3. POMIAR I OCENA POZIOMU BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH

- W praktyce, poziom bezpieczeństwa wyrażany jest na **skali porządkowej**,
- trwają prace pozwalające wyrazić go na **skali interwałowej** lub **ilorazowej**.

Zalety pomiaru poziomu bezpieczeństwa na skali interwałowej (ilorazowej):

- dokładne porównywanie poziomu bezpieczeństwa różnych systemów,
- określenie skuteczności zabezpieczeń (np. możliwość zbadania zmian poziomu bezpieczeństwa wywołanych wprowadzeniem zabezpieczeń),
- dokładne obliczenie kosztów, jakie należy ponieść, aby zwiększyć poziom bezpieczeństwa systemu o określoną wartość,
- dokładne monitorowanie poziomu bezpieczeństwa.

3.1. Metoda „najsłabszego ogniwa”

Podstawą jest założenie, że *system jest tak mocny, jak jego najsłabszy element*.
Metoda polega na zmierzeniu lub oszacowanie poziomu bezpieczeństwa (B_i) elementów systemu i przyjęciu najmniejszej wartości za poziom bezpieczeństwa całego systemu (PB):

$$PB = min\{B_1, B_2, ..., B_n\}$$

Wada: system nie składa się z jednorodnych zasobów pod względem wartości, podatności i zagrożeń.

3.2. Pomiar poziomu bezpieczeństwa z użyciem „ocen bezpieczeństwa”

Metoda polega na:

- wyodrębnieniu zestawu cech (F_i), które odpowiadają za bezpieczeństwo systemu (cechy powinny tworzyć zbiór rozłączny),
- przypisanie cesze F_i wagi w_i, która oznacza wpływ cechy na poziom bezpieczeństwa.
- ustalenie poziomu bezpieczeństwa (B_i) danej cechy (musi on spełniać warunek: $0 \le B_i \le 1$. Jeżeli cecha F_i nie występuje w systemie, to jej $B_i = 0$).

Tabela 1. Cechy systemu informatycznego wpływające na jego bezpieczeństwo

Cecha [F_i]	Nazwa cechy	Waga [w_i]	Poziom bezpieczeństwa [B_i]
F_1	Stosowanie programów antywirusowych	8	0,8
F_2	Tworzenie kopii danych	10	0,5
F_3	Używanie niszczarek do dokumentów	3	0
...	...	...	...
F_n	Procedury postępowania podczas awarii	4	0,1

Źródło: opracowanie własne

Ocena poziomu bezpieczeństwa systemu (PB) wyrażona jest wzorem:

$$PB = \frac{1}{W}\sum_{i=1}^{n} w_i B_i, \; gdzie \; W = \sum_{i=1}^{n} w_i$$

Przy takich założeniach:

- poziom bezpieczeństwa systemu całkowicie zabezpieczonego wynosi *1*,
- poziom bezpieczeństwa systemu całkowicie niezabezpieczonego wynosi *0*.

Wady metody:

- brak standardowej listy cech (F_i) i ich wag (w_i)
- brak obiektywnych metod wyznaczania poziomu bezpieczeństwa cech (B_i).

3.3. Pomiar poziomu bezpieczeństwa przy użyciu list kontrolnych (ang. checklists)

Założenia metody:

- lista kontrolna to zbiór pytań, na które użytkownik odpowiada w sposób binarny (np. tak/nie, jest/nie ma),
- pytania zawarte w liście muszą być szczegółowe i jednoznaczne,
- waga poszczególnych pytań powinna być zbliżona (jeżeli tak nie jest, to należy przypisać im różną ilość punktów),
- pytania - na ogół - podzielone są na określone kategorie (np. dotyczące tego samego fragmentu systemu),
- po przeprowadzeniu badania uzyskane punkty należy zsumować zgodnie z przyjętymi zasadami i porównać wynik ze wzorcem (często wynik przestawiany jest graficznie).

Użyteczność listy kontrolnej zależy od spełniania przez nią warunków:

- lista nie może pomijać żadnego istotnego elementu - zestaw pytań musi obejmować całość badanego obszaru (systemu lub jego fragmentu),
- w przypadku elementów o różnym poziomie istotności należy przypisać pytaniom odpowiednie wagi (różną liczbę punktów, zadać różną liczbę pytań),
- należy ustalić wzorce (np. klasy bezpieczeństwa systemu) i odpowiadające im progi punktowe,
- odpowiedzi muszą być udzielone zgodnie ze stanem faktycznym.

Listy kontrolne pozwalają uzyskać pomiar tylko o charakterze **orientacyjnym** i wykorzystywane są zazwyczaj jako element pomocniczy przy przeprowadzaniu audytu lub analizy ryzyka.

Zaleta:

- listy kontrolne zwracają uwagę na problemy i zjawiska, które mają znaczenie dla bezpieczeństwa SI,
- uzyskanie odpowiedzi negatywnej może być punktem wyjścia do podjęcia dalszych działań.

3.4. Klasy bezpieczeństwa systemów informatycznych

Trudności z pomiarem bezpieczeństwa SI doprowadziły do opracowania standardów wyznaczających *kryteria bezpieczeństwa*, których spełnienie przez system pozwala przypisać go do określonej *klasy bezpieczeństwa*.

Kryteria (wymagania) dotyczą na ogół istnienia określonych zabezpieczeń oraz pewności ich działania. Ocenie podlegają także wybrane elementy systemu informatycznego (np. system operacyjny, sieć komputerowa).

Standardy określające kryteria bezpieczeństwa

- *Trusted Computer Systems Evaluation Criteria (TCSEC)* - dokument opracowany w 1985 roku przez Departament Obrony USA.
- *Trusted Network Interpretation of the TCSEC* (w 1987 roku) i *Trusted Database Interpretation of the TCSEC* (w 1991 roku) - dokumenty opracowane przez National Computer Security Center - jest to rozszerzenie standardu TCSEC na systemy sieciowe i bazy danych.

- *Information Technology Security Evaluation Criteria* (*ITSEC*). *Harmonised Criteria of France - Germany - the Netherlands - the United Kingdom* - dokument opracowany w roku 1991 przez grupę państw europejskich.
- *Canadian Trusted Computer Product Evaluation Criteria* (*CTCPEC*) *version 3.0* - document opracowany w Kanadzie w roku 1993 jako kombinacja standardów ITSEC i TCSEC.
- *Common Criteria for Information Technology Security Evaluation* (*CCITSE*) - dokument opracowany przez *Common Criteria Implementation Board* i ISO w 1999 roku.

3.4.1. TCSEC

Standard TCSEC zawiera opis kryteriów, wg których można przypisać system do odpowiedniej klasy bezpieczeństwa. Zakłada on istnienie czterech kategorii klas bezpieczeństwa (A, B, C, D), w obrębie których jest siedem klas: A1, B3, B2, B1, C2, C1, D1.

Kategoria D - klasa D1.

Klasa D1: należą do niej systemy z najniższym poziomem bezpieczeństwa. W praktyce oznacza to brak zabezpieczeń zasobów i identyfikacji użytkowników (np. system operacyjny MS Windows 9x).

Kategoria C - klasy C1 i C2.

Klasa C1:

- użytkownicy i zasoby muszą posiadać unikalne identyfikatory,
- dostęp do systemu i zasobów jest kontrolowany poprzez nadawanie praw dostępu.
- użytkownicy muszą się uwierzytelniać i posiadać określone prawa.

Klasa C2:

- wymagania klasy C1,
- mechanizmy umożliwiające audyt i śledzenie operacji użytkowników i wykorzystywania zasobów.

Kategoria B - klasy: B1, B2, B3.

Klasa B1:

- wymagania klasy C2,
- obowiązek przypisania etykiet do wszystkich zasobów i obiektów systemu (etykiety świadczą o ich ważności oraz stanowią podstawę kontrolowania i przydzielania dostępu przez system).

Klasa B2:

- wymagania klasy B1,
- istnienie zdefiniowanego i udokumentowanego modelu bezpieczeństwa,
- istnienie rozbudowanych mechanizmów uwierzytelniania i kontrolowania użytkowników.

Klasa B3:

- wymagania klasy B2,
- rejestrowanie wszystkich operacji użytkowników, tworzenie tzw. list bezpieczeństwa, po awarii uruchamianie się systemu z takim samym poziomem bezpieczeństwa.

Kategoria A

Klasa A1: systemy tej klasy nie różnią się funkcjonalnie od systemów klasy B3. Różnica polega na konieczności weryfikowania istniejących mechanizmów zabezpieczeń i kontroli, aby sprawdzić ich zgodność z obowiązującym modelem bezpieczeństwa.

3.5. Główne przyczyny trudności pomiaru i oceny poziomu bezpieczeństwa SI:

- złożony charakter zagadnienia bezpieczeństwa zasobów SI,
- zmienność poziomu bezpieczeństwa w czasie.

Ad 1. Złożony charakter zagadnienia

Jeżeli dany zasób (A) narażony jest na zagrożenie (t), to poziom jego bezpieczeństwa (PB_A) zależy od jego podatności (v) na zagrożenie (t) oraz od wystąpienia tego zagrożenia.

W szczególnych przypadkach:

- jeżeli zagrożenie (t) nie występuje ($t = 0$), to $PB_A = 1$,
- jeżeli zasób (A) na zagrożenie (t) nie jest podatny ($v = 0$), to $PB_A = 1$.

Jednak w praktyce zasób (A) narażony jest na wiele zagrożeń $\{t_1, t_2, ..., t_m\}$, na które jego podatność $\{v_1, v_2, ..., v_m\}$ jest różna.

$\{v_1, v_2, ..., v_m\}$ - to zbiór podatności, gdzie v_i to podatność na zagrożenie t_i

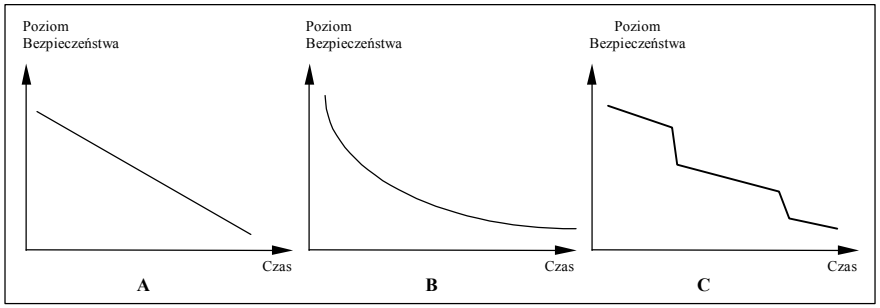
Pomiar podatności jest trudny, dlatego często proponuje się zastąpienie go pomiarem *ryzyka*, które łączy w sobie dwa elementy - podatność zasobu i występujące zagrożenia (ryzyko to prawdopodobieństwo, że zagrożenie wykorzysta podatność zasobu, aby spowodować jego straty lub zniszczenie).

Ad 2. Zmienność poziomu bezpieczeństwa w czasie

Podczas pomiaru i oceny poziomu bezpieczeństwa SI należy uwzględnić także *czynnik czasu*.

Zależność pomiędzy czasem a poziomem bezpieczeństwa:

Jeżeli w systemie informatycznym nie są dokonywane żadne zmiany mające na celu utrzymanie poziomu bezpieczeństwa, to *poziom bezpieczeństwa maleje wraz z upływem czasu*.



Rys. 4. Przykładowe zmiany poziomu bezpieczeństwa w czasie
Źródło: opracowanie własne

W praktyce najczęściej zmniejszający się poziomu bezpieczeństwa jest dodatkowo pogłębiany nagłymi spadkami (C) - jest to skutek np. wykryciem błędów i luk w systemie ochrony lub wprowadzeniem nowej technologii pozwalającej na pokonanie zabezpieczeń.

Pozostałe przyczyny trudności pomiaru i oceny poziomu bezpieczeństwa SI:

- złożony i niejednorodny charakter systemów informatycznych,
- brak standardowych rozwiązań w zakresie budowy i ochrony SI,
- duża dynamika rozwoju i zmienność SI,
- brak metod pozwalających na wyznaczenie ryzyka, podatności i zagrożeń zasobów,
- duża liczba zagrożeń przypadająca na poszczególne zasoby,

- pośredni charakter wielu zagrożeń (wykorzystywanie przez zagrożenia podatności *innych* zasobów),
- brak danych empirycznych (na temat występowania zagrożeń, podatności i ryzyka),
- nieprzewidywalny charakter błędów i luk w programach, systemach operacyjnych, zabezpieczeniach, itd.,
- trudności z wyznaczeniem wartości zasobu i wpływu jego uszkodzenia lub zniszczenia na poziom bezpieczeństwa systemu.

4. PRAWNE WYMOGI W ZAKRESIE BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH

Do podstawowych aktów prawnych, które mają wpływ na bezpieczeństwo i ochronę danych w systemach informatycznych polskich przedsiębiorstw należą:

- ustawa *Kodeks karny* [k.k.],
- ustawa *o rachunkowości*,
- ustawa *o ochronie danych osobowych* [ustawa ODO],
- ustawa *o prawie autorskim i prawach pokrewnych* [ustawa PAiPP],
- ustawa *o zwalczaniu nieuczciwej konkurencji* [ustawa ZNK].

4.1. Kodeks karny - ustawa z dnia 6 czerwca 1997 roku (Dz.U. z 1997 r. Nr 88, poz. 553)

- Bezpośrednia ochrona informacji oraz odpowiedzialność karna za popełnienie tzw. *przestępstw komputerowych* (rozdział XXXIII pt. „Przestępstwa przeciwko ochronie informacji")

4.1.1. Ujawnienie informacji wbrew zobowiązaniu

Art. 266 §1 - *kto wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu ujawnia lub wykorzystuje informację, z którą zapoznał 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.*

Wniosek: jeżeli konieczne jest zachowanie poufności informacji, które nie są chronione ustawowo, to **należy wymagać od użytkowników (pracowników) zobowiązania, że nie będą ich ujawniać lub wykorzystywać**.

4.1.2. Niszczenie i fałszerstwo dokumentów

Definicja *dokumentu*

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*.

Kodeks przewiduje wysokie kary za ich:

- fałszowanie (art. 270 §1):

  §1. Kto, w celu użycia za autentyczny, podrabia lub przerabia dokument lub takiego dokumentu jako autentyczny używa, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności od 3 miesięcy do lat 5.

- niszczenie, ukrywanie i usuwanie (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.

4.1.3. Nieuprawnione uzyskanie i podsłuch informacji

Karalne jest (rozdział XXXIII „Przestępstwa przeciwko ochronie informacji"):

- nieuprawnione pozyskiwanie informacji (art. 267 §1):

  §1. Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, 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.

- podsłuch informacji (art. 267 §2):

  §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.

- ujawnianie nielegalnie zdobytych informacji (art. 267 §3):

  §3. Tej samej karze podlega, kto informację uzyskaną w sposób określony w §1 lub 2 ujawnia innej osobie.

Wniosek: ponieważ ochrona prawna uzależniona jest od *przełamania* przez sprawcę zabezpieczeń, to **aby móc korzystać z prawnej ochrony poufności, informacje muszą zostać najpierw odpowiednio zabezpieczone**.

Uwaga:

- wymóg zabezpieczenia nie dotyczy sytuacji, kiedy osoba nieuprawniona wykorzystuje podsłuch (karalne są już same przygotowania do przestępstwa)
- art. 267 §1 uznawany jest za główną ochronę prawną przed nieuprawnionym wejściem do SI (tzw. *hackingiem*).

4.1.4. Sabotaż komputerowy

Art. 269 §1 - karze pozbawienia wolności od 6 miesięcy do lat 8 podlega osoba, która *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.*

Art. 269 §2 - takiej samej karze podlega osoba, która *niszczy albo wymienia nośnik informacji lub niszczy albo uszkadza urządzenie służące automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji* określonej w §1.

- przepis ten chroni także systemy telekomunikacyjne, a w szczególności lokalne i rozległe sieci komputerowe.

Art. 287 §1 - karze pozbawienia wolności od 3 miesięcy do lat 5 podlega osoba, która *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.*

4.1.5. Niszczenie lub zmiana istotnej informacji

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.*
>
> *§2. Jeżeli czyn określony w §1 dotyczy zapisu na komputerowym nośniku informacji, sprawca podlega karze pozbawienia wolności do lat 3.*

- kodeks przewiduje większą karę za zniszczenie informacji zapisanej elektronicznie, niż na papierze,

- bez względu na motywy (wandalizm, chęć wyrządzenia szkody, zatarcie śladów włamania, itp.) każdy z tych czynów podlega karze pod warunkiem, że informacja jest *istotna*,
- w kodeksie nie ma definicji istotnej informacji - rozstrzygnięcie tej kwestii pozostawione zostało sądom,
- jeżeli sprawca kieruje się chęcią odniesienia korzyści majątkowej lub wyrządzenia innej osobie szkody, podlega karze pozbawienia wolności od 3 miesięcy do lat 5 (art. 287 §1),
- jeżeli szkoda lub osiągnięte korzyści majątkowe były znacznej wartości, to podlega karze pozbawienia wolności od roku do lat 10 (art. 294 §1).

4.1.6. Nielegalne uzyskanie i paserstwo programów komputerowych

Art. 278 §1 - *kto zabiera w celu przywłaszczenia cudzą rzecz ruchomą podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*

Art. 278 §2 - *tej samej karze podlega, kto bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy w celu osiągnięcia korzyści majątkowych*.

Art. 293 §1 - *zastosowanie do programu komputerowego mają przepisy artykułów 291 i 292.*

Na podstawie tych artykułów:

- polega karze pozbawienia wolności od 3 miesięcy do lat 5 kto nabywa, pomaga w zbyciu albo przyjmuje rzecz *uzyskaną za pomocą czynu zabronionego* (art. 291 §1),

- podlega karze grzywny, karze ograniczenia albo pozbawienia wolności do lat 2, kto 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).

4.1.7. Oszustwo komputerowe

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.

Uwaga:

- przepis ten kładzie nacisk na motywy sprawcy (osiągnięcie korzyści majątkowych, osiągnięcie szkody), a nie na sposób popełnienia czynu, dlatego ma zastosowanie do różnych przestępstw komputerowych,
- kara jest większa (od roku do lat 10), jeżeli szkoda lub osiągnięte korzyści majątkowe są znacznej wartości (art. 294 §1).

4.1.8. Oszustwo telekomunikacyjne

Art. 285 §1:

§1. Kto, włączając się do urządzenia telekomunikacyjnego, uruchamia na cudzy rachunek impulsy telefoniczne, podlega karze pozbawienia wolności do lat 3.

4.1.9. Zagrożenie zdrowia, życia lub mienia o znacznej wartości

Rozdział XX „Przestępstwa przeciwko bezpieczeństwu powszechnemu"

Art. 165 §1:

§1. 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.

Uwaga: dla karalności tego czynu nie są ważne motywy, ale za czyn nieumyślny grozi pozbawienie wolności do lat 3 (art. 165 §2).

4.1.10. Szpiegostwo przy użyciu komputera

Rozdział XVII kodeksu, pt. „Przestępstwa przeciwko Rzeczypospolitej Polskiej"

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.

4.1.11. Kodeks karny - podsumowanie

Poza treścią przepisów kodeksu istotna jest także skuteczność wymiaru sprawiedliwości w tym zakresie, tzn.:

- zgłaszanie organom ścigania (policji, prokuraturze) popełnionych przestępstw komputerowych,
- umiejętność oraz skuteczność policji i prokuratury w ściganiu tych przestępstw,
- orzekanie przez sądy karalności popełnianych czynów.

Zgłaszanie przestępstw

- kodeks postępowania karnego [k.p.k.] nie zawiera żadnych szczególnych unormowań w kwestiach zgłaszania organom ścigania popełnionych przestępstw komputerowych,
- obowiązuje ogólna zasada - każdy kto zetknie się z przypadkiem karygodnego naruszenia bezpieczeństwa informacji, może o tym zawiadomić policję lub prokuraturę,
- organy te mają obowiązek przyjąć zawiadomienie i po przeprowadzeniu czynności sprawdzających wszcząć postępowanie lub odrzucić wniosek,
- nieuprawnione pozyskiwanie i podsłuch informacji oraz jej niszczenie jest ścigane tylko na wniosek poszkodowanego (art. 267 §4, art. 268 §4),
- poza wnioskiem potrzebne jest jeszcze uzasadnione podejrzenie popełnienia przestępstwa, dlatego pokrzywdzony powinien przedstawić wszystkie okoliczności, które uzasadniają to podejrzenie.

Wykrywalność zgłaszanych przestępstw komputerowych

- wykrywalność tych przestępstw sięga ok. 70% [KGP www],
- brak jest danych o tym ile wniosków o wszczęcia postępowania odrzucono,
- brak jest danych o tym ile przestępstw komputerowych nie zostało w ogóle zgłoszonych do organów ścigania.

Tabela 2. Liczba wszczętych przez Policję postępowań w latach 1999-2014 (w nawiasach liczba przestępstw stwierdzonych)

Lata	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	Sabotaż komputerowy art. 269a
1999	217	43	182	59	10	bd
2000	323	82	249	66	7	bd
2001	279	75	259	60	9	bd
2002	368	94	294	89	6	bd
2003	168	99	362	114	2	bd
2004	390	125	378	105	12	bd
2005	568	131	430	152	2	1
2006	444	159	538	201	3	19
2007	492	133	616	244	6	11
2008	404	121	694	366	6	13
2009	bd	155	982	555	6	34
2010	bd	162	1194	690	7	22
2011	bd	131 (47)	1583 (948)	885 (629)	3 (5)	38(30)
2012	bd	159 (77)	1657 (1513)	796 (884 ?)	9 (5)	35 (30)
2013	bd	148 (50)	2203 (1655)	765 (589)	14 (9)	37 (34)
2014	bd	127 (33)	2868 (1901)	743 (572)	10 (6)	27 (48)

Źródło: opracowanie własne na podstawie [KGP www]

Dodatkowe trudności

- często umyślne naruszenie bezpieczeństwa informacji nie spełnia kryteriów karalności np. „obejście" zabezpieczeń (zasada *wszystko co nie jest zabronione, jest dozwolone*),
- trudno jest udowodnić sprawcy, że miał dostęp do informacji,
- nieustalona jest karalność np. włamań do systemu, których celem **nie jest** uzyskanie informacji, osiągnięcie korzyści materialnych, czy wyrządzenie szkód, ale np. wykazanie nieskuteczności zabezpieczeń.

4.2. Ustawa o rachunkowości - z dnia 29 września 1994 roku (Dz.U. z 1994 r. Nr 121, poz. 591)

Pierwotna treść ustawy poddana została późniejszym zmianom, a w 2001 roku nowelizacji. Od 1 stycznia 2002 roku obowiązuje jej znowelizowana postać, określana mianem *nowej ustawy o rachunkowości*.

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.*

Wniosek: **aby w świetle prawa uznać zapis (dokument) za dowód księgowy musi być zapewniona jego odpowiednia ochrona.**

4.2.1. Ochrona dowodów księgowych

Ustawodawca jednoznacznie nakłada na jednostkę **obowiązek posiadania systemu ochrony danych** (rozdział 8, pt. „Ochrona danych”):

Art. 71 ust. 1 - *zbiory* należy *przechowywać w należyty sposób i chronić przed niedozwolonymi zmianami, nieupoważnionym rozpowszechnianiem, uszkodzeniem lub zniszczeniem.*

Art. 71 ust. 2 - ochrona danych powinna polegać na:

- *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.*

Obowiązek posiadania kompletnej dokumentacji systemu

Art. 10 ust. 1 - jednostka musi posiadać m.in.:

- *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.*

Odpowiedzialność

- odpowiedzialny za ochronę oraz utworzenie i aktualizację dokumentacji odpowiedzialny jest kierownik jednostki (art. 10 ust. 2),

- nie wywiązywanie 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).

Wniosek: **przedsiębiorstwo musi posiadać dokument opisujący system informatyczny i system 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. W dużej mierze odpowiada on *dokumentowi polityki bezpieczeństwa*.

4.3. Ustawa o ochronie danych osobowych - z dnia 29 sierpnia 1997 roku (Dz.U. z 1997 r. Nr 133, poz. 883)

Generalny Inspektor Ochrony Danych Osobowych

- organ do spraw ochrony danych osobowych, powoływany i odwoływany przez Sejm RP za zgodą Senatu,
- informacje o funkcjonowaniu tego urzędu można znaleźć w jego corocznych sprawozdaniach, które zawierają także statystyki, podsumowania, uzasadnienia podjętych decyzji oraz odpowiedzi na pytania, które w danym okresie się pojawiły.

4.3.1. Zakres stosowania ustawy

Art. 3 ust. 1 - *ustawę stosuje się do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych oraz podmiotów niepaństwowych realizujących zadania publiczne*.

Art. 3 ust. 2 - *ustawę stosuje się również do osób fizycznych i prawnych oraz jednostek organizacyjnych nie mających osobowości prawnej, które przetwarzają dane w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych.*

Art. 3 ust. 4 - ustawy nie stosuje się do *osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych lub domowych*.

4.3.2. Zbiory danych osobowych i ich przetwarzanie

Art. 6 ust. 1 - *za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej*.

Art. 3 ust. 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*.

Art. 6 ust. 3 - *informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu i działań*.

Ustawodawca posłużył się klauzulą ogólną i nie określił zamkniętego zestawu danych osobowych. Wypracowanie wykładni tego pojęcia realizowane jest przez rozstrzygnięcia GIODO, wsparte orzecznictwem Naczelnego Sądu Administracyjnego.

Uwaga: nie wszystkie dane osobowe można przetwarzać.

Art. 27 ust. 1 - *zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych (...)*.

Przetwarzanie tych danych dopuszczalne jest tylko w pewnych, ściśle określonych warunkach (art. 27 ust. 2), np. gdy zezwala na to przepis innej ustawy, osoba wyrazi zgodę na piśmie, jest to niezbędne do dochodzenia praw przed sądem lub konieczne do prowadzenia badań naukowych.

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 muszą być zarejestrowane w biurze GIODO, który wydaje zgodę na ich przetwarzanie (art. 40),
- nie wszystkie zbiory danych muszą być zgłoszone do rejestracji - np. administratorzy danych *dotyczących osób u nich zatrudnionych, zrzeszonych lub uczących się* oraz *przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej* (art. 43 ust. 1),
- zwolnienie z obowiązku rejestracji nie oznacza, że można nie przestrzegać przepisów ustawy i stosownych rozporządzeń.

4.3.3. Administratora danych osobowych i jego obowiązki w zakresie bezpieczeństwa systemu informatycznego

Podmiotem odpowiedzialnym za ochronę danych osobowych jest **administrator danych osobowych** (ADO)

Wg ustawy ADO to *organ, instytucja, jednostka organizacyjna, podmiot lub osoba (...) decydująca o celach i środkach przetwarzania danych osobowych* (art. 7).

Uwaga: Administrator danych osobowych to nie funkcja, ale **status** związany z przetwarzaniem danych osobowych.
Tym samym nie jest prawnie skuteczne, aby np. zarząd przedsiębiorstwa zobowiązał swojego pracownika do pełnienia obowiązków ADO.

- administratorem danych osobowych jest np. każde przedsiębiorstwo, ponieważ w ramach systemu kadrowego przetwarza dane pracowników,
- ADO może powierzyć innemu podmiotowi, w drodze pisemnej umowy, przetwarzanie danych osobowych (art. 31 ust. 1),
- powierzenie przetwarzania tych danych **nie powoduje** zmiany statusu przedsiębiorstwa jako administratora danych i tym samym nie uwalnia go od odpowiedzialności za niezgodne z prawem przetwarzanie.

Obowiązki ADO w zakresie bezpieczeństwa SI - zgodnie z ustawą [ODO]
Ustawa (rozdz. 5, pt. „Zabezpieczenie zbiorów danych osobowych") nakłada na ADO szereg obowiązków, m.in.:

- obowiązek zapewnienia właściwej ochrony zbiorom danych osobowych - m.in. ich poufności, integralności i dostępności (art. 36):

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.

- obowiązek zapewnienia rozliczalności danych (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 (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 (...).

- obowiązek powołania osób upoważnionych do obsługi SI (art. 37):

  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. 1. Administrator danych prowadzi ewidencję osób zatrudnionych przy ich przetwarzaniu.

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.

Uwaga: Bardziej szczegółowe wytyczne dotyczące obowiązków ADO oraz warunków, jakim powinny odpowiadać urządzenia i SI służące przetwarzaniu danych osobowych zostały określone zgodnie z ustawą (art. 45) w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. *w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*.

Obowiązki ADO w zakresie bezpieczeństwa SI - zgodnie z rozporządzeniem MSWiA [1998]

Szczegółowość rozporządzenia jest bardzo duża. Jest to jedyny akt prawny, który tak dokładnie precyzuje wymagania w zakresie bezpieczeństwa SI.

Zgodnie z nim do głównych obowiązków ADO należy m.in.:

- 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, w tym kryptograficznej ochrony informacji, w szczególności podczas ich przesyłania za pośrednictwem urządzeń do transmisji danych (§2 pkt 3),
- określenie zabezpieczeń adekwatnych do zagrożeń i ryzyka (§2 pkt 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 (ABI)*, odpowiedzialnego **bezpośrednio** za bezpieczeństwo danych w SI (§3),
- określenie indywidualnej odpowiedzialności osób za utrzymanie bezpieczeństwa danych w zakresie czynności służbowych (§4) oraz zaznajomienie ich z przepisami dotyczącymi ich ochrony (§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 częstotliwości 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 sprzętu komputerowego oraz określenie sposobu ich zabezpieczeń i zasad dostępu (§7).

4.3.4. Administratora bezpieczeństwa informacji (ABI) i jego obowiązki w zakresie bezpieczeństwa SI

Zgodnie z rozporządzeniem MSWiA [1998] administrator danych osobowych ma 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.

Uwaga: Oznacza to, że właśnie osoba pełniąca funkcję ABI, posiadając odpowiednie pełnomocnictwa ze strony ADO, kieruje i odpowiada za realizację polityki bezpieczeństwa SI, w którym przetwarzane są dane osobowe.

Obowiązki (ABI) w zakresie bezpieczeństwa SI

Podane w rozporządzeniu MSWiA wymagania dotyczące bezpieczeństwa SI można podzielić na kilka grup:

1. Bezpieczeństwo związane z użytkownikami obsługującymi system:

- 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); identyfikator wraz z imieniem i nazwiskiem użytkownika jest zapisany w ewidencji, którą prowadzi administrator danych (art. 39 ustawy),
- 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), zaś 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).

2. Bezpieczeństwo zasilania:

- urządzenia i systemy informatyczne zasilane energią elektryczną powinny być zabezpieczone przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej (§8).

3. Bezpieczeństwo nośników informacji zawierających dane osobowe:

- 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 tych 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 również 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).

4. Bezpieczeństwo komputerów przenośnych:

- należy zachować szczególną ostrożność podczas transportu i przechowywania ich poza obszarem przeznaczonym do przetwarzania danych (§9),
- dostęp do komputera musi być zabezpieczony hasłem (§9),
- nie wolno zezwalać na używanie komputera osobom nieupoważnionym (§9).

5. Rejestrowanie historii zmian danych każdej osoby, której dane są przetwarzane w systemie, a w szczególności rejestrowanie:

- daty wprowadzenia, źródła danych i identyfikatora użytkownika, który wprowadził dane (§16 pkt 1-3),

- informacji o udostępnianiu danych osobowych (§16 pkt 4),
- informacji o wniesionych sprzeciwach lub żądaniach zaprzestania przetwarzania, zgodnie z ustawą - art. 32 ust. 1 pkt 7 i 8 (§16 pkt 5).

Uwaga:

- bezpośredni nadzór nad realizacją przedstawionych wymagań należy do zadań ABI,
- Biuro GIODO, obliguje ABI do śledzenia nowych rozwiązań w dziedzinie zabezpieczania SI i wdrażania narzędzi, metod pracy oraz sposobów zarządzania systemem wzmacniających jego bezpieczeństwo,
- Biuro GIODO zaleca, aby działania ABI były dostosowane do architektury systemu informatycznego, stosowanych narzędzi oraz do sytuacji organizacyjnej i finansowej ADO.

Uwaga:

w praktyce obowiązek wprowadzenia w przedsiębiorstwach funkcji ABI wywołuje szereg pytań i wątpliwości dotyczących m.in.:

- charakteru stanowiska ABI,
- umiejscowienia ABI w strukturze organizacyjnej,
- współpracy i podziału kompetencji ABI z innymi służbami (np. specjalistą ds. bezpieczeństwa SI, głównym informatykiem, administratorem systemu, działem kontroli wewnętrznej),
- wymaganych od ABI umiejętności i wykształcenia.

Wniosek: Z ustawy o ochronie danych osobowych, rozporządzenia MSWiA [1998] i zaleceń Biura Generalnego Inspektora Danych Osobowych wynika, że przedsiębiorstwa, które przetwarzają, przesyłają i przechowują dane osobowe

w swoim systemie informatycznym, **mają obowiązek zarządzania bezpieczeństwem SI w zakresie ochrony danych osobowych.**

4.4. Ustawa o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 roku (Dz.U. z 1994 r. Nr 24, poz. 83)

Z punktu widzenia bezpieczeństwa SI najważniejsze jest, że zgodnie z ustawą [PAiPP] program komputerowy jest przedmiotem prawa autorskiego, tak samo jak utwory artystyczne, literackie i fonograficzne, a więc jako utwór podlega ochronie prawnej (art. 1 ust. 2 pkt 1).

Ochrona obejmuje **każdą formę** programu (dokumentację projektową, kod źródłowy, postać wykonywalną) i karalne jest m.in.:

- przywłaszczenie autorstwa (plagiat) lub wprowadzenie w błąd co do autorstwa całości lub części programu komputerowego (art. 115 ust. 1).
- rozpowszechnianie bez podania nazwiska lub pseudonimu autora cudzego programu komputerowego (art. 115 ust. 2),
- inne naruszenie cudzego prawa autorskiego w celu uzyskania korzyści majątkowej (art. 115 ust. 3).,
- rozpowszechnianie bez upoważnienia albo wbrew jego warunkom cudzego programu (art. 116 ust. 1-4),
- utrwalanie albo zwielokrotnianie (powielanie) bez uprawnień lub wbrew jego warunkom cudzego programu w celu rozpowszechnienia (art. 117 ust. 1-2),
- nabywanie, pomaganie w zbyciu, przyjmowanie lub ukrywanie w celu osiągnięcia korzyści majątkowych programów komputerowych zwielokrotnionych bez uprawnień (wbrew ich warunkom) (art. 118 ust. 1-3).

Wniosek:

- art. 116-118 dają podstawy do ścigania uczestników procederu zwanego „piractwem komputerowym”,
- uczynienie z tego procederu stałego źródła dochodu albo organizowanie lub kierowanie grupą przestępczą grozi najwyższą sankcją w ustawie (do lat 5),
- w przypadku skazania sprawcy, sąd orzeka przepadek przedmiotów pochodzących z przestępstwa oraz może orzec przepadek przedmiotów służących do popełnienia przestępstwa, nawet jeśli nie są własnością sprawcy (art. 121 ust. 1-2).

Wniosek:

Wykorzystywanie w przedsiębiorstwie, dla realizacji jego celów, powielonych bez uprawnień programów komputerowych jest przestępstwem.

Oznacza to, że:

- nie wolno nie tylko posługiwać się „pirackimi” kopiami programów,
- używać oprogramowania legalnie zakupionego wbrew warunkom licencji (np. instalować na większej liczbie stanowisk).

Ponadto, korzystanie z nielegalnego oprogramowania, stanowi też inne zagrożenie - w przypadku kontroli - wykrycie takiego oprogramowania oznacza jego zarekwirowanie, a tym samym ewentualne problemy z funkcjonowaniem SI.

4.5. Ustawa o zwalczaniu nieuczciwej konkurencji z dnia 16 kwietnia 1993 roku (Dz.U. z 1993 r. Nr 47, poz. 211)

Ustawa *reguluje zapobieganie i zwalczanie nieuczciwej konkurencji w działalności gospodarczej, a w szczególności produkcji przemysłowej i rolnej, budownictwie, handlu i usługach - w interesie publicznym, przedsiębiorców oraz klientów, a zwłaszcza konsumentów.*

Definicja: **Czyn nieuczciwej konkurencji** to działanie:

- sprzeczne z prawem lub dobrymi obyczajami, jeżeli zagraża lub narusza interes innego przedsiębiorcy lub klienta, a także:
- przekazanie lub wykorzystanie cudzych informacji stanowiących *tajemnicę przedsiębiorstwa* albo ich nabycie od osoby nieuprawnionej, jeżeli zagraża istotnym interesom przedsiębiorcy (art. 11 ust. 1).

Uwaga: Przepis ten dotyczy również osób, które pracowały dla przedsiębiorstwa. Zachowanie tajemnicy obowiązuje przez okres 3 lat od zakończenia pracy, chyba że umowa stanowi inaczej albo ustał stan tajemnicy.

Definicja: **Tajemnica przedsiębiorstwa** to nie ujawnione do wiadomości publicznej informacje techniczne, technologiczne, handlowe lub organizacyjne, co do których przedsiębiorca podjął *niezbędne działania* w celu zachowania ich poufności (art. 11 ust. 4).

Wniosek: **Aby przedsiębiorstwo mogło skorzystać z prawnej ochrony informacji, zgodnie z ustawą o zwalczaniu nieuczciwej konkurencji, informacje muszą zostać najpierw odpowiednio zabezpieczone**.

Tabela 3. Zagrożenie karą za czyny nieuczciwej konkurencji - wg [ustawa ZNK]

Czyn podlegający karze	Podstawa prawna	Zagrożenie karą
Ujawnienie tajemnicy przedsiębiorstwa lub wykorzystanie jej we własnej działalności gospodarczej, gdy wyrządza to poważną szkodę przedsiębiorcy	art. 23 ust. 1	grzywna, ograniczenie lub pozbawienie wolności do lat 2
Bezprawne uzyskanie tajemnicy przedsiębiorstwa i ujawnienie jej innej osobie lub wykorzystanie we własnej działalności gospodarczej	art. 23 ust. 2	grzywna, ograniczenie lub pozbawienie wolności do lat 2
Rozpowszechnianie nieprawdziwych lub wprowadzających w błąd informacji o przedsiębiorstwie (np. o towarach, cenach) w celu zaszkodzenia mu	art. 26 ust. 1-2	grzywna lub areszt

Źródło: opracowanie własne

4.6. Akty prawne - podsumowanie

Tabela 4. Porównanie wybranych praw i obowiązków przedsiębiorstw w zakresie bezpieczeństwa SI na podstawie obowiązujących aktów prawnych

Prawa i obowiązki przedsiębiorstwa	ustawa (wraz z rozporządzeniami)				
	k.k. 1997	o rach. 1994	ODO 1994	PAIPP 1994	ZNK 1993
prawo do traktowania dokumentów elektronicznych na równi z papierowymi	x	x	x	x	
prawo do prawnej ochrony zabezpieczonych informacji	x				x
obowiązek ochrony (wybranych) informacji		x	x		x
obowiązek objęcia tajemnicą (wybranych, kluczowych) informacji	x				x
obowiązek posiadania dokumentacji systemu informatycznego		x	x		
obowiązek posiadania dokumentacji systemu ochrony		x	x		
obowiązek ochrony przed nieupoważnionym dostępem do informacji		x	x		
obowiązek uwierzytelniania i kontroli dostępu do SI			x		
obowiązek powołania osób upoważnionych do obsługi SI			x		
obowiązek powołania osób odpowiedzialnych za bezpieczeństwo SI			x		
obowiązek szkoleń użytkowników systemu z zakresu bezpieczeństwa			x		
obowiązek tworzenia kopii zapasowych		x	x		
obowiązek monitorowania systemu i reagowania na incydenty			x		
obowiązek opracowania szczegółowych zasad i procedur korzystania z SI (np. rejestrowanie użytkowników, korzystanie z haseł, kontrola antywirusowa, awaria)			x		
obowiązek opracowania szczegółowych zasad obchodzenia się z danymi (np. przechowywanie nośników, niszczenie zużytych nośników)		x	x		
obowiązek określenia chronionych stref bezpieczeństwa i zasad dostępu do nich			x		

Źródło: opracowanie własne

- informacje w postaci elektronicznej osiągnęły lub przewyższyły rangą tradycyjne dokumenty papierowe [k.k. 1997; ustawa o rachunkowości 1994],
- prawna ochrona przysługuje informacjom, które są odpowiednio zabezpieczone [k.k. 1997; ustawa ZNK 1993],
- zapewnienie ochrony ważnych informacji i danych w przedsiębiorstwie (np. dane księgowe, dane osobowe, tajemnice państwowe) nie ma charakteru uznaniowego, ale jest ustawowym obowiązkiem [ustawa o rachunkowości 1994; ustawa ODO 1997],
- ochrona SI powinna być kompleksowa i polegać na zaprojektowaniu, wdrożeniu i realizowaniu polityki bezpieczeństwa systemu [ustawa o rachunkowości 1994; ustawa ODO 1997].
- za ochronę informacji i danych przedsiębiorstwa odpowiedzialne jest jego kierownictwo [ustawa o rachunkowości 1994; ustawa ODO 1997].

Wniosek: A**ktualne przepisy prawa nakładają na przedsiębiorstwo obowiązek zarządzania bezpieczeństwem swojego systemu informatycznego**, a odpowiedzialność za prawidłową realizację tego zadania ponosi jego kierownictwo.