Warszawska Wyższa Szkoła Informatyki

Zarządzanie Cyberbezpieczeństwiem w Administracji Publicznej

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 Administracji Publicznej

Czas trwania studiów: 2 semestry (180 godzin)

Forma studiów: zajęcia realizowane w formie hybrydowej: 50 % zajęć stacjonarnych i 50 % zajęć w formie zdalnej.

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

Organizacja studiów.

Program studiów podyplomowych w specjalności *Zarządzanie Cyberbezpieczeństwem w Administracji Publicznej* 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 Administracji Publicznej* obejmuje łącznie 180 godzin dydaktycznych. Studia będą realizowane w technologii „blended learning", a więc część zajęć tradycyjnej (ok. 50%) a część w formie wideokonferencji (ok. 50%). Czas trwania studiów wynosi 1 rok (dwa semestry). Zajęcia odbywają się co dwa tygodnie w trybie weekendowym wg. poniższego harmonogramu:

zjazd numer:	tryb zajęć:
1	stacjonarny
2	widekonferencyjny
3	stacjonarny
4	widekonferencyjny
5	stacjonarny
6	widekonferencyjny
7	widekonferencyjny
8	stacjonarny
9	widekonferencyjny
10	stacjonarny
11	widekonferencyjny
12	stacjonarny

Metodyka kształcenia:

Zajęcia na studiach podyplomowych w specjalności *Zarządzanie Cyberbezpieczeństwem w Administracji Publicznej* 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 m.in praktycy branży bezpieczeństwa teleinformatycznego .

Ramowy program studiów.

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

Lp.	Nazwa przedmiotu	Zagadnienia	Liczba godzin
1.	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.** Relewantne typy dokumentów na poziomie UE: komunikaty, strategie, dyrektywy, rozporządzenia **3.** Omówienie najważniejszych dokumentów definiujących zagadnienia bezpieczeństwa sieci i informacji w UE (min. strategia cyberbezpieczeństwa, dyrektywa NIS, rozporządzenie e-IDAS) **4.** Regulacje europejskie w obszarze cyberbezpieczeństwa a stan uregulowań na poziomie krajowym **5.** Omówienie aspektów krajowego bezpieczeństwa w kontekście istniejących i powstających dokumentów programowych (min. doktryna cyberbezpieczeństwa, strategia bezpieczeństwa	6

		cyberprzestrzeni i inne)	
2.	Elementy strategii bezpieczeństwa cyberprzestrzeni na poziomie krajowym	**1.** Krajowa strategia bezpieczeństwa cyberprzestrzeni jako kluczowy element systemu ochrony w państwie **2.** Odniesienie do strategii UE **3.** Przykłady strategii istniejących w innych krajach (głównie UE) **4.** Omówienie pożądanych elementów, które powinny się znajdować w strategii **5.** Analiza (z udziałem słuchaczy) sposobu uwzględnienia kluczowych elementów strategii w istniejących, strategicznych dokumentach krajowych	6
3.	Podstawy analizy systemowej i inżynierii bezpieczeństwa systemów informacyjnych państwa	**1.** Podstawy badań systemowych. Geneza i rozwój modeli i metod systemowych na potrzeby bezpieczeństwa państwa **2.** Systemowe ujęcie struktur administracyjnych. **3.** Badania systemowe na potrzeby bezpieczeństwa narodowego i obronności. Technologie podwójnego zastosowania. **4.** Geneza i rozwój analizy systemowej na potrzeby zarządzania bezpieczeństwem państw. Doświadczenia RAND. **5.** Analiza systemowa na potrzeby inżynierii bezpieczeństwa systemów informacyjnych. **6.**Cyberprzestrzeń w ujęciu systemowym. **7.** Modelowanie systemowe. Modele systemów informacyjnych. Wartościowanie informacji w zarządzaniu cyberbezpieczeństwem.	10
4.	Zarządzanie bezpieczeństwem informacji w administracji państwowej i samorządowej	**1.** Podstawowe pojęcia bezpieczeństwa informacji (pojęcie informacji, rola i znaczenie informacji w organizacji, piramida informacji, kryteria klasyfikacji informacji, podstawowe atrybuty bezpieczeństwa informacji, polityka bezpieczeństwa informacji, model PDCA). **2.** Standardy i normy w bezpieczeństwie informacji. (pojęcie standardu, standardy mające charakter ustaw, standardy o charakterze norm krajowych i międzynarodowych, standardy o charakterze najlepszych praktyk stowarzyszeniowych. **3.** Identyfikowanie i wartościowanie aktywów organi-zacji (aktywa podstawowe, aktywa wspierające, wartościowanie aktywów, szacowanie skutków). **4.** Zapewnienie ochrony danych osobowych i informacji niejawnych (definicje i podstawowe pojęcia, zakres stosowania ustaw, przypadki szczególne, zadania obowiązki służb ds.	10

		bezpieczeństwa informacji, stosowanie ustawy w organizacji, zabezpieczenia, polityka ubezpieczeń-stwa danych osobowych i instrukcja przetwarzania, typowe problemy organizacji).	
5.	Zarządzanie ryzykiem zagrożeń bezpieczeństwa organizacji i instytucji	**1.** Koncepcja ryzyka i struktura zarządzania ryzykiem. Taksonomia ryzyka. **2.** Analiza pojęć podstawowych – zagrożenie, ryzyko, niepewność, bezpieczeństwo, zarządzanie ryzykiem. **3.** Niepewność i ryzyko. Rodzaje ryzyka. Metody identyfikacji ryzyka. **4.** Podstawy prawne analizy ryzyka w administracji publicznej **5.** Metodyka analizy ryzyka. **6.** Metody pomiaru ryzyka. 7.Analiza jakościowa i ilościowa ryzyka. **7.** Ocena ryzyka i reakcja na ryzyko. **8.** Wycena ryzyka. **9.** Monitorowanie, kontrola i dokumentowanie ryzyka. **10.** Zarządzanie ryzykiem informacyjnym. **11.** Dokumentowanie oraz monitorowanie ryzyka	18
6.	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	12

7.	Prognozowanie zagrożeń w systemie zarządzania cyberbezpieczeństwem organizacji i instytucji	**1.** Wprowadzenie do problematyki zagrożeń informacyjnych. teoretyczne problemy bezpieczeństwa cyberprzestrzeni. Klasyfikacja i ogólna charakterystyka zagrożeń bezpieczeństwa systemów. Przestępczość komputerowa **2.** Formy i charakterystyka zagrożeń z i dla cyberprzestrzeni. Skutki społeczne zagrożeń. Percepcja społeczna zagrożeń. Zagrożenia infrastruktury krytycznej państwa. **3.** Środki i metody ataków w cyberprzestrzeni. Bezpieczne zasady i metody wyszukiwania informacji w Internecie. 4.Metody analizy podatności na ataki obiektów i systemów infrastruktury krytycznej. Zagrożenia w przekazie medialnym. **4.** Identyfikacja zagrożeń informacyjnych bezpieczeństwa dla użytkownika organizacji i ich skutków. Aspekty technologiczne zjawiska cyberprzestępczości. **5.** Metody identyfikacji zagrożeń informacyjnych bezpieczeństwa krytycznej infrastruktury państwa i ich skutków **6.** Przestępczość zorganizowana w cyberprzestrzeni. Analiza przypadków, prognozowanie rozwoju zjawiska **7.** Zagrożenia bezpieczeństwa danych systemów operacyjnych - archiwizacja informacji. Podatność na ataki - protokół TCP/IP **8.** Przestępstwa komputerowe na świecie i w Polsce. Studia przypadków **9.** Analiza dostępnych narzędzi oraz list dyskusyjnych o tematyce hakerskiej. Zagrożenia dla zdalnego przetwarzania oraz przetwarzania w chmurze	12

8.	System zarządzania kryzysowego w warunkach zagrożeń cyberbezpieczeństwa państwa	**1.** Pojęcie i istota sytuacji kryzysowej i kryzysu. Treści zarządzania kryzysowego. Struktura zarządzania kryzysowego w Polsce **2.** Rola i zadania administracji publicznej w zarządzaniu kryzysowym **3.** Identyfikacja zagrożeń na podstawie wybranych przykładów cyberzagrożeń Planowanie działań zapobiegawczych i możliwości reagowania. **4.** Scenariusz rozwoju sytuacji kryzysowej **5.** Ochrona ludności w Polsce. Podstawy, zakres, organizacja. Charakterystyka podstawowych sposobów zbiorowej ochrony ludności w Polsce **6.** Charakterystyka wybranych systemów ratowniczych (System ratownictwa medycznego, SAR, KRSG) **7.** Zadania wybranych organów i instytucji w zakresie ochrony ludności **8.** Struktura, zadania i organizacja KSWSiA **9.** Zadania wybranych systemów ratowniczych na przykładzie wybranej sytuacji kryzysowej **10.** Organizacja zarządzania kryzysowego w gminie i powiecie **11.** Planowanie cywilne w gminie i powiecie **12.** Organizacja Zespołu Zarządzania Kryzysowego w Gminie i powiecie	10
9.	System cyberbezpieczeństwa UE i NATO	**1.** Teoretyczne problemy bezpieczeństwa cyberprzestrzeni. **2.** Charakterystyka zagrożeń i podatności systemów informacyjnych w UE. **3.** Analiza wybranych międzynarodowych incydentów w cyberprzestrzeni. **4.** Analiza przypadków zagrożeń bezpieczeństwa cyberprzestrzeni UE i NATO. **5.** Bezpieczeństwo cyberprzestrzeni w amerykańskich poglądach doktrynalnych. **6.** Ogólna charakterystyka amerykańskiego systemu bezpieczeństwa w cyberprzestrzeni. Charakterystyka założeń amerykańskiej strategii bezpieczeństwa cyberprzestrzeni. **7.** Bezpieczeństwo cyberprzestrzeni w amerykańskich poglądach doktrynalnych – studium przypadków. **8.** Bezpieczeństwo cyberprzestrzeni w poglądach doktrynalnych UE, NATO i wybranych państw. Założenia strategii bezpieczeństwa cyberprzestrzeni	10

		9. Bezpieczeństwo cyberprzestrzeni w ujęciu Unii Europejskiej. **10.** Bezpieczeństwo cyberprzestrzeni w koncepcjach strategicznych NATO. Modele cyberobrony.	
10.	Systemy informacyjne w zarządzaniu kryzysowym	**1.** Wprowadzenie do zarządzania kryzysowego – podstawowe pojęcia i definicje. Informacja, systemy informacyjne zarządzania kryzysowego. Podstawowe funkcje systemów informacyjnych zarządzania kryzysowego, systemy informacji przestrzennej. **2.** Modelowanie obiektów operacyjnych Policji i PSP w systemach zarządzania kryzysowego. Graficzne zobrazowanie zdarzeń kryzysowych. **3.** Opracowanie warstw informacyjnych własnego projektu w systemie informacji przestrzennej. Lokalizacja obiektów w systemach informacyjnych zarządzania kryzysowego. **4.** Określenie obszaru przestrzennego własnego projektu i podstawowe analizy w systemie informacji przestrzennej. **5.** Modelowanie obiektów militarnych w systemach zarządzania kryzysowego. Zobrazowywanie informacji w systemie informacji przestrzennej. **6.** Wykorzystanie systemu JTLS do ćwiczeń zarządzania kryzysowego. Bazy danych wykorzystywane w systemach zarządzania kryzysowego Analiza danych przestrzennych w systemach zarządzania kryzysowego. **7.** Przygotowanie baz danych systemu JTLS dla zdefiniowanego scenariusza. **8.** Dane rastrowe w wybranym systemie informacji przestrzennej. **9.** Systemy symulacji w zarządzaniu kryzysowym. **10.** Wykorzystanie JTLS dla potrzeb ćwiczenia zarządzania kryzysowego. Numeryczny model terenu w systemie informacji przestrzennej. Prowadzenie symulacji działań w systemie JTLS według przygotowanego scenariusza. **11.** Zdjęcia lotnicze i satelitarne w systemie informacji przestrzennej. **12.** Zasady Opracowania dokumentacji własnego projektu na potrzeby zarządzania kryzysowego.	10
11.	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	22

		na poziomie własnej sieci **4.** Współdziałanie technologii bezpieczeństwa w praktyce – analiza przebiegu cyberataku na podstawie strumienia danych oraz zapisów pracy systemów bezpieczeństwa	
12.	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
13.	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
15	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	10
16	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
17	Usługi elektronicznej identyfikacji i usługi	**1.** Zagadnienie elektronicznej identyfikacji	4

	zaufania	**2.** Usługi zaufania **3.** Rozporządzenie eIDAS **4.** Polskie regulacje dotyczące eIDAS	
18	Egzamin końcowy		10
	suma		**180**

Kadra.

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

- *Piotr Sienkiewicz*-prof. dr hab. inż. Absolwent Wydziału Cybernetyki Wojskowej Akademii Technicznej. Doktor nauk technicznych(WAT 1975), dr habil. nauk wojskowych(1980), profesor nadzwyczajny(1986). Pracownik Wojskowego Instytutu Łączności, Akademii Sztabu Generalnego WP, Akademii Obrony Narodowej(od 1990 r. na stanowisku szefa Centrum Informatyki, prorektora ds. dydaktycznych, dyrektora Instytutu Inżynierii Systemów Bezpieczeństwa). W latach 1997-1999 wicedyrektor Departamentu Kadr i Szkolnictwa Wojskowego MON, w latach 2005-2012 prorektor Warszawskiej Wyższej Szkoły Informatyki. Wykładowca wielu uczelni(m.in. UJ, USz), promotor 50 rozpraw doktorskich(oraz honorowego doktoratu prof. Z. Brzezińskiego). Autor ponad 400 artykułów, rozpraw, referatów itp., kierownik kilkunastu projektów badawczych, autor 13 książek(m.in. „Inżynieria systemów", „Inżynieria systemów kierowania", „Teoria efektywności systemów", „Analiza systemowa", „Inżynieria systemów bezpieczeństwa"). Powoływany jako ekspert KBN i NCBiR. Prezes Polskiego Towarzystwa Cybernetycznego, wiceprezes Polskiego Towarzystwa Badań Operacyjnych i Systemowych, członek Polskiego Oddziału Klubu Rzymskiego, Polskiego Towarzystwa Ekonomicznego. Uczestnik prac m.in. Komitetu Prognoz PAN, Rady Szkolnictwa Wyższego i Nauki oraz kilkudziesięciu rad i komitetów naukowych krajowych i międzynarodowych konferencji. Obecnie dyrektor Instytutu Inżynierii Systemów Bezpieczeństwa w Wydziale Bezpieczeństwa Narodowego AON.

- *Wiesław Błażejczyk*-posiada stopień naukowy doktora nauk wojskowych w specjalności „Zarządzanie systemami informacyjnymi". Adiunkt w Instytucie Inżynierii Systemów Bezpieczeństwa Akademii Obrony Narodowej. W ramach pracy dydaktycznej prowadzi następujące zajęcia: Badania operacyjne, Techniki i metody ilościowe w zarządzaniu, Bezpieczeństwo informacyjne, Nauki o informacji, Zarządzanie zasobami informacyjnymi, Prognozowanie i symulacje, Geopolityka, Ochrona osób, mienia i infrastruktury, Statystyka, Analiza systemowa, Analiza ryzyka.

- *Edyta Szczepaniuk*-posiada stopień naukowy doktora w dziedzinie nauk społecznych w dyscyplinie nauki o bezpieczeństwie. Obecnie pracuje na stanowisku adiunkta w Akademii Obrony Narodowej. Posiada obszerną wiedzę z zakresu teorii bezpieczeństwa, analizy systemowej, inżynierii

systemów bezpieczeństwa, bezpieczeństwa cyberprzestrzeni, nowoczesnych technologii, problemów bezpieczeństwa informacyjnego, elektronicznej administracji.

- *Halina Świeboda*-pracownik naukowo-dydaktyczny AON, aktualnie adiunkt-kierownik Zakładu Zarządzania Ryzykiem w Instytucie Inżynierii Systemów Bezpieczeństwa WBN, mgr ekonomii w zakresie gospodarowania zasobami pracy i kapitału, dr nauk wojskowych w specjalności bezpieczeństwo informacyjne (narodowe).Dodatkowe kwalifikacje i kompetencje to Certyfikat zarządzania projektami, PRINCE2® Foundation, Kurs ADL, Certyfikowany audytor wewnętrzny zarządzania bezpieczeństwem informacji wg. Normy ISO 27001:2005 DNV Business Assurance, Risk Based Certification, Zastosowania sztucznej inteligencji – pakiet SPHINX AITECH Artificial Intelligence Laboratory Katowice. Aktywnie uczestniczy w wielu konferencjach naukowych międzynarodowych i krajowych między innymi uczestniczka Międzynarodowych Konferencji Naukowych, Badania i Operacyjne i Systemowe BOS, organizatorka konferencji „Metodologia badań bezpieczeństwa narodowego - „Bezpieczeństwo 2010, 2011, 2012" oraz sympozjów naukowych z okazji światowego Dania Społeczeństwa Informacyjnego. Jest aktywnym członkiem Polskiego Towarzystwa Ekonomicznego i Polskiego Towarzystwa Współpracy z Klubem Rzymskim, a ponad to jest członkiem Polskiego Towarzystwa Badań Operacyjnych i Systemowych.

- *Marian Urbanek*-pracownik naukowo-dydaktyczny AON, posiada stopień naukowy doktora, były z-ca Dyrektora Centrum Symulacji i Komputerowych Gier Wojennych.

- *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.

- *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.

- *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.

- *Krzysztof Silicki*- mgr inż. Absolwent Politechniki Warszawskiej. Od roku 1992 związany z NASK. Doradca Dyrektora NASK, Dyrektor ds. Współpracy z ENISA (Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji).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.

- *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).

*zastrzega się możliwość zaangażowania wykładowców o równoważnych kompetencjach.

Adresaci studiów i sylwetka absolwenta.

Adresatami studiów są pracownicy administracji publicznej 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 Administracji* 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 organizacji
- 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.

W związku z realizacją części zajęć w trybie zdalnym od uczestników wymagane jest posiadanie własnego komputera, który spełnia minimalne wymagania :

- 2 GB RAM, CPU P4 1,6 GHz, grafika 128 MB HDTV [1366 x 768 True Color (32Bit) Color].
- System operacyjny Microsoft Windows 7 lub nowszy.
- Działający mikrofon i słuchawki (lub głośniki).
- Opcjonalnie kamerka.
- Karta sieciowa lub sieć Wi-Fi z dostępem do Internetu (opcjonalnie modem UMTS).

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.