (art. 20, ust. 5, pkt 4).

Sprostanie przedstawionym wymaganiom stawianym wobec dowodów księgowych nie jest łatwe. Obecnie dowody księgowe mogą być zarówno papierowe, jak i wprowadzane „automatycznie za pośrednictwem urządzeń łączności, komputerowych nośników danych lub tworzone według algorytmu (programu) na podstawie informacji zawartych w księgach" (art. 20 ust. 5) pod warunkiem, że:

– „uzyskają one trwale czytelną postać zgodną z treścią odpowiednich dowodów księgowych,

– możliwe jest stwierdzenie źródła ich pochodzenia oraz ustalenie osoby odpowiedzialnej za ich wprowadzenie,

– stosowana procedura zapewnia sprawdzenie poprawności przetworzenia odnośnych danych oraz kompletności i identyczności zapisów,

– dane źródłowe w miejscu ich powstania są odpowiednio chronione, w sposób zapewniający ich niezmienność, przez okres wymagany do przechowywania danego rodzaju dowodów księgowych".

Z powyższych warunków wynika ważny wniosek – aby w świetle prawa uznać zapis (dokument) za dowód księgowy, musi być zapewniona jego odpowiednia ochrona. Spełnienie tego warunku w praktyce możliwe jest tylko dzięki wdrożeniu w przedsiębiorstwie odpowiednich zabezpieczeń, tym bardziej, że

[16] Uwzględniając przyjęte definicje rachunkowości, zarówno jako nauki, jak i systemu, wyróżnia się następujące, pełnione przez nią funkcje [Dobija 2000]:

– ekonomiczną – służy do mierzenia wielkości ekonomicznych,

– sprawozdawczą – pozwala na okresowe generowanie sprawozdań przeznaczonych zarówno dla podmiotów wewnętrznych, jak i zewnętrznych,

– homeostatyczną – umożliwia jednostce przetrwanie dzięki utrzymywaniu zbioru określonych wielkości ekonomicznych we właściwych granicach,

– podatkową – na jej podstawie rozwija się pomiar wielkości podatków,

– komunikacyjną – generuje informacje dla środowiska społecznego,

– statystyczną – dostarcza informacji statystyce jednostki i państwa,

– dowodową – jest środkiem dowodowym w działalności gospodarczej.

ustawodawca jednoznacznie nakłada na jednostkę obowiązek posiadania systemu ochrony danych. Zagadnieniu temu poświęcony jest cały rozdział ustawy (rozdz. 8, pt. „Ochrona danych"), w którym ustawodawca stwierdza m.in., że zbiory[17] należy (art. 71 ust. 1) „przechowywać w należyty sposób i chronić przed niedozwolonymi zmianami, nieupoważnionym rozpowszechnianiem, uszkodzeniem lub zniszczeniem".

Nie daje jednak odpowiedzi na pytanie, jakie zabezpieczenia mają do tego służyć. W zamian podkreśla tylko, że ochrona danych powinna polegać na (art. 71 ust. 2):

– „stosowaniu odpornych na zagrożenia nośników danych,

– doborze stosownych środków ochrony zewnętrznej,

– systematycznym tworzeniu rezerwowych kopii zbiorów danych zapisanych na nośnikach komputerowych pod warunkiem zapewnienia trwałości zapisu informacji […] przez czas nie krótszy od wymaganego do przechowywania ksiąg rachunkowych,

– stosowaniu odpowiednich rozwiązań programowych i organizacyjnych, chroniących przed nieupoważnionym dostępem lub zniszczeniem".

Takie wytyczne nie wskazują żadnego konkretnego sposobu postępowania i niejednokrotnie stwarzają problemy osobom odpowiedzialnym za funkcjonowanie systemu rachunkowości. Zaletą takiego podejścia ustawodawcy do zagadnienia ochrony danych jest nieskrępowane rozwijanie się różnych rozwiązań informatycznych, które na swój sposób próbują sprostać przedstawionym wymaganiom. Ustawodawca, przewidując zapewne taką możliwość, nałożył na jednostki obowiązek posiadania kompletnej dokumentacji systemu. W związku z czym jednostki muszą posiadać m.in. (art. 10 ust. 1):

– „wykaz zbiorów danych tworzących księgi rachunkowe na komputerowych nośnikach danych,

– opis systemu informatycznego, zawierający wykaz programów, procedur lub funkcji […] wraz z opisem algorytmów i parametrów oraz programowych zasad ochrony danych, w tym w szczególności metod zabezpieczenia dostępu do danych i systemu ich przetwarzania,

– opis systemu służącego ochronie danych i ich zbiorów".

Za utworzenie i aktualizację dokumentacji odpowiedzialny jest kierownik jednostki (art. 10 ust. 2). Niewywiązywanie się z tych obowiązków traktowane jest jako prowadzenie ksiąg wbrew przepisom ustawy i podlega grzywnie lub karze pozbawienia wolności do lat dwóch, albo obu tym karom łącznie (art. 77).

Z treści ustawy wynika ważny wniosek dotyczący bezpieczeństwa SI – przedsiębiorstwo musi posiadać dokument opisujący system informatyczny i system

[17] Pod tym pojęciem ustawodawca rozumie księgi rachunkowe, dowody księgowe, dokumenty inwentaryzacyjne i sprawozdania finansowe (art. 71 ust. 1).

ochrony danych. Dokument taki powinien zawierać przyjęte rozwiązania w zakresie m.in. ochrony programów i urządzeń komputerowych, tworzenia kopii rezerwowych, sprawdzania tożsamości użytkowników mających dostęp do danych. Oznacza to, że odpowiada on, w dużej mierze, „dokumentowi polityki bezpieczeństwa".

4. Ustawa o ochronie danych osobowych

Podstawowym aktem prawnym w zakresie ochrony danych osobowych jest ustawa o ochronie danych osobowych [ustawa ODO 1997, nr 133, poz. 883]. Ustawa ma zastosowanie do „organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych oraz podmiotów niepaństwowych realizujących zadania publiczne" (art. 3 ust. 1). Ponadto „ustawę stosuje się również do osób fizycznych i prawnych oraz jednostek organizacyjnych niemających osobowości prawnej, które przetwarzają dane w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych" (art. 3 ust. 2). Ustawy nie stosuje się do „osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych lub domowych" (art. 3 ust. 4).

Ustawa określa, co należy rozumieć pod pojęciem danych osobowych. Zgodnie z nią (art. 6 ust. 1), „za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej"[18]. Ta bardzo szeroka definicja danych osobowych została zawężona dzięki zaznaczeniu w art. 6 ust. 3, że „informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu i działań"[19].

Zgodnie z art. 7 pkt 1 „zbiór danych osobowych […] to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie". Zbiory z danymi osobowymi, na podstawie art. 40, muszą być zarejestrowane w biurze Generalnego Inspektora Ochrony Danych Osobowych[20], który

[18] Według ustawy w art. 3 ustęp 2 „osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne". Ustawodawca formułując artykuł 6 ustawy, posłużył się klauzulą ogólną i nie określił zamkniętego zestawu informacji, które mają być uznane za dane osobowe.

[19] Ponieważ w ustawie nie zostało podane, jak należy rozumieć pojęcie „nadmierne koszty", dlatego przyjmuje się, że danymi osobowymi są te dane, które pozwalają na natychmiastową identyfikację konkretnej osoby lub na określenie jej tożsamości przy pewnym nakładzie kosztów, czasu i działań [*Zadania administratora*…, 2002].

[20] Wraz z wejściem w życie ustawy na podstawie jej 8 art. został powołany także urząd *Generalnego Inspektora Ochrony Danych Osobowych* (GIODO). Jest to organ do spraw ochrony danych

wydaje zgodę na ich przetwarzanie. Zgoda taka jest uwarunkowana m.in. zastosowaniem odpowiednich zabezpieczeń, określonych w ustawie (rozdz. 5), a rozwiniętych w rozporządzeniu MSWiA [1998]. Jednak nie wszystkie zbiory danych muszą być zgłoszone do rejestracji. Z tego obowiązku zwolnieni są m.in. administratorzy „danych dotyczących osób u nich zatrudnionych, zrzeszonych lub uczących się" (art. 43 ust. 1 pkt 4) oraz przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej (art. 43 ust. 1 pkt 8). Wynika z tego, że pracodawca nie ma obowiązku rejestracji zbiorów z danymi osobowymi swoich pracowników ani z danymi kontrahentów, co nie oznacza, że jest on zwolniony z przestrzegania przepisów ustawy i stosownych rozporządzeń.

Ważnym elementem w funkcjonowaniu ustawowego systemu ochrony danych osobowych jest określenie podmiotu odpowiedzialnego za ich ochronę. Według ustawodawcy jest nim „administrator danych osobowych" (ADO), czyli „organ, instytucja, jednostka organizacyjna, podmiot lub osoba […] decydująca o celach i środkach przetwarzania danych osobowych" (art. 7). Oznacza to, że administrator danych osobowych to nie funkcja, ale status związany z przetwarzaniem danych osobowych. W praktyce administratorem danych osobowych jest np. każde przedsiębiorstwo, ponieważ w ramach systemu kadrowego przechowuje i przetwarza dane swoich pracowników. Administrator może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych (art. 31 ust. 1). Jednak zlecenie to nie powoduje zmiany statusu przedsiębiorstwa jako administratora danych, ani wyłączenia jego odpowiedzialności za niezgodne z prawem przetwarzanie danych osobowych.

Ustawa, przede wszystkim w rozdz. 5, pt. „Zabezpieczenie zbiorów danych osobowych", nakłada na administratora danych wiele obowiązków, m.in.: obowiązek zapewnienia właściwej ochrony zbiorom danych osobowych (ich poufności, integralności i dostępności)[21], obowiązek zapewnienia rozliczalności danych[22],

osobowych powoływany i odwoływany przez Sejm RP za zgodą Senatu. Szczegółowe informacje o funkcjonowaniu tego urzędu można znaleźć w jego corocznych sprawozdaniach (np. [*Sprawozdanie…*, 2001, 2002]).

[21] Art. 36: „Administrator danych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem".

[22] Art. 38: „Administrator danych przetwarzanych w systemie informatycznym jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane, zwłaszcza gdy przekazuje się je za pomocą urządzeń teletransmisji danych".

obowiązek zapewnienia autentyczności danych[23] oraz obowiązek powołania osób upoważnionych do obsługi systemu informatycznego[24]. Ponadto szczegółowe wytyczne dotyczące obowiązków administratora danych oraz warunków, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zostały określone zgodnie z ustawą (art. 45) w Rozporządzeniu MSWiA [1998].

Rozporządzenie to jest bardzo szczegółowe. Jest to jedyny akt prawny, który tak dokładnie precyzuje wymagania i obowiązki w zakresie bezpieczeństwa SI. Na jego podstawie do głównych obowiązków ADO należy m.in. [Rozporządzenie MSWiA 1998]:

– określenie celów, strategii i polityki bezpieczeństwa systemów informatycznych, w których przetwarzane są dane osobowe (§2 pkt 1),

– identyfikacja i analiza zagrożeń oraz ryzyka w tych systemach (§2 pkt 2),

– określenie potrzeb w zakresie zabezpieczeń adekwatnych do zagrożeń i ryzyka (§2 pkt. 3–4),

– monitorowanie skuteczności wdrożonych zabezpieczeń (§2 pkt 5),

– opracowanie i wdrożenie programu szkoleń z zakresu bezpieczeństwa (§2 pkt 6),

– wykrywanie i właściwe reagowanie na przypadki naruszenia zasad bezpieczeństwa (§2 pkt 7),

– wyznaczenie administratora bezpieczeństwa informacji, odpowiedzialnego bezpośrednio za bezpieczeństwo danych w systemie informatycznym (§3),

– określenie indywidualnej odpowiedzialności osób za utrzymanie bezpieczeństwa danych w zakresie swoich czynności służbowych (§4) oraz zaznajomienie ich z przepisami dotyczącymi ochrony danych osobowych (§5),

– opracowanie instrukcji określających sposób postępowania w sytuacjach naruszenia ochrony danych osobowych (§6) oraz instrukcji zarządzania systemem informatycznym dotyczących m.in. zarządzania hasłami, rejestrowania użytkowników, zasad korzystania ze stanowisk komputerowych oraz sieci, metod i czę-

[23] Art. 26 ust. 1: „Administrator danych przetwarzający dane […] jest obowiązany zapewnić, aby dane te były: […] merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane […], przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą.

[24] Art. 37: „Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych, mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez administratora danych".

Art. 39 ust. 1: „Administrator danych prowadzi ewidencję osób zatrudnionych przy ich przetwarzaniu".

Art. 39 ust. 2: „Osoby, o których mowa w ust. 1, mające dostęp do danych osobowych, obowiązane są do zachowania ich w tajemnicy. Obowiązek ten istnieje również po ustaniu zatrudnienia".

stotliwości tworzenia kopii awaryjnych, przechowywania nośników i wydruków, kontroli antywirusowej, konserwacji systemu (§11),

– określenie obszarów (budynków, pomieszczeń, części pomieszczeń), w których są przetwarzane dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz określenie sposobu ich zabezpieczeń i zasad dostępu (§7).

Rozporządzenie MSWiA [1998] nakłada na administratora danych osobowych obowiązek wyznaczenia osoby, tzw. administratora bezpieczeństwa informacji (ABI), „odpowiedzialnej za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń". To właśnie osoba pełniąca funkcję administratora bezpieczeństwa informacji, posiadając odpowiednie pełnomocnictwa ze strony administratora danych osobowych, kieruje i odpowiada za realizację polityki bezpieczeństwa systemu informatycznego służącego przetwarzaniu danych osobowych[25]. Przedstawione w rozporządzeniu MSWiA [1998] i ustawie [ODO 1997] wymagania i zalecenia, choć kierowane przede wszystkim w stronę administratora danych osobowych, w praktyce są realizowane przez administratora bezpieczeństwa. Podzielić je można na kilka grup (zob. np. [Grzywak 2000]):

– bezpieczeństwo związane z użytkownikami obsługującymi system informatyczny[26],

– bezpieczeństwo zasilania[27],

---

[25] Te dwa pojęcia: administrator danych osobowych (ADO) i administrator bezpieczeństwa informacji (ABI) są ze sobą mylone (por. np. [*Sprawozdanie…*, 1999]). Relacja pomiędzy nimi jest następująca: administratorem danych osobowych jest przedsiębiorstwo, a administratorem bezpieczeństwa informacji pracownik odpowiedzialny za bezpieczeństwo danych osobowych w przedsiębiorstwie.

[26] Zgodnie z rozporządzeniem MSWiA [1998]:

– uwierzytelnianie użytkowników i kontrola dostępu są obowiązkowe (§14 ust. 1); bezpośredni dostęp do danych osobowych przetwarzanych w SI może mieć miejsce wyłącznie po podaniu identyfikatora i hasła (§14 ust. 5),

– każdy użytkownik ma odrębny identyfikator i hasło (§14 ust. 3); hasło użytkownika musi być zmieniane co najmniej raz w miesiącu (§14 ust. 6), a po jego wygaśnięciu nadal trzymane w tajemnicy (§14 ust. 8),

– identyfikator użytkownika nie powinien być zmieniany ani przydzielany innej osobie (§14 ust. 7); identyfikator użytkownika, który utracił prawo dostępu do danych należy niezwłocznie wyrejestrować z systemu, a hasło unieważnić (§14 ust. 9),

– zaleca się stosowanie wygaszaczy ekranu po pewnym okresie bezczynności użytkownika (§15).

[27] Zgodnie z rozporządzeniem MSWiA [1998] urządzenia i systemy informatyczne powinny być zabezpieczone przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (§8).

Tabela 3. Zagrożenie karą za nieprzestrzeganie przepisów ustawy o ochronie danych osobowych

Czyn podlegający karze	Podstawa prawna	Zagrożenie karą
Przetwarzanie niedozwolonych danych osobowych lub przetwarzanie ich bez uprawnienia	art. 49 ust. 1	grzywna, ograniczenie lub pozbawienie wolności do lat 2
– gdy dane dotyczą m.in. pochodzenia rasowego, poglądów politycznych, przekonań religijnych, nałogów.	art. 49 ust. 2	grzywna, ograniczenie lub pozbawienie wolności od 3
Przechowywanie danych osobowych niezgodnie z celem utworzenia zbioru	art. 50	grzywna, ograniczenie lub pozbawienie wolności do roku
Celowe udostępnianie danych osobowych osobom nieupoważnionym	art. 51 ust. 1	grzywna, ograniczenie lub pozbawienie wolności do lat 2
Nieświadome udostępnianie danych osobowych osobom nieupoważnionym	art. 51 ust. 2	grzywna, ograniczenie lub pozbawienie wolności do roku
Naruszenie obowiązku zabezpieczenia danych osobowych przed zabraniem, uszkodzeniem lub zniszczeniem	art. 52	grzywna, ograniczenie lub pozbawienie wolności do roku
Niezgłoszenie zbioru do rejestracji	art. 53	grzywna, ograniczenie lub pozbawienie wolności do roku
Niepoinformowanie osoby, której dane dotyczą, o jej prawach	art. 54	grzywna, ograniczenie lub pozbawienie wolności do roku

Źródło: opracowanie własne na podstawie [k.k. 1997].

– bezpieczeństwo nośników informacji zawierających dane osobowe[28],
– bezpieczeństwo komputerów przenośnych[29],

[28] Zgodnie z rozporządzeniem MSWiA [1998]:

– urządzenia, dyski i inne nośniki przeznaczone do likwidacji, naprawy lub przekazania innemu, nieuprawnionemu podmiotowi, muszą zostać na trwałe pozbawione tych danych (§10 ust. 1–3); wydruki przeznaczone do usunięcia muszą być zniszczone w stopniu uniemożliwiającym odczytanie danych (§10 ust. 4),

– kopie awaryjne nie powinny być przechowywane w tych samych pomieszczeniach co nośniki eksploatowane na bieżąco (§12 ust. 1), powinny być one okresowo sprawdzane i usuwane po ustaniu ich użyteczności (§12 ust. 2),

– nośniki informacji oraz wydruki nie przeznaczone do udostępnienia, należy przechowywać w warunkach uniemożliwiających dostęp do nich osobom niepowołanym (§13).

[29] Zgodnie z rozporządzeniem MSWiA [1998]: należy zachować szczególną ostrożność podczas transportu i przechowywania komputerów przenośnych poza obszarem przeznaczonym do przetwarzania danych; należy dostęp do nich zabezpieczyć hasłem; nie wolno zezwalać na ich używanie osobom nieupoważnionym (§9).

– rejestrowanie historii zmian danych każdej osoby, której dane są przetwarzane w systemie[30].

Bezpośredni nadzór nad realizacją przedstawionych wyżej wymagań należy do zadań administratora bezpieczeństwa informacji. Ponadto Biuro GIODO obliguje administratora bezpieczeństwa informacji (zob. [*Zadania administratora*…, 2002]) do śledzenia nowych rozwiązań w dziedzinie zabezpieczania systemów informatycznych i wdrażania narzędzi, metod pracy oraz sposobów zarządzania SI wzmacniających bezpieczeństwo systemu.

Z ustawy o ochronie danych osobowych [1997], rozporządzenia MSWiA [1998] i zaleceń Biura Generalnego Inspektora [*Zadania administratora*…, 2002] wynika, że przedsiębiorstwa, które przetwarzają, przesyłają i przechowują dane osobowe w swoim systemie informatycznym, mają obowiązek zarządzania bezpieczeństwem SI w zakresie ochrony danych osobowych. Za niedopełnienie tego obowiązku grozi kara grzywny, ograniczenie lub pozbawienie wolności (zob. tabela 3).

5. Podsumowanie

Podsumowując omówione akty prawne w zakresie bezpieczeństwa systemów informatycznych przedsiębiorstw, należy wymienić:

– Kodeks karny [k.k. 1997] obejmuje bezpośrednią ochroną prawną informacje w postaci „tradycyjnej" i elektronicznej oraz przewiduje odpowiedzialność karną za popełnienie przestępstw komputerowych. Chroni on informację w sytuacji, kiedy zostanie ona ujawniona lub wykorzystana wbrew zobowiązaniu oraz kiedy zostanie ona uzyskana w drodze przełamania zabezpieczeń. Wynika z tego, że jeżeli przedsiębiorstwu zależy na zachowaniu poufności informacji, to należy wymagać tego od pracowników oraz odpowiednio ją zabezpieczyć. Zabezpieczenia te powinny stanowić rzeczywistą przeszkodę, tak aby nie było możliwe ich obejście. W praktyce oznacza to, że należy na bieżąco aktualizować i rozwijać system ochrony;

– ustawa o rachunkowości [1994] uznaje dowody (dokumenty) księgowe również w postaci elektronicznej, ale pod warunkiem, że są one odpowiednio chronione. W powiązaniu z dalszymi jej przepisami oznacza to, że posiadanie systemu ochrony danych rachunkowych jest ustawowym obowiązkiem każdego przedsiębiorstwa. Ponadto ustawa nakłada obowiązek posiadania kompletnej dokumen-

[30] W szczególności muszą być rejestrowane: daty wprowadzenia, źródła danych i identyfikatora użytkownika, który wprowadził dane (§16 pkt 1–3); informacje o udostępnianiu danych osobowych (§16 pkt 4); informacje o wniesionych sprzeciwach lub żądaniach zaprzestania przetwarzania (§16 pkt 5).

tacji systemu, w tym szczegółowego opisu systemu informatycznego oraz opisu systemu ochrony. Osobą odpowiedzialną za te działania jest kierownik jednostki;

– ustawa o ochronie danych osobowych [ustawa ODO 1997] wraz z rozporządzeniem MSWiA [1998] nakłada na przedsiębiorstwo wymóg zapewnienia kompleksowej ochrony systemu informatycznego i zbiorów z danymi osobowymi. Osiągnięcie bezpieczeństwa realizowane powinno być poprzez wiele działań, takich jak np.: określenie celów, strategii i polityki bezpieczeństwa SI, monitorowanie skuteczności zabezpieczeń, przeprowadzenie szkoleń. Oznacza to, że przedsiębiorstwa posiadające dane osobowe w swoim systemie informatycznym mają obowiązek zarządzania bezpieczeństwem SI w zakresie ochrony tych danych.

Na zakończenie można stwierdzić, że analiza omówionych aktów prawnych pozwala na wyciągnięcie jednego wniosku – aktualne przepisy prawa bezwzględnie wymagają od przedsiębiorstw zapewnienia kompleksowej ochrony systemom informatycznym (zarządzania bezpieczeństwem SI), a odpowiedzialność za prawidłową realizację tego zadania ponosi ich kierownictwo.

Literatura

Adamski A. [2001], *Computer Crime in Poland: Three Years' Experience in Enforcing the Law*, referat na konferencji towarzyszącej podpisaniu konwencji Rady Europy w sprawie cyberprzestępczości, 22 listopad 2001, Budapeszt.

Adamski A. [1998a], *Hacking a nowy kodeks karny*, „Informatyka" nr 9.

Adamski A. [1998b], *Prawo do bezpiecznej sieci* [w:] *Bezpieczeństwo Sieci*, Computer-World Raport, Wydawnictwo IDG Poland SA, Warszawa.

Bezpieczeństwo systemów komputerowych [2000], red. A. Grzywak, Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2000.

CERT Polska [CERT PL www], serwis internetowy, http://www.cert.pl/ (25.01.2005).

Dziedziczak I. [1998], *Atrybuty wiarygodności systemów informatycznych wspierających prowadzenie ksiąg rachunkowych*, „Informatyka", nr 1.

Fischer B. [1997a], *Hackpospolita Polska. Przestępczość komputerowa* (2), „Prawo i Życie" nr 23.

Fischer B. [1997b], *Przestępczość komputerowa*, „Prawo i Życie" nr 22.

Fischer B. [1997c], *Przestępczość komputerowa* (3), „Prawo i Życie" nr 24.

Fischer B. [2000], *Przestępstwa komputerowe i ochrona informacji*, Kantor Wydawniczy Zakamycze, Kraków 2000.

Generalny Inspektor Ochrony Danych Osobowych, GIODO www, serwis internetowy, http://www.giodo.gov.pl/ (25.01.2005).

Jakubski K.J. [1999], *Przestępczość komputerowa – próba zdefiniowania zjawiska* [w:] *Internet – problemy prawne* [1999], red. R. Skubisz, Wydawnictwo Polihymnia, Lublin.

Karoński M., Kutyłowski M. [2001], *Krytyczna opinia na temat projektów ustawy o podpisie elektronicznym skierowana do Przewodniczącego Komisji Łączności Sejmu Rzeczypospolitej Polskiej*, Poznań 2001.

Komenda Główna Policji, KGP www, serwis internetowy, http://www.policja.pl/ (07.06.2005).

Organizacja rachunkowości [2000], red. M. Dobija, Wydawnictwo AE w Krakowie, Kraków.

Przypadki naruszające bezpieczeństwo teleinformatyczne [2000], CERT PL Raport, CERT PL www.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, [rozporządzenie MSWiA 1998], Dz.U. z 1998 r., nr 80, poz. 521, z późn. zm.

Siłuszek A. [2000], *Przestępstwa komputerowe*, „PCKurier 8", Wydawnictwo Lupus, Warszawa.

Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych za okres 01.01.1999 r. – 31.12.1999 r. [1999], GIODO, GIODO www.

Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych za okres 01.01.2001 r. – 31.12.2001 r. [2001], GIODO, GIODO www.

Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych za okres 01.01.2002 r. – 31.12.2002 r. [2002], GIODO, GIODO www.

Ustawa z 29 września 1994 r. o rachunkowości [ustawa o rachunkowości 1994], Dz.U. z 1994 r., nr 121, poz. 591, z późn. zm.

Ustawa z 6 czerwca 1997 r. Kodeks karny, [k.k. 1997], Dz.U. z 1997 r., nr 88, poz. 553.

Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych [ustawa ODO 1997], Dz.U. z 1997 r., nr 133, poz. 883, z późn. zm.

Ustawa z 22 stycznia 1999 r. o ochronie informacji niejawnych [ustawa OIN 1999], Dz.U. z 1999 r., nr 11, poz. 95, z późn. zm.

Ustawa z 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych [ustawa PAiPP 1994], Dz.U. z 1994 r., nr 24, poz. 83, z późn. zm.

Ustawa z 18 września 2001 r. o podpisie elektronicznym [ustawa PE 2001], Dz.U. z 2001 r., nr 130, poz. 1450, z późn. zm.

Ustawa z 13 października 1998 r. o systemie ubezpieczeń społecznych [ustawa SUS 1998], Dz.U. z 1998 r., nr 137, poz. 887, z późn. zm.

Ustawa z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji [ustawa ZNK 1993], Dz.U. z 1993 r., nr 47, poz. 211, z późn. zm.

Wójcik J.W. [1998], *Przestępstwa komputerowe w nowym kodeksie karnym*, „Przegląd Organizacji", nr 11.

Wójcik J.W. [1999], *Przestępstwa komputerowe*, cz. I.: *Fenomen cywilizacyjny*, Centrum Informatyki Menedżerskiej, Warszawa 1999.

Zadania administratora bezpieczeństwa informacji [2002], Biuro Generalnego Inspektora Ochrony Danych Osobowych – Departament Informatyki, materiały, (GIODO, GIODO www.

Legal Requirements for Computer Systems Security in Polish Enterprises – Penal Code, Act of Accounting, Act of Personal Data Protection

The paper is devoted to computer system security requirements that are imposed on Polish enterprises by legal regulations. The most important legal acts that are related to computer system security issues in Poland have been presented. The legal requirements derived from regulations have been characterised and analysed. Consequently, a general conclusions concerning the responsibility of ensuring a complex protection for computer systems in Polish enterprises have been formulated.

Key words: computer systems security, information protection, penal code, act of accounting, act of personal data protection.