Jerzy Depo

Przestępstwo przeciwko ochronie informacji niejawnych i innych prawnie chronionych

Zeszyt Naukowy 6, 175-186

2011

JERZY DEPO

Przestępstwa przeciwko ochronie informacji niejawnych i innych prawnie chronionych

Offences against the protection of classified information and other legally protected information

Abstract: Author of this article, relying on the Classified Information Protection Act from 5th of July 2010, describes, that protected information are those, which disclosure may cause serious harm for the Republic of Poland (among other thing, threat to national security, disrupt of the functioning of the judiciary, adverse impact on the functioning of the national economy or interfere to current foreign politics of the Republic of Poland). Depending on the kind of harm, that disclosure of certain information may cause, specific data are accompanied by the relevant clauses – "secret", "top secret", "confident" or "restricted". Disclosure or abuse (understood here as to use in unlawful manner) classified information implies sanction of law. They may vary depending on public function of the person. The Act provides penalties for offenses, which concern classified and other legally protected information, which are the result of unlawful obtaining of such information or obstructing to become acquainted with it. Author also draws attention to offenses associated with computerized data – their destruction or disruption of the entire system is liable to penalty. There is also illicit, to make computer programs, which are adjusted to commit offenses referred to Classified Information Protection Act. Other acts, which helps to protect safety of information, and which are mentioned by author, are: Banking Law, Personal Data Protection Act and Act on Counteraction Money Laundering and Terrorism Founding.

Key words: classified information, secret information, top secret information, confidential information, sanction

Abstrakt: Autor niniejszej pracy, powołując się na Ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, opisuje, że dane, które podlegają ochronie, to te, których ujawnienie spowodowałoby poważną szkodę dla Rzeczypospolitej Polskiej (między innymi zagrożenie bezpieczeństwa kraju, zakłócenie funkcjonowania organów sprawiedliwości, niekorzystny wpływ na funkcjonowanie gospodarki narodowej czy utrudnianie prowadzenia bieżącej polityki zagranicznej Rzeczypospolitej Polskiej). W zależności od rodzaju wyrządzonej szkody, jaki może spowodować ujawnienie określonych informacji, konkretne dane zostają opatrzone odpowiednimi klauzulami – „tajne", „ściśle tajne", „poufne" oraz „zastrzeżone". Ujawnienie lub wykorzystanie (rozumiane tutaj jako posłużenie się w niezgodny z prawem sposób) informacji niejawnej grozi zastosowaniem sankcji prawa. Różnią się one w zależności od wykonywanej przez daną osobę funkcji publicznej. Ustawa przewiduje kary za przestępstwa dotyczące informacji niejawnych i innych prawnie chronionych, wynikające bądź to z bezprawnego uzyskania takich informacji, bądź utrudniania zapoznania się z nimi. Autor zwraca również uwagę na przestępstwa związane z danymi informatycznymi – karalne jest ich niszczenie czy zakłócenie całego systemu informatycznego. Niedozwolone jest również wytwarzanie programów komputerowych przystosowanych do popełnienia przestępstw określonych w Ustawie o ochronie informacji niejawnych. Inne ustawy, które pomagają chronić bezpieczeństwo informacji, i które zawarto w artykule, to Ustawa Prawo Bankowe, Ustawa o ochronie danych osobowych i Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Słowa kluczowe: informacja niejawna, informacja tajna, informacja ściśle tajna, informacja poufna, sankcje

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[1] stanowi, że ochronie prawnej podlegają:

[1] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228).

1. Dane (informacje o klauzuli „ściśle tajne"), których nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że:
   a) zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej;
   b) zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej;
   c) zagrozi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej;
   d) osłabi gotowość obronną Rzeczypospolitej Polskiej;
   e) doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;
   f) zagrozi lub może zagrozić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie;
   g) zagrozi lub może zagrozić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych[2].
2. Dane (informacje o klauzuli „tajne"), których nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej przez to, że:
   a) uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej;
   b) pogorszy stosunki Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi;
   c) zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych Rzeczypospolitej Polskiej;

[2] *Ibidem*, art. 5 ust. 1, pkt 1-7.

d) utrudni wykonywanie czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione;
e) w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości;
f) przyniesie stratę znacznych rozmiarów w interesach ekonomicznych Rzeczypospolitej Polskiej[3].

3. Dane (informacje o klauzuli „poufne"), których nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że:
a) utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
b) utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;
c) zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli;
d) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
e) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
f) zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej;
g) wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej[4].

4. Dane (informacje o klauzuli „zastrzeżone"), których nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru

[3] *Ibidem*, art. 5 ust. 2, pkt 1-6.
[4] *Ibidem*, art. 5 ust. 3, pkt 1-7.

sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej[5].

5. Informacje niejawne przekazane przez organizacje międzynarodowe lub inne państwa na podstawie umów międzynarodowych oznaczonych polskim odpowiednikiem posiadanej klauzuli tajności[6].

W aktualnym stanie prawnym sprawy związane z ochroną i czynami przeciwko ochronie informacji niejawnych penalizuje, przede wszystkim ustawa z 6 czerwca 1997 r. – Kodeks karny[7]. A czynami przestępczymi są w szczególności naruszenia przepisów przedmiotowej ustawy (UoOIN) ujęte w rozdziale XXXIII, w art. 265 – ujawnianie lub wykorzystanie informacji niejawnych, art. 266 – ujawnianie informacji niejawnych w związku z wykonywaną funkcją, art. 267 – bezprawne uzyskanie informacji, w art. 268 – utrudnianie zapoznania się z informacją, art. 268a – niszczenie danych informatycznych, art. 269 – uszkodzenie danych informatycznych, w art. 269a – zakłócenie systemu komputerowego i w art. 269b – wytwarzanie programów komputerowych[8].

Ujawnianie lub wykorzystanie informacji niejawnej:

Art. 265 § 1. „Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje niejawne o klauzuli «tajne» lub «ściśle tajne», podlega karze pozbawienia wolności od 3 miesięcy do lat 5”[9];

[5] *Ibidem*, art. 5 ust. 4.

[6] W języku angielskim, polskim oznaczeniom odpowiadają: „ściśle tajne” – *top secret*, „tajne” – *secret*, „poufne” – *confidential*, „zastrzeżone” – *restricted*.

[7] Ustawa z dnia 6 czerwca 1997 r. – Kodeks Karny (Dz. U. z 1997 r. Nr 88, poz. 553 z późn. zm.).

[8] *Ibidem*, s. 95-97.

[9] Określona tu norma karnoprawna przewiduje dwie różniące się od siebie postacie popełnienia przestępstwa: 1) ujawnienie informacji niejawnej, 2) wykorzystanie informacji niejawnej wbrew przepisom ustawy. Różnice dotyczą: 1) sprawcy (strony podmiotowej) przestępstwa – w pierwszym przypadku, sprawcą jest każdy, kto w sposób uprawniony bądź nieuprawniony wszedł w posiadanie informacji niejawnej, w drugim zaś sprawcą przestępstwa będzie osoba z mocy ustawy zobligowana do ochrony tej informacji, 2) przedmiotowej strony przestępstwa – sposobu działania sprawcy; w pierwszym przypadku chodzi o ujawnienie informacji, w drugim – o niezgodne z prawem posłużenie się informacją niejawną

§ 2. „Jeżeli informację określoną w § 1 ujawniono osobie działającej w imieniu lub na rzecz podmiotu zagranicznego, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 8”[10];

§ 3. „Kto nieumyślnie ujawnia informację określoną w § 1, z którą zapoznał się w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku”[11].

Ujawnianie informacji niejawnej w związku z wykonywaną funkcją:

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”[12];

§ 2. „Funkcjonariusz publiczny[13], który ujawnia osobie nieuprawnionej informację niejawną o klauzuli «zastrzeżone» lub «poufne» lub infor-

[10] Przestępstwo określone w § 2 ma kwalifikowaną postać czynu i polega na ujawnieniu informacji niejawnej osobie działającej w imieniu lub na rzecz podmiotu zagranicznego, a osoba ta może być zarówno obywatelem polski, jak i cudzoziemcem.

[11] W paragrafie 3 ujęto karalność nieumyślnego ujawnienia informacji niejawnej (dopuszczenia do utraty lub zagubienia materiału niejawnego – dokumentu lub przedmiotu), przez osoby, które zapoznały się z nią w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem. Sprawca tego czynu odpowiada jednak tylko wtedy, gdy utrata lub zagubienie materiału niejawnego spowodowało skutek w postaci ujawnienia informacji niejawnej. O tym, kto jest osobą pełniącą funkcję publiczną stanowi art. 19.

[12] Do znamion przestępstwa określonego w tym przepisie należy ujawnienie lub wykorzystanie informacji niejawnej tylko wtedy, gdy następuje ono wbrew przepisom ustawy lub przyjętemu zobowiązaniu.

[13] W myśl § 13 k.k. funkcjonariuszem publicznym jest: 1) Prezydent Rzeczypospolitej Polskiej, 2) poseł, senator, radny, 3) poseł do Parlamentu Europejskiego, 4) sędzia, ławnik, prokurator, funkcjonariusz finansowego organu postępowania przygotowawczego lub organu nadrzędnego nad finansowym organem postępowania przygotowawczego, notariusz, komornik, kurator sądowy, syndyk, nadzorca sądowy i zarządca, osoba orzekająca w organach dyscyplinarnych działających na podstawie ustawy, 5) osoba będąca pracownikiem administracji rządowej, innego

mację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3”[14].

Bezprawne uzyskanie informacji:

Art. 267 § 1. „Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2”;

§ 2. „Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego”;

§ 3. „Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem”.

Utrudnianie zapoznania się z informacją:

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”;

---

organu państwowego lub samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe, a także inna osoba w zakresie, w którym uprawniona jest do wydawania decyzji administracyjnych, 6) osoba będąca pracownikiem organu kontroli państwowej lub organu kontroli samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe, 7) osoba zajmująca kierownicze stanowisko w innej instytucji państwowej, 8) funkcjonariusz organu powołanego do ochrony bezpieczeństwa publicznego albo funkcjonariusz Służby Więziennej, 9) osoba pełniąca czynną służbę wojskową.

[14] Chodzi o funkcjonariusza publicznego, który ujawnia informację niejawną osobie nieuprawnionej, tj. takiej, która nie została przepisami prawa dopuszczona do jej poznania.

§2. „Jeżeli czyn określony w § l dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3".

Niszczenie danych informatycznych:

Art. 268a § 1. „Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3";

§ 2. „Kto, dopuszczając się czynu określonego w § l, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5";

§ 3. „Ściganie przestępstwa określonego w § l lub 2 następuje na wniosek pokrzywdzonego".

Uszkodzenie danych informatycznych:

Art. 269 § 1. „Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8";

§ 2. „Tej samej karze podlega, kto dopuszcza się czynu określonego w § l, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych".

Zakłócenie systemu informatycznego:

Art. 269a. „Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu kompu-

terowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5".

Wytwarzanie programów komputerowych:

Art. 269b § 1. „Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § l pkt 4, art. 267 § 3, art. 268a § l albo § 2, w związku z § l, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3".

Kradzież programu komputerowego:

Art. 278 § 1. „Kto zabiera w celu przywłaszczenia cudzą rzecz ruchomą, podlega karze pozbawienia wolności od 3 miesięcy do lat 5";

§ 2. „Tej samej karze podlega, kto bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy w celu osiągnięcia korzyści majątkowej".

Oszustwo komputerowe:

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

Zakres czynów oraz sankcje karne za naruszenie przepisów w zakresie ochrony określonych informacji penalizują również inne ustawy; m.in.:

Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe[15]:

[15] Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2002 r. Nr 72, poz. 665 z późn. zm.).

Art. 170 Ust. 4. Zatajanie lub podawanie uprawnionym organom nieprawdziwych informacji dotyczących banku i jego klientów,

Ust. 5. Ujawnianie lub wykorzystywanie niezgodnie z upoważnieniem informacji bankowych.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[16]:

Art. 49 § 1. Przetwarzanie danych osobowych w zbiorze bez prawa przetwarzania tych danych;

§ 2 . Przetwarzanie danych wrażliwych bez prawa ich przetwarzania.

Art. 50. Przetwarzanie danych osobowych w zbiorze niezgodnie z celem utworzenia zbioru.

Art. 51 § 1. Udostępnianie danych osobowych lub umożliwianie dostępu do nich osobom nieupoważnionym.

Art. 52. Naruszenie choćby nieumyślne obowiązku zabezpieczenia danych osobowych przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem.

Art. 53. Nie zgłaszanie do rejestracji zbioru danych będąc do tego zobowiązanym.

Art. 54. Nie dopełnienie obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w ustawie.

Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[17]:

Art. 35 Ust. 1 pkt. 3. Niedopełnienie obowiązku poinformowania Generalnego Inspektora Informacji Finansowej o transakcji mogącej mieć związek z praniem brudnych pieniędzy lub finansowaniem terroryzmu;

[16] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 102, poz. 926 z późn. zm.).

[17] Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2010 r. Nr 46, poz. 276.).

Ust. 2. Ujawnienie osobom niepowołanym (posiadaczom rachunku lub osobom, których transakcja dotyczy) informacji zgromadzonych zgodnie z ustawą.

Art. 36. Odmowa przekazania Generalnemu Inspektorowi informacji lub dokumentów, albo zatajenie lub przekazanie nieprawdziwych danych dotyczących transakcji, rachunków i osób.

Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym[18]:

Art. 107 ust. 2 pkt 9. Utrata przez funkcjonariusza CBA materiału zawierającego informacje niejawne jest naruszeniem dyscypliny służbowej.

Szczególnym przestępstwem, zarówno przeciwko Rzeczypospolitej Polskiej, jak i informacjom niejawnym, są czyny określone w art. 130 k.k.

Przestępstwo szpiegostwa:

Art. 130 § 1. „Kto bierze udział w działalności obcego wywiadu przeciwko Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności od roku do lat 10";

§ 2. „Kto, biorąc udział w obcym wywiadzie albo działając na jego rzecz, udziela temu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności na czas nie krótszy od lat 3";

§ 3. „Kto, w celu udzielenia obcemu wywiadowi wiadomości określonych w § 2, gromadzi je lub przechowuje, wchodzi do systemu informatycznego 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. „Kto działalność obcego wywiadu organizuje lub nią kieruje, podlega karze pozbawienia wolności na czas nie krótszy od lat 5, albo karze 25 lat pozbawienia wolności".

[18] Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 z późn. zm.).

Bibliografia

1. Ustawa z 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 1997 r. Nr 88, poz. 553 z późn. zm.).
2. Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2002 r. Nr 72, poz. 665 z późn. zm.).
3. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 102, poz. 926 z późn. zm.).
4. Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2010 r. Nr 46, poz. 276).
5. Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708 z późn. zm.).
6. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228).

Recenzent – Reviewer:
dr hab. prof. nadzw. Leszek Korzeniowski – kierownik Zakładu Zarządzania na Wydziale Turystki i Rekreacji Akademii Wychowania Fizycznego w Krakowie, prezes European Assosiation for Security (EAS).