Warszawska Wyższa Szkoła Informatyki

Zarządzanie Cyberbezpieczeństwiem w działalności przedsiębiorstw

studia podyplomowe

Informacje o kierunku.

Uczelnia: Warszawska Wyższa Szkoła Informatyki

Poziom studiów: studia podyplomowe dla absolwentów studiów I,II oraz III stopnia

Nazwa kierunku: Zarządzanie Cyberbezpieczeństwem w działalności przedsiębiorstw

Czas trwania studiów: 2 semestry (160 godzin)

Forma studiów: zajęcia realizowane w formie stacjonarnej

Kwalifikacje i certyfikaty: Dyplom ukończenia studiów podyplomowych Warszawskiej Wyższej Szkoły Informatyki o kierunku Zarządzanie Cyberbezpieczeństwem w działalności przedsiębiorstw.

Organizacja studiów.

Program studiów podyplomowych w specjalności *Zarządzanie Cyberbezpieczeństwem w działalności przedsiębiorstw* realizowany w Warszawskiej Wyższej Szkole Informatyki uwzględnia szerokie spektrum zagrożeń wynikających z niewłaściwego zabezpieczenia i niepoprawnego korzystania z zasobów sieci. Program spełnia wymagania standardów kształcenia określone przez Ministra Nauki i Szkolnictwa Wyższego oraz zalecenia standardów akredytacji Państwowej Komisji Akredytacyjnej. Szczególny nacisk położony został na kwestie praktyczne związane z zarządzaniem cyberbezpieczeństwem.

Program studiów podyplomowych w specjalności *Zarządzanie Cyberbezpieczeństwem w działalności przedsiębiorstw* obejmuje łącznie 160 godzin dydaktycznych. Czas trwania studiów wynosi 1 rok (dwa semestry). Zajęcia odbywają się co dwa tygodnie w trybie weekendowym (stacjonarnie).

Metodyka kształcenia:

Zajęcia na studiach podyplomowych w specjalności *Zarządzanie Cyberbezpieczeństwem w działalności przedsiębiorstw* prowadzone są w większości w postaci warsztatów, podczas których słuchacze rozwiązują studia przypadków opracowane przez wykładowcę na podstawie rzeczywistych

incydentów. Dominuje dyskusja oraz wymiana doświadczeń, zajęcia prowadzą praktycy branży bezpieczeństwa teleinformatycznego .

Ramowy program studiów.

Poniższy program powstał we współpracy Warszawskiej Wyższej Szkoły Informatyki oraz Naukowej i Akademickiej Sieci Komputerowej.

Lp.	Nazwa przedmiotu	Zagadnienia	Liczba godzin
1.	Wstęp do bezpieczeństwa teleinformatycznego	1. Wiarygodność systemów komputerowych 2. Czym jest bezpieczeństwo TI 3. Mechanizmy zarządzania bezpieczeństwem 4. Wstęp do kryptografii 5. Bezpieczeństwo a system DNS	4
2.	Bezpieczeństwo sieci teleinformatycznych	1. Wprowadzenie do problematyki bezpieczeństwa sieci teleinformatycznych (terminologia, organizacje, normy) 2. Zarządzanie bezpieczeństwem (polityka bezpieczeństwa, tworzenie procedur bezpieczeństwa) 3. Podstawy kryptografii i środowisko PKI 4. Kontrola dostępu 5. Zarządzanie zaufaniem 6. Aktualne trendy ataków (typy, zapobieganie) 7. Zagrożenia i podatności (źródła, miary) 8. Systemy wykrywania włamań IDS/IPS Sieci VPN	10
3.	Cyberprzestępczość i inne zagrożenia we współczesnej sieci Internet	1. Zagrożenia w sieci Internet – ewolucja i klasyfikacja 2. Obsługa incydentów w sieci Internet i najważniejsze problemy z nią związane 3. Funkcjonowanie podziemia przestępczego w sieci Internet – spojrzenie od strony technicznej 4. Sposoby wykrywania, analizowania i śledzenia zagrożeń w sieci Internet	16
4.	Przeciwdziałanie cyberatakom – technologie i mechanizmy bezpieczeństwa w sieciach i systemach IT	1. Firewalling 2. Systemy IPS/IDS, 3. Bezpieczeństwo i systemy ochrony stacji roboczych 4. Systemy Antymalware protection 5. Systemy monitoringu, korelacji zdarzeń i przeciwdziałania atakom na dostępność systemów 6. Dobór i utrzymanie technologii zabezpieczeń oraz proces oceny skuteczności działania systemów bezpieczeństwa	16

5.	Aspekty bezpieczeństwa sieci i informacji wynikające z uregulowań prawnych i dokumentów programowych UE oraz krajowych.	1. Wprowadzenie do zagadnienia – podejście UE do tematyki cyberbezpieczeństwa 2. Omówienie najważniejszych dokumentów definiujących zagadnienia bezpieczeństwa sieci i informacji w UE (min. strategia cyberbezpieczeństwa, dyrektywa NIS) 3. Regulacje europejskie w obszarze cyberbezpieczeństwa a stan uregulowań na poziomie krajowym	6
6.	Przykładowe skutki dla przedsiębiorców wynikające z uregulowań dotyczących bezpieczeństwa teleinformatycznego	1. Wymagania i mechanizmy dotyczące bezpieczeństwa obowiązujące w sektorze telekomunikacyjnym. 2. Planowane mechanizmy i wymagania bezpieczeństwa ICT przewidziane w dyrektywie NIS • operatorzy usług kluczowych • dostawcy usług cyfrowych 3. Obowiązki wynikające z innych przepisów	6
7.	Zarządzanie ryzykiem zagrożeń bezpieczeństwa organizacji i instytucji	1. Analiza ryzyka – wprowadzenie 2. Rodzaje ryzyk i obszary występowania. 3. Metody szacowania ryzyka 4. Normy i metodyki 5. Zarządzanie ryzykiem w bezpieczeństwie informacji PN-ISO\IEC 27005:2014	12
8.	Charakterystyka zagrożeń internetowych dotyczących szkodliwych treści	1. Sposoby korzystania z internetu i nowych technologii 2. Rodzaje zagrożeń oraz nadużyć internetowych związanych z treściami 3. Treści przedstawiające seksualne wykorzystania małoletnich charakterystyka zjawiska 4. Regulacja prawne w odniesieniu do szkodliwych treści – perspektywa krajowa i międzynarodowa 5. Profilaktyka w odniesieniu do zagrożeń internetowych 6. Małoletni - szczególny użytkownik 7. Współpraca międzynarodowa na rzecz bezpieczeństwa korzystania z internetu	6
9.	Laboratorium bezpieczeństwa teleinformatycznego	1. Nauka korzystania z podstawowych narzędzi, omówienie poszczególnych protokołów 2. Tworzenie i używanie środowiska wirtualnego do podstawowej analizy i monitorowania złośliwych aplikacji 3. Wykrywanie i przeciwdziałanie atakom i infekcjom na poziomie własnej sieci 4. Współdziałanie technologii bezpieczeństwa w praktyce – analiza przebiegu cyberataku na podstawie strumienia danych oraz zapisów pracy systemów bezpieczeństwa	24

10.	Aktywne zarządzanie bezpieczeństwem infrastruktury IT – na przykładzie koncepcji SOC	1. Koncepcja Security Operations Center (SOC) 2. Modele monitorowania i zarzadzania bezpieczeństwem w oparciu o SOC 3. Źródła informacji zbierane w centrum 4. Scenariusze zagrożeń, alerty 5. Procedury reagowania 6. Usługi typu MSS	12
11.	Cloud Computing i Big Data – bezpieczeństwo danych	1. Główne wyzwania bezpieczeństwa Big Data oraz przetwarzania w chmurze 2. Modele świadczonej usługi a problemy z obszaru bezpieczeństwo danych: • SaaS – Software as a Service, • PaaS – Platform as a Service • IaaS – Infrastructure as a Service, • SaaS - Security as a Service) 3. Zalety i wady oraz przyszłość rozwiązań chmurowych perspektywa operatora i klienta.	5
12.	Usługi elektronicznej identyfikacji i usługi zaufania	1. Zagadnienie elektronicznej identyfikacji 2. Usługi zaufania 3. Rozporządzenie eIDAS 4. Polskie regulacje dotyczące eIDAS	5
13.	Psychologiczne i społeczne aspekty bezpieczeństwa w Internecie	1. Charakterystyka zagrożeń internetowych – psychospołeczne aspekty nadużyć. 2. Informacja i dezinformacja – tworzenie komunikatu, analiza prawdziwości przekazu, obieg i dystrybucja informacji. 3. Manipulacja – metody wpływania na odbiorcę, budowanie fałszywego przekazu. 4. Sposoby i techniki analizy przekazu informacyjnego	6
14	Zagadnienia prywatności i ochrony danych osobowych		12
15	Wprowadzenie do eksploracji danych w cyberbezpieczeństwie		4
16	Ochrona infrastruktury krytycznej państwa		6
17	Prezentacje prac grupowych (egzamin)		10
	suma		**160**

Zajęcia w ramach specjalności *Zarządzanie Cyberbezpieczeństwem w działalności przedsiębiorstw* prowadzi doświadczona kadra składającą się głównie z praktyków*:

• *Piotr Bisialski* - menedżer produktów bezpieczeństwa w NASK z 8 letnim doświadczeniem w branży ICT. Inżynier specjalizacji Systemy Teleinformatyczne na Wojskowej Akademii Technicznej. Uzyskał również tytuł magistra inżyniera w Wyższej Szkole Informatyki Stosowanej i Zarządzania ze specjalizacją Zarządzanie w teleinformatyce. Na co dzień realizuje projekty z zakresu bezpieczeństwa teleinformatycznego. Trener programów szkoleniowych z zakresu usług telekomunikacyjnych i bezpieczeństwa teleinformatycznego

• *Andrzej Chrząszcz* - absolwent wydziału Elektrycznego Politechniki Warszawskiej. W latach 1992-1993 pracownik Centrum Informatycznego Uniwersytetu Warszawskiego. Od 1994 roku pracuje w Naukowej i Akademickiej Sieci Komputerowej. W latach 1994-1995 odpowiedzialny za Zespół Operatorów Centralnego węzła sieci NASK. Od 1996 pracownik Zespołu Ochrony Sieci. W ramach prac zespołu zajmuje się projektowaniem i implementacją rozwiązań z dziedziny bezpieczeństwa sieciowego oraz audytami systemów informatycznych. Bierze udział w tworzeniu i późniejszych pracach zespołu CERT POLSKA. Współorganizator i wykładowca konferencji SECURE. Współautor opracowań z dziedziny bezpieczeństwa sieci dla Komitetu Badań Naukowych, autor publikacji z dziedziny sieci komputerowych i bezpieczeństwa teleinformatycznego. Posiada wiedzę z zakresu audytów systemów Informacyjnych potwierdzoną certyfikatem CISA (Certified Information System Auditor), a także wiedzę w zakresie rozwiązania RSA SecurID potwierdzoną Certyfikatem RSA SecurID Certified Administrator. Szkolenie z zakresu zarządzanie projektami i znajomość metodyki PRINCE 2.

- *Anna Felkner* - absolwentka studiów magisterskich na Wydziale Informatyki Politechniki Białostockiej i studiów doktoranckich na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej. Obecnie pracuje jako adiunkt w Pracowni Metod Bezpieczeństwa Sieci i Informacji Pionu Naukowego NASK. Główne zainteresowania badawcze dotyczą bezpieczeństwa systemów informatycznych, w szczególności kontroli dostępu i zarządzania zaufaniem. Autorka licznych publikacji naukowych. Zaangażowana w projekty badawcze krajowe i międzynarodowe m. in. nt. bezpieczeństwa teleinformatycznego.

- *Tomasz Grudziecki* - mgr inż., jest starszym specjalistą w Zespole Projektów Bezpieczeństwa w CERT Polska działającym w strukturach organizacyjnych instytutu badawczego NASK. Posiada 9 lat doświadczenia w analizie zagrożeń sieciowych oraz tworzeniu i używaniu systemów do proaktywnego wykrywania incydentów bezpieczeństwa. Autor i współautor prezentacji, raportów i artykułów poświęconych bezpieczeństwu IT. Instruktor branżowych szkoleń i warsztatów.

- *Paweł Jacewicz* - pracuje w Zespole Projektów Bezpieczeństwa CERT Polska na stanowisku Starszego Specjalisty. Specjalizuje się w tworzeniu systemów wczesnego ostrzegania opartych na rozwiązaniach typu honeypot. Dodatkowo, interesuje się zagadnieniami z obszarów takich jak ataki na aplikacje klienckie oraz bezpieczeństwo aplikacji webowych. Jest współautorem szeregu prac opublikowanych przez agencję ENISA poświęconych zagadnieniom bezpieczeństwa IT.

- *Janusz Janiszewski* - absolwent wydziału Elektrycznego Politechniki Warszawskiej. Od 1996 roku pracuje w Naukowej i Akademickiej Sieci Komputerowej. Od początku pracuje w Zespole Bezpieczeństwa i CERT NASK (później CERT POLSKA). W ramach prac zespołu zajmuje się projektowaniem i wdrażaniem systemów bezpieczeństwa sieciowego oraz audytami Systemów teleinformatycznych. Od 1999 roku pełni w NASK funkcje Oficer Bezpieczeństwa. Brał udział w tworzeniu i późniejszych pracach zespołu CERT POLSKA. Współorganizator i wykładowca konferencji SECURE. Autor opracowań z dziedziny bezpieczeństwa sieci. Wykładowca i autor szkoleń z zakresu bezpieczeństwa teleinformatycznego. Certyfikowany Administrator i Ekspert Checkpoint (CCSA, CCSE) dla wersji 4.1 i NG. Szkolenie z zakresu zarządzanie projektami i znajomość metodyki PRINCE 2.

- *Andrzej Kaczmarek* - absolwent Wydziału Elektroniki Politechniki Wrocławskiej. W 1986 r. uzyskał tytuł doktora nauk technicznych na Wydziale Elektrotechniki, Automatyki, Informatyki i Elektroniki AGH. Od 1998 r. jest dyrektorem departamentu informatyki w Biurze Generalnego Inspektora Ochrony Danych Osobowych. W ramach wykonywanej pracy zajmuje się nadzorem merytorycznym nad rozwojem systemów informatycznych Biura GIODO oraz oceną zgodności systemów informatycznych z wymaganiami określonymi w ustawie o ochronie danych osobowych. Od roku 1999 uczestniczy w pracach międzynarodowej grupy roboczej (International Working Group on Data Protection in Telecommunications), zajmującej się ochroną danych osobowych w telekomunikacji.

- *Tomasz Kruk* - informatyk, dyrektor operacyjny instytutu badawczego NASK, w ramach którego funkcjonuje m.in. zespół CERT Polska. W latach 2010 – 2015 członek Komitetu Sterującego ds. badań naukowych i prac rozwojowych w obszarze bezpieczeństwa i obronności państwa w NCBiR. Od 2012 roku członek Rady Polskiej Izby Informatyki i Telekomunikacji. Wykłada informatykę na Politechnice Warszawskiej. Ekspert w zakresie bezpieczeństwa informacji i systemów informatycznych dużej skali.

- *Marta Różycka* - absolwentka Informacji Naukowej i Bibliotekoznawstwa na Uniwersytecie Warszawskim. Od trzech lat związana z projektem „Safer Internet" – a szczególnie z polskim punktem kontaktowym, przyjmującym zgłoszenia o treściach nielegalnych i szkodliwych w Internecie.

- *Maciej Siciarek* - absolwent Instytutu Telekomunikacji Wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej. Od 1998 pracuje w Naukowej i Akademickiej Sieci Komputerowej. W latach 1998-2001 zajmował się projektowaniem, implementacją i utrzymaniem sieci rozległych oraz sieci korporacyjnych VPN dla dużych przedsiębiorstw oraz administracji państwowej. Od 2001 roku w Zespole Integracji i Bezpieczeństwa Systemów kontynuuje prace nad bezpieczeństwem systemów teleinformatycznych.

- *Krzysztof Silicki* - mgr inż. Absolwent Politechniki Warszawskiej. Od roku 1992 związany z NASK. Doradca Dyrektora NASK, Wiceprzewodniczący Rady Zarządzającej Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA).W latach 2001-2013 Krzysztof Silicki był Dyrektorem ds. Technicznych NASK (jbr, potem instytut badawczy). Od 2004 jest Przedstawicielem Rzeczpospolitej Polskiej w ENISA, jako członek Rady Zarządzającej tej agencji. Od roku 2014 także w Radzie Wykonawczej ENISA. Założyciel pierwszego w Polsce zespołu reagującego na incydenty naruszające bezpieczeństwo w sieci – CERT NASK (w roku 1996), działającego współcześnie jako CERT Polska. Pomysłodawca i współorganizator organizowanej przez NASK od 1997 r. konferencji „SECURE" – pierwszej w Polsce konferencji poświęconej tematyce bezpieczeństwa IT. Zaangażowany w szereg projektów podwyższających bezpieczeństwo internetu w Polsce. Autor publikacji dziedzinowych oraz szkoleń z bezpieczeństwa IT.
- *Dariusz Stefański* - Projektant Systemów Bezpieczeństwa w Naukowa i Akademicka Sieć Komputerowa NASK - Naukowa i Akademicka Sieć Komputerowa NASK.

- *Krzysztof Stryjek* - absolwent Wydziału Elektrycznego Politechniki Warszawskiej. Praktyka zawodowa obejmowała stanowiska programisty, administratora sieci, serwerów UNIXowych jak również MS Windows. Obecnie zatrudniony w NASK w Zespole Bezpieczeństwa i Integracji Systemów, bierze udział w audytach systemów teleinformatycznych. Prelegent konferencji SECURE. Znajomość zagadnień z zakresu zarządzania ciągłością działania potwierdzona szkoleniem i certyfikatem w zakresie normy BS-25999. Certyfikowany inżynier Fortinet (Fortigate, Fortimail).

- *dr hab. Inż. Jerzy Surma* - jest absolwentem Wydziału Informatyki i Zarządzania Politechniki Wrocławskiej oraz ukończył m.in. Executive Program na MIT Sloan School of Management. W ostatnich latach pracował jako visiting scholar w Harvard Business School oraz jako profesor na University of Massachusetts Lowell. Był dyrektorem ds. Konsultingu Biznesowego w IMG Information Management Polska. Naukowo zajmuje się analizami oraz eksploracją danych m.in. w zakresie Social Media, Business Intelligence oraz Cyber Threat Intelligence.

- Agnieszka Wrońska - kierownik Działu Akademia NASK w Naukowej i Akademickiej Sieci Komputerowej instytucie badawczym, doktor nauk humanistycznych, licencjonowany trener

i superwizor, członek-założyciel Polskiego Stowarzyszenia Pedagogów i Animatorów KLANZA, inicjator i koordynator wielu programów i projektów animacji kulturalnej i środowiskowej, również międzynarodowych. Posiada duże doświadczenie w realizacji zadań badawczych i dydaktycznych dla różnych grup wiekowych o zróżnicowanych potrzebach edukacyjnych i społecznych. Realizowała szereg działań na rzecz bezpieczeństwa dzieci i młodzieży w Internecie. Ekspert w projektach m.in.: Komisji Europejskiej Safer Internet, „Kursor", „Przygody Plika i Foldera w sieci", „Podaj dalej – Senior dla Kultury". Autorka licznych publikacji oraz podręczników edukacyjnych dla uczniów szkół podstawowych.

Adresaci studiów i sylwetka absolwenta.

Adresatami studiów są pracownicy przedsiębiorstw odpowiedzialni za zagrożenia cybernetyczne.

Osoba uczestnicząca w studiach powinna posiadać ogólną i podstawową wiedzę z:

a) działania systemów operacyjnych typu Windows oraz Linux

b) obsługi tychże systemów (w tym podstawowej umiejętności posługiwania się konsolą linuksową)

c) działania sieci teleinformatycznych, w tym podstawowe informacje dot. protokołów IP, TCP i UDP

d) podstawy protokołów sieciowych warstw wyższych, takich jak HTTP/HTTPS i DNS (czyli jak działa infrastruktura WWW) oraz SMTP (poczta elektroniczna)

Student specjalności *Zarządzanie Cyberbezpieczeństwem w działalności przedsiębiorstw* nabywa wiedzę i umiejętności z zakresu szeroko pojętego bezpieczeństwa IT, w szczególności powinien być przygotowany do:

- praktycznego wykorzystania wiedzy z zakresu przeciwdziałania cyberatakom oraz mechanizmów bezpieczeństwa w sieciach i systemach IT
- praktycznego wykorzystania wiedzy o mechanizmach oceny sieci i jakości zabezpieczeń
- prognozowania zagrożeń w systemie zarządzania cyberbezpieczeństwem
- stosowania w praktyce systemów technologii bezpieczeństwa komputerowego
- tworzenia i używania środowiska wirtualnego do analizy i monitorowania złośliwych aplikacji
- obsługi incydentów w sieci Internet
- doboru i utrzymania technologii zabezpieczeń
- opracowania koncepcji zabezpieczenia fizycznego infrastruktury teleinformatycznej na podstawie wymagań normatywnych w zakresie ochrony informacji i zabezpieczenia techniczno-organizacyjnego
- administrowania systemami komputerowymi zgodnie z polityką bezpieczeństwa informacji

Warunki uczestnictwa w studiach podyplomowych .

Uczestnikiem studiów podyplomowych może zostać osoba, która posiada dyplom ukończenia studiów I lub II stopnia.

Koszt studiów.

Opłata za całość studiów wynosi 3900zł.

Studia podyplomowe w Warszawskiej Wyższej Szkole Informatyki.

Warszawska Wyższa Szkoła Informatyki jest uznanym ośrodkiem kształcenia specjalistów na studiach podyplomowych. Uczelnia uzyskała granty unijne na prowadzenie studiów podyplomowych:
dyplomy ukończenia specjalistycznych studiów podyplomowych IT Warszawskiej Wyższej Szkoły Informatyki oraz certyfikaty branżowe IT otrzymało w ciągu ostatnich 8 lat ponad 1000 absolwentów w ramach poniższych specjalizacji:

a) *Bazy Danych i Business Intelligence-142 osoby*
b) *Bezpieczeństwo Systemów i Sieci komputerowych – 8 osób*
c) Bezpieczeństwo Systemów Teleinformatycznych-97 osób
d) Internetowe aplikacje bazodanowe-20 osób
e) Systemy i Sieci teleinformatyczne-135 osób
f) Zarządzanie Projektami-119 osób
g) Zarządzanie Projektami Informatycznycznymi-179 osób
h) Zarządzanie Sieciami Teleinformatycznymi-115 osób
i) Administrowanie Sieciami Komputerowymi-19 osób
j) IT Project Manager-80 osób
k) Bazy Danych i analiza danych w biznesie-60 osób
l) Technologie multimedialne i grafika komputerowa-18 osób
m) Zarządzanie środowiskiem serwerowym-38 osób

Pracowników na studia podyplomowe do WWSI kierowały zarówno czołowe firmy z branży ICT, jak również firmy z innych sektorów gospodarki. W gronie pracodawców, którzy zatrudniają absolwentów studiów podyplomowych Warszawskiej Wyższej Szkoły Informatyki znajdują się między innymi: Computer Service Support S.A., Grupa Wydawnicza INFOR S.A., Przedsiębiorstwo Informatyki ZETO Bydgoszcz S.A., Małopolska Agencja Doradczo Edukacyjna Sp. z o.o z Krakowa, Telekomunikacja Polska S.A., Crowley Data Poland Sp. z o.o., BONAIR S.A., TP INTERNET Sp. z o.o., WITTCHEN Sp. z o.o., Xerox Polska Sp. z o.o., ACCENTURE Sp. z o.o, AGORA S.A., Asseco Poland S.A., Aster Sp. z o.o., AVIVA Towarzystwo Ubezpieczeń na Życie S.A, Bank Gospodarki Żywnościowej S.A., Bank Handlowy w

Warszawie S.A., Bank Millenium S.A., Bank Polska Kasa Opieki S.A., BRE BANK S.A., Capgemini Polska Sp. z o.o, Citibank Handlowy, Cyfrowy Polsat S.A., DEUTSCHE BANK PBC S.A., Fabryka Dywanów "Agnella" S.A., Fujitsu Technology Solutions Sp. z o.o., Hewlett-Packard Polska, Inteligo Financial services S.A., Krajowa Izba Rozliczeniowa S.A., Kredyt Bank S.A., Laboratorium Kosmetyczne "Joanna" Sp. j., Nadleśnictwo Nowe Ramuki, NASK, NETIA S.A., Nokia Siemens Networks Sp. z o.o., PKO BANK POLSKI S.A., Polska Telefonia Cyfrowa Sp. z o.o., POLKOMTEL S.A., Powszechny Zakład Ubezpieczeń S.A., RAIFFEISEN BANK POLSKA S.A., RUCH S.A., Skarbnica Mennicy Polskiej S.A., SOCIETE GENERALE SA Oddział w Polsce, Szkoła Wyższa Psychologii Społecznej, Telewizja Polska S.A., The Royal Bank of Scotland N.V. S.A. Oddział w Polsce, Towarzystwo Ubezpieczeniowe Compensa S.A., Towarzystwo Ubezpieczeń i Reasekuracji WARTA S.A., Wojskowy Instytut Chemii i Radiometrii i wiele innych.