Program
studiów podyplomowych
„Cyberbezpieczeństwo przemysłowe”

Bydgoszcz 2023r.

Spis treści

Rozdział 1. Charakterystyka ramowego programu studiów

1.1. Ramowy opis

Cyberprzestrzeń stanowi równorzędne pole działania państw, korporacji i innych organizacji w XXI w. w stosunku do tradycyjnych obszarów działania i aktywności politycznej, strategicznej i gospodarczej Społeczeństwo informacyjne postawiło umiejętności pozyskania, gromadzenia, sortowania, analizy, wizualizacji, udostępniania i niszczenia informacji na równi z innymi sposobami oddziaływania na otoczenie, w tym rynek produktów i usług. Wyodrębnianie wiedzy z danych, wykorzystywanie zasobów cyfrowego otoczenia dla realizacji celów strategicznych czy gospodarczych, realizowanie efektywnej strategii komunikacyjnej w cyfrowym otoczeniu informacyjnym to ważne obszary wsparcia – ale też potencjalnych zagrożeń. Dane niosą ze sobą potencjalną wartość, a zatem ich nieuprawnione skopiowanie przez konkurencję czy ujawnienie publiczne stanowi uszczerbek na opinii (wartości marki) czy wręcz utratę zysku (np. ujawnienie *know-how*). Jesteśmy również świadkami bezprecedensowej wojny informacyjnej podejmowanej w domenie cyfrowej, stanowiącej kolejny obszar działań zbrojnych. Zapewnienie organizacjom i osobom fizycznym stabilnej przyszłości dotyczy zatem również domeny informacyjnej. Zapewnienie bezpieczeństwa informacji oznacza bowiem często również zapewnienie ciągłości świadczenia usług kluczowych dla gospodarki i bezpieczeństwa publicznego. Temu celowi służy cyberbezpieczeństwo – definiowane zgodnie z Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa jako „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy". Wszechobecność ww. systemów informacyjnych powoduje, że cyberbezpieczeństwo należy zatem realizować na wszystkich poziomach, zarówno w organizacjach, jak i mając na względzie bezpieczeństwo osób fizycznych. Celowe i skuteczne staje się zatem pozyskanie wiedzy i praktyki, w jaki sposób planować i realizować polityki i strategie w cyberprzestrzeni, jak identyfikować zagrożenia i jak im przeciwdziałać, jak tym samym zapewnić bezpieczne funkcjonowanie organizacji (w tym przedsiębiorstw) w cyfrowym otoczeniu. Służą temu proponowane studia podyplomowe „Cyberbezpieczeństwo przemysłowe", mające pomóc specjalistom w sprostaniu jednemu z największych wyzwań bieżących czasów.

Perspektywy rozwojowe studiów podyplomowych „Cyberbezpieczeństwo przemysłowe" są bardzo duże: wg raportu Accenture w 2020 roku aż 87% organizacji zostało narażonych na próby cyberataku, a liczba cyberataków w 2021 r. wzrosła o 31 proc. w stosunku do 2020r. Szacuje się, że w branży cyberbezpieczeństwa (w tym cyberbezpieczeństwa przemysłowego) globalnie brakuje kilku milionów specjalistów, a jedynie ok. 25% z nich ma wystarczające kwalifikacje. Należy również zaznaczyć, że era gospodarki cyfrowej dopiero się zaczyna, a zagrożenia będą rosły z czasem (por. odejście od gotówki w stronę „cyfrowego pieniądza" czy przejście na naukę i pracę zdalną).

1.2. Cele studiów

- Zdobycie przez absolwentów bardziej konkretnych umiejętności praktycznych i specjalistycznej wiedzy z cyberbezpieczeństwa oraz jego zastosowań w przemyśle w porównaniu z programem z tego zakresu na studiach licencjackich czy magisterskich, a tym samym lepsze przygotowanie i silniejszą pozycję na rynku pracy.
- Przygotowanie kandydatów do pełnienia funkcji specjalisty odpowiedzialnego za cyberbezpieczeństwo w podmiotach gospodarczych (w tym w przemyśle), jednostkach

samorządu terytorialnego, instytucjach rządowych i finansowych, organizacjach, fundacjach i stowarzyszeniach należących do wszystkich sektorów gospodarki i życia społecznego.
- Wypełnienie luki w przygotowaniu kandydatów na ww. stanowiska.
- Umożliwienie podwyższenia kwalifikacji w obszarze cyberbezpieczeństwa przemysłowego wszystkim absolwentom kierunków technicznych zainteresowanych tym tematem.

1.3. Adresaci studiów

- pracownicy sektora prywatnego, zwłaszcza działów odpowiedzialnych za bezpieczeństwo teleinformatyczne,
- pracownicy jednostek administracji publicznej, zwłaszcza działów odpowiedzialnych za bezpieczeństwo teleinformatyczne,
- analitycy zagrożeń dla bezpieczeństwa organizacji i gromadzonych przez nich danych.

Wymagania rekrutacyjne: ukończone studia I stopnia (licencjat lub inżynierskie).

Rozdział 2. Profil kompetencyjny absolwenta studiów (sylwetka absolwenta)

2.1. Rola i zadania specjalistów w zakresie cyberbezpieczeństwa przemysłowego

Główną rolą specjalistów w zakresie cyberbezpieczeństwa przemysłowego jest zapobieganie naruszeniom w obszarze cyberbezpieczeństwa, gdyż koszty (finansowe, wizerunkowe) naruszeń mogą być bardzo wysokie, a szkody (np. ujawnienie danych klientów) niemożliwe do naprawienia. W sytuacji bezpośredniego zagrożenia rolą specjalisty do spraw cyberbezpieczeństwa jest szybkie reagowania na zagrożenie zgodnie z wcześniej założonymi scenariuszami działania, tak aby zapobiec naruszeniom lub zminimalizować ich skutki.

Główne zadania specjalisty do spraw cyberbezpieczeństwa przemysłowego, w zależności od poziomu w organizacji, na jakim działa, obejmują:

- regularny audyt danych i procedur dostępu do nich (w tym kopii zapasowych) oraz audyt bezpieczeństwa systemów informacyjnych,
- tworzenie polityk bezpieczeństwa, które zapewnią poufność, integralność, dostępność i autentyczność informacji, ale również np. polityki bezpieczeństwa w relacjach z dostawcami i usługodawcami,
- analiza i ocena ryzyka wystąpienia ataku hakerskiego czy wycieku danych,
- wdrożenie środków technicznych i organizacyjnych, takich jak bieżące aktualizowanie oprogramowania, inwentaryzacja urządzeń czy wymuszanie na użytkownikach stosowania odpowiednio odpornych loginów, haseł i innych zabezpieczeń (np. polityki pustego biurka).
- okresowe kontrole i raporty oraz monitorowanie ich realizacji,
- tworzenie procedur na wypadek ewentualnych ataków,
- edukacja osób zatrudnionych w danej organizacji,
- ochrona danych przed wyciekiem (szczególnie danych wrażliwych objętych RODO),
- odpowiednia konfiguracja sieci i urządzeń,
- wdrożenie polityki postępowania z nośnikami danych i urządzeniami, w tym prywatnymi,
- współpraca z programistami podczas tworzenia i modernizacji systemów i aplikacji,
- rozpoznawanie incydentów i niezwłoczne reagowanie na nie,
- w części przypadków: testowanie szczelności zabezpieczeń i poszukiwanie luk,
- aktualizacja wiedzy i utrzymywanie kontaktów w ramach krajowego systemu cyberbezpieczeństwa.

Kluczowe kompetencje w pracy specjalisty do spraw cyberbezpieczeństwa przemysłowego to:

- wiedza,
- doświadczenie,
- umiejętności techniczne i kompetencje miękkie (współpracy z zarządem organizacji i działem IT, szkolenia użytkowników i administratorów systemów teleinformatycznych),
- umiejętność analizy i przewidywania,
- opanowanie,
- umiejętność szybkiego reagowania na zagrożenia,
- odpowiedzialność,

- umiejętność koncentracji na zadaniu,
- solidność i uczciwość.

Rozdział 3. Ramowe efekty uczenia się

Wiedza (W):

EK_W01: Posiada pogłębioną znajomość zagrożeń występujące w sieciach teleinformatycznych, ma wiedzę o metodach testowania, monitorowania sieci i reagowania na zagrożenia bezpieczeństwa cybernetycznego, w tym w ramach złożonych zadań w zmiennych i nie w pełni przewidywalnych warunkach.

EK_W02: Posiada zaawansowaną znajomość cyklu rozwoju oraz współczesne metodyki rozwoju oprogramowania, a także trendy w programowaniu, w tym wybrane algorytmy sztucznej inteligencji, blockchain, komputerach kwantowych w cyberbezpieczeństwie.

EK_W03: Ma pogłębioną wiedzę o trendach rozwojowych i najistotniejszych nowych osiągnięciach w obszarze cyberbezpieczeństwa, w tym w ramach złożonych zadań w zmiennych i nie w pełni przewidywalnych warunkach cyberprzestrzeni.

Umiejętności (U):

EK_U01: Potrafi w sposób zaawansowany tworzyć, analizować i testować oprogramowanie pod kątem bezpieczeństwa, potrafi stosować wybrane algorytmy sztucznej inteligencji.

EK_U02: Potrafi w sposób zaawansowany skonfigurować i uruchomić narzędzia do monitorowania i testowania ruchu sieciowego oraz identyfikować normalny i nietypowy ruch lub oznaki włamania. Potrafi przeprowadzić testy i audyt bezpieczeństwa sieci.

EK_U03: Potrafi opracować i prowadzić dokumentację związaną z cyberbezpieczeństwem, w tym w przemyśle.

Kompetencje społeczne (K):

EK_K01: Potrafi w sposób pogłębiony krytycznie oceniać odbierane treści, uznawać znaczenie wiedzy w rozwiązywaniu problemów poznawczych i praktycznych. Potrafi odpowiednio określić priorytety służące realizacji określonego zadania w obszarze cyberbezpieczeństwa, w tym w ramach złożonych zadań w zmiennych i nie w pełni przewidywalnych warunkach cyberprzestrzeni.

EK_K02: Rozumie potrzebę przekazywania społeczeństwu informacji i opinii dotyczących osiągnięć techniki i innych aspektów działalności gospodarczej i społecznej. W sposób pogłębiony rozumie rolę środków masowego przekazu oraz szkodliwość dezinformacji.

Rozdział 4. Program studiów

4.1. Ramowy program kształcenia

Liczba semestrów: 2

Liczba miesięcy nauki: 12

Liczba zjazdów: 10

Liczba godzin: 190

Forma zaliczenia: Projekt końcowy.

4.2. Program studiów z siatką godzinową i punktami ECTS

Lp.	Przedmiot	Liczba godzin	ECTS
1.	Społeczeństwo informacyjne i Społeczeństwo sieciowe (wykład)	6	1
2.	Teoria bezpieczeństwa w ujęciu systemowym (wykład)	6	1
3.	Konflikty hybrydowe i zagrożenia asymetryczne (wykład)	6	1
4.	Budowa i zarządzanie zespołem ds. cyberbezpieczeństwa (wykład)	6	1
5.	Bezpieczeństwo urządzeń i systemów Przemysłu 4.0 (wykład)	10	1
6.	Sztuczna inteligencja w cyberbezpieczeństwie (wykład)	6	1
7.	Internet, Big Data i small data sets jako źródło informacji (wykład)	6	1
8.	Strategia cyberbezpieczeństwa Polski w domenie cyfrowej (wykład)	10	2
9.	Zarządzanie ryzykiem w obszarze cyberbezpieczeństwa i bezpieczeństwa informacyjnego (wykład)	6	1
10.	Bezpieczeństwo w Internecie Rzeczy (w tym blockchain i Pegasus) (wykład)	6	1
11.	Zagrożenia w obszarze cyberbezpieczeństwa (wykład)	10	2
12.	Cyberataki i przeciwdziałanie im (wykład)	10	2
13.	Komputery kwantowe - szanse i zagrożenia (wykład)	6	1
14.	Ochrona własności intelektualnej, danych osobowych i informacji niejawnych (w tym dokumentacja Inspektora Ochrony Danych) (laboratorium)	10	2

15.	Dokumentacja cyberbezpieczeństwa	6	1
16.	Audyt danych i audyt systemów informatycznych (laboratorium)	8	1
17.	Bezpieczeństwo serwerów	6	1
18.	Programowanie rozwiązań bezpieczeństwa systemów komputerowych (PHP, C#, Java, Python) (laboratorium)	14	2
19.	Bezpieczeństwo systemów internetowych (laboratorium)	8	1
20.	Bezpieczeństwo systemów mobilnych	8	1
21.	Przygotowanie administratora i szkolenie użytkowników (laboratorium)	10	2
22.	Bezpieczeństwo sieci komputerowych (laboratorium)	10	1
23.	Analityka danych internetowych (laboratorium)	6	1
24.	Projekt końcowy (laboratorium)	10	2
		Razem	31

4.3. Podział modułowy programu studiów

Podział modułowy programu studiów obejmuje:

- 40 godzin zagadnień teoretycznych (wykładów: 6 przedmiotów) prowadzonych w 1 grupie 30-osobowej,
- 54 godziny zagadnień metodycznych (seminaria, konwersatoria i ćwiczenia: 7 przedmiotów) prowadzonych w 1 grupie 30-osobowej,
- 96 godzin zagadnień praktycznych (laboratoria: 11 przedmiotów) prowadzonych w 2 grupach 15-osobowych (ze względu na liczbę miejsc w laboratorium).

Moduł I. Zagadnienia teoretyczne

Lp.	Przedmiot	Liczba godzin
1.	Społeczeństwo informacyjne i Społeczeństwo sieciowe (wykład)	6
2.	Teoria bezpieczeństwa w ujęciu systemowym (wykład)	6
3.	Konflikty hybrydowe i zagrożenia asymetryczne (wykład)	6
4.	Budowa i zarządzanie zespołem ds. cyberbezpieczeństwa (wykład)	6
5.	Bezpieczeństwo urządzeń i systemów Przemysłu 4.0 (wykład)	10
6.	Sztuczna inteligencja w cyberbezpieczeństwie (wykład)	6

Moduł II. Zagadnienia metodyczne

Lp.	Przedmiot	Liczba godzin

1.	Internet, Big Data i small data sets jako źródło informacji (ćwiczenia)	6
2.	Strategia cyberbezpieczeństwa Polski w domenie cyfrowej (konwersatorium)	10
3.	Zarządzanie ryzykiem w obszarze cyberbezpieczeństwa i bezpieczeństwa informacyjnego (ćwiczenia)	6
4.	Bezpieczeństwo w Internecie Rzeczy (w tym blockchain i Pegasus) (konwersatorium)	6
5.	Zagrożenia w obszarze cyberbezpieczeństwa (konwersatorium)	10
6.	Cyberataki i przeciwdziałanie im (konwersatorium)	10
7.	Komputery kwantowe - szanse i zagrożenia (konwersatorium)	6

Moduł III. Zagadnienia praktyczne

Lp.	Przedmiot	Liczba godzin
1.	Ochrona własności intelektualnej, danych osobowych i informacji niejawnych (w tym dokumentacja Inspektora Ochrony Danych) (laboratorium)	10
2.	Dokumentacja cyberbezpieczeństwa (laboratorium)_	6
3.	Audyt danych i audyt systemów informatycznych (laboratorium)	8
4.	Bezpieczeństwo serwerów (laboratorium)	6
5.	Programowanie rozwiązań bezpieczeństwa systemów komputerowych (PHP, C#, Java, Python) (laboratorium)	14
6.	Bezpieczeństwo systemów internetowych (laboratorium)	8
7.	Bezpieczeństwo systemów mobilnych (laboratorium)	8
8.	Przygotowanie administratora i szkolenie użytkowników (laboratorium)	10
9.	Bezpieczeństwo sieci komputerowych (laboratorium)	10
10.	Analityka danych internetowych (laboratorium)	6
11.	Projekt końcowy (laboratorium)	10