SZKOŁA GŁÓWNA SŁUŻBY POŻARNICZEJ
Wydział Inżynierii Bezpieczeństwa Cywilnego

ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA INFRASTRUKTURY KRYTYCZNEJ

Program studiów podyplomowych

Rafał Wróbel
Paweł Gromek

ZATWIERDZAM

Warszawa, ……

…….

Warszawa 2016

Spis treści

I. ZAŁOŻENIA DYDAKTYCZNO – WYCHOWAWCZE

1. Cel studiów

Celem studiów jest przygotowanie profesjonalnie wyszkolonej kadry administracji publicznej, przedstawicieli sektora prywatnego oraz wszelkich stron zainteresowanych problematyką zarządzania ciągłością działania infrastruktury krytycznej do efektywnej pracy zawodowej w zakresie ochrony infrastruktury krytycznej.

2. Warunki przyjęcia na studia

a. Studia podyplomowe mogą realizować wszystkie osoby zainteresowane problematyką zarządzania ciągłością działania infrastruktury krytycznej, które:
   - posiadają wykształcenie wyższe (minimum ukończone studia I stopnia),
   - uzyskały pozytywną opinię dotyczącą zakwalifikowania na studia podyplomowe uczelnianej komisji rekrutacyjnej,
   - uiściły w terminie wskazanym przez organizatora studiów opłatę za studia.

b. W przypadku dużej liczby osób zainteresowanych o przyjęciu na studia decyduje kolejność zgłoszenia. Kandydatom, którzy nie zostali zakwalifikowani na studia podyplomowe w danej edycji, przysługuje pierwszeństwo w procesie kwalifikacji w edycji następnej.

c. Kandydaci na studia mają obowiązek złożyć:
   - formularz zgłoszeniowy, zawierający fotografię,
   - odpis lub poświadczoną kserokopię dyplomu ukończenia studiów wyższych,
   - deklarację płatności,

d. Przyjęcie na studia odbywa się po spełnieniu przez kandydata wszystkich warunków określonych w pkt a-c oraz:
   - zawarciu umowy o warunkach płatności za studia,
   - złożeniu przez kandydata wniesienia opłaty za pierwszy semestr studiów bądź całość studiów (z zastrzeżeniem postanowień zawartych w pkt I.9 Regulaminu studiów podyplomowych w SGSP w Warszawie.

3. Sylwetka absolwenta

Po ukończeniu studiów słuchacz powinien:

a. w sferze poznawczej:
   - znać zagadnienia organizacyjno – prawne ochrony infrastruktury krytycznej i zarządzania ciągłością działania,
   - rozumieć terminy infrastruktura krytyczna i zarządzanie ciągłością działania, a także terminy pokrewne,
   - wymienić systemy infrastruktury krytycznej,
   - dokonać identyfikacji zagrożeń infrastruktury krytycznej
   - definiować współzależność infrastruktur krytycznych względem siebie,
   - omówić formy ochrony infrastruktury krytycznej,
   - znać elementy składowe Narodowego Programu Ochrony Infrastruktury Krytycznej,
   - wskazać sposób tworzenia, aktualizacji i strukturę planów ochrony infrastruktury krytycznej, a także dokumentacji związanej z zarządzaniem ciągłością działania,
   - przedstawić obowiązki i zasady współpracy w zakresie Narodowego Programu Ochrony Infrastruktury Krytycznej organów administracji publicznej i służb odpowiedzialnych za bezpieczeństwo narodowe,
   - wykazać się znajomością rynku zabezpieczeń infrastruktury krytycznej,
   - definiować działania na rzecz ochrony infrastruktury krytycznej, w tym działania wpisujące się w zarządzanie ciągłością działania,
   - znać ścieżki rozchodzenia się zagrożenia wewnątrz systemu oraz między systemami infrastruktury krytycznej,
   - wskazać systemy infrastruktury krytycznej szczególnie istotne dla funkcjonowania państwa, jego gospodarki oraz administracji publicznej,
   - dokonać alokacji systemu infrastruktury krytycznej w systemie bezpieczeństwa państwa,
b. w sferze praktycznej:
   - umieć wyznaczać obiekty infrastruktury krytycznej,
   - dokonać analizy zagrożeń i analizy ryzyka na potrzeby ochrony infrastruktury krytycznej,
   - stosować formy ochrony infrastruktury krytycznej,
   - określać zasady rozprzestrzeniania się zagrożeń wewnątrz wybranego systemu oraz między systemami,

- projektować rozwiązania na rzecz poprawy ochrony infrastruktury krytycznej,
- dokonać pomiaru efektów ochrony infrastruktury krytycznej,

c. w sferze motywacyjnej, mieć ukształtowane postawy:
   - odpowiedzialności za bezpieczeństwo państwa, jego obywateli, gospodarki oraz funkcjonowania administracji oraz przedsiębiorców,
   - otwartości w stosunku do rozwijających się obszarów wiedzy,
   - zdolności do rozwijania zagadnień na poziomie strategicznym i operacyjnym.

Absolwenci studiów podyplomowych przeznaczeni są do sprawowania funkcji doradczych i administracyjnych w instytucjach zajmujących się szeroko rozumianą ochroną infrastruktury krytycznej, a także stosujących lub zamierzających stosować dobre praktyki z zakresu zarządzania ciągłością działania. Ich głównym zadaniem jest prowadzenie zakrojonych na szeroką skalę działań w zakresie:

a. gromadzenia i przetwarzania informacji dotyczących zagrożeń infrastruktury krytycznej,
b. opracowywania i wdrażania procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej,
c. odtwarzania infrastruktury krytycznej,
d. współpracy publiczno-prywatnej na rzecz ochrony infrastruktury krytycznej,
e. innych działań wpisujących się w tematykę zarządzania ciągłością działania infrastruktury krytycznej.

Nabyte w trakcie trwania studiów wiadomości i umiejętności pozwolą na aktywny udział w partnerstwie publiczno- prywatnym, wypracowanie metodologii ułatwiającej ocenę ryzyka i ustalenie współzależności między systemami infrastruktury krytycznej. Równocześnie absolwenci posiądą wiedzę w zakresie;

a. dostępnych i prognozowanych form ochrony infrastruktury krytycznej,
b. sposobów pomiaru efektów ochrony infrastruktury krytycznej,
c. zasad funkcjonowania rynku zabezpieczeń ochrony infrastruktury krytycznej.

Absolwenci studiów podyplomowych nabywają umiejętności właściwe kandydatom na pełnomocników ds. ochrony infrastruktury krytycznej, osobom odpowiedzialnym za utrzymanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej, a także audytorów wewnętrznych systemów zarządzania ciągłością działania.

II. REALIZACJA PROCESU DYDAKTYCZNEGO

1. Organizacja studiów

a. Studia są prowadzone w trybie niestacjonarnym.
b. Organizatorem studiów podyplomowych jest Wydział Inżynierii Bezpieczeństwa Cywilnego Szkoły Głównej Służby Pożarniczej w Warszawie.
c. Organizator ustala formę i częstotliwość zjazdów, co podaje słuchaczom do wiadomości najpóźniej w trakcie pierwszego zjazdu.
d. Zajęcia dydaktyczne mogą być prowadzone przez:
   – nauczycieli akademickich Szkoły Głównej Służby Pożarniczej, w tym przede wszystkim, nauczycieli realizujących na co dzień zagadnienia z zakresu infrastruktury krytycznej, jej ochrony, oceny i analizy ryzyka, a także zarządzania ciągłością działania,
   – innych specjalistów z przygotowaniem kierunkowym, zwłaszcza pracowników Rządowego Centrum Bezpieczeństwa, przedsiębiorstw specjalizujących się w problematyce zarządzania ciągłością działania oraz innych ośrodków naukowych.
e. Plan nauczania stanowi podstawę procesu nauczania dydaktycznego.
f. Lekcja stanowi podstawową formę nauczania, a jej odpowiednikiem jest jedna godzina dydaktyczna trwająca 45 minut. Łączenie dwóch jednostek lekcyjnych jest dopuszczalne.
g. Studia podyplomowe będą realizowane poprzez zajęcia teoretyczne oraz ćwiczenia i ćwiczeń laboratoryjnych w uczelni. Dopuszcza się możliwość przeprowadzania zajęć poza uczelnią w przypadku możliwości zwiększenia tym samym efektu dydaktycznego.
h. Studia podyplomowe uznaje się za ukończone wówczas, gdy słuchacz uzyskał pozytywną ocenę z egzaminu końcowego oraz złożył pozytywnie ocenioną pracę końcową.
i. Warunkiem dopuszczenia do egzaminu końcowego jest uzyskanie wszystkich zaliczeń i egzaminów ujętych w programie studiów, złożenie pracy końcowej i jej pozytywna weryfikacja w systemie antyplagiatowym (SAP).
j. Aktywności dotyczące przygotowania pracy końcowej (1), egzaminu końcowego, w tym sposób ustalania oceny końcowej z przebiegu studiów (2)

oraz wydawania i świadectwa studiów (3) są realizowane zgodnie z regulaminem studiów podyplomowych w SGSP w Warszawie.

k. Na realizację programu studiów przewidziano:
   - rozpoczęcie studiów
   - zajęcia dydaktyczne prowadzone w formie zjazdów,
   - egzamin
   - zakończenie studiów

l. Dokumentacja przebiegu nauczania prowadzona jest przez Szkołę Główną Służby Pożarniczej.

2. Warunki metodyczne

a. Przy ustalaniu rozkładu zajęć dydaktycznych uwzględniono zasady:
   - różnicowania zajęć w każdym dniu szklenia,
   - unikania planowania kilkugodzinnych zajęć z rzędu z tego samego zagadnienia,
   - równomiernego, w miarę możliwości, obciążenia zajęciami dydaktycznymi w poszczególnych dniach tygodnia,
   - synergicznego łączenia ze sobą poszczególnych treści kształcenia.

b. Dobór metod i technik kształcenia jest uwarunkowany celami kształcenia, materiałem nauczania, a także szczegółowymi zadaniami dydaktycznymi.

c. Zajęcia teoretyczne mogą być prowadzone równocześnie dla całej grupy słuchaczy studiów podyplomowych.

d. W ramach godziny przewidzianej na rozpoczęcie studiów podyplomowych organizator jest zobowiązany zapewnić przekazanie słuchaczom informacji nt.:
   - zasad realizacji programu,
   - programu studiów podyplomowych z uwzględnieniem przyjętej formy i częstotliwości zjazdów,
   - zalecanej literatury polskiej i zagranicznej,
   - warunków przystąpienia do testu końcowego, w tym przygotowania i złożenia pracy końcowej,
   - warunków ukończenia studiów podyplomowych,.

e. W ramach realizacji poszczególnych zakresów tematycznych prowadzący zajęcia określą i wskażą słuchaczom zakres materiału do opanowania w procesie samokształcenia.
f. Prowadzący zajęcia mogą dostarczyć słuchaczom materiały dydaktyczne w formie papierowej lub elektronicznej.

3. Zasady dotyczące oceniania efektów oraz zaliczenia studiów

a. Ocena efektów edukacyjnych słuchaczy będzie prowadzona w sposób systematyczny przez prowadzących zajęcia poprzez:
   - pytania ustne,
   - zadania problemowe,
   - zadania utrwalające i sprawdzające wiedzę.
b. Słuchacze na bieżąco są informowano o uzyskiwanych efektach cząstkowych.
c. Warunkiem ukończenia studiów jest:
   - uczestnictwo w co najmniej 70 % zajęć dydaktycznych przewidzianych w planie nauczania (nieobecność na zajęciach w wymiarze większym niż 30% liczby godzin przewidzianych w programie studiów skutkuje skreśleniem z listy słuchaczy),
   - złożenie pozytywnie ocenionej pracy końcowej,
   - uzyskanie pozytywnej oceny z egzaminu końcowego.
d. Przystąpienie do egzaminu końcowego możliwe jest jedynie po uprzednim uzyskaniu zaliczenia ze wszystkich zakresów tematycznych przewidzianych w planie studiów, a także złożeniu pozytywnie ocenionej pracy końcowej.
e. Praca końcowa może być prowadzona przez promotora wyznaczonego przez organizatora z grona osób prowadzących zajęcia dydaktyczne w ramach przedmiotowych studiów. Organizator przedstawi na spotkaniu organizacyjnym wykaz promotorów prac końcowych.
f. Słuchaczowi przysługuje dowolność wyboru promotora pracy końcowej, przy równoczesnym respektowaniu limitu 5 prac przypadających na jednego promotora. W uzasadnionych przypadkach organizator może wyrazić zgodę na doraźną zmianę limitu prac.
g. Ocenę końcową ze studiów nalicza się zgodnie z regulaminem studiów podyplomowych realizowanych w SGSP.

h. Słuchacz, który nie został dopuszczony do egzaminu końcowego ze względu na brak wymaganych zaliczeń lub nie przystąpił do niego z innych przyczyn, może przystąpić do egzaminu w dodatkowym terminie po uzyskaniu zgody organizatora. Decyzję w tej sprawie podejmuje dziekan wydziału za pośrednictwem kierownika studiów podyplomowych.
i. Słuchaczowi, który nie zdał egzaminu końcowego przysługuje jeden egzamin poprawkowy w terminie ustalonym przez dziekana. Egzamin dodatkowy jest płatny i ostateczny.
j. W przypadku, gdy słuchacz z przyczyn losowych nie mógł stawić się na egzaminie końcowym, ma on prawo ubiegać się o termin dodatkowy. Decyzje w tej sprawię podejmuje dziekan.
k. W sprawach nierozstrzygniętych decyduje dziekan właściwego wydziału.

III. RAMOWY PLAN STUDIÓW

1. Wykaz przedmiotów z podziałem godzin dydaktycznych oraz punktami ECTS

Lp.	Zakres tematyczny	Punkty ECTS	Forma zaliczenia				
				W	Ć	ĆL	R
1	2	3	4	5	6	7	9
1.	Infrastruktura krytyczna dawniej i dziś	2	zaliczenie	2			2
2.	Zasady identyfikacji infrastruktury krytycznej i europejskiej infrastruktury krytycznej	2	zaliczenie	2	-		2
3.	Zagadnienia organizacyjno–prawne ochrony infrastruktury krytycznej	3	ocena	10			10
4.	Zagrożenia infrastruktury krytycznej na wybranych przykładach. Współzależność infrastruktur krytycznych względem siebie	4	ocena	10	4		14
5.	Alokacja systemu infrastruktury krytycznej w systemie zarządzania kryzysowego	3	zaliczenie	4	6		10

6.	Rola podmiotów odpowiedzialnych za ochronę infrastruktury krytycznej	6	ocena	16	6		22
7.	Analiza ryzyka	2	zaliczenie	6			6
8.	Systemy infrastruktury krytycznej	5	ocena	11	9		20
9.	Współpraca na rzecz ochrony infrastruktury krytycznej	3	zaliczenie	6	4		10
10.	Metodologie ochrony infrastruktury krytycznej w innych państwach	2	zaliczenie	4	2		6
11.	Programy i plany w ochronie infrastruktury krytycznej	4	zaliczenie	6	8		14
12.	Działania na rzecz zapewnienia bezpieczeństwa infrastruktury krytycznej	3	zaliczenie	4	6		10
13.	Problemy infrastruktury krytycznej w praktyce	2	zaliczenie	4	2		6
14.	Ćwiczenia na rzecz ochrony infrastruktury krytycznej. MTD	4	zaliczenie	6	-	8	14
15.	Budowa i wdrożenie systemu zarządzania ciągłością działania w organizacji	2	ocena	8	-		8
16.	Zarządzanie ryzykiem ukierunkowanym na zarządzanie ciągłością działania (Analiza wpływu na Biznes – Business Impact Analysis)	6	ocena	10	14		24
17.	Strategia zarządzania ciągłością działania w organizacji	2	zaliczenie	4	2		6
18	Zasady testowania, przeglądu i audytu wewnętrznego i zewnętrznego systemu zarządzania ciągłością działania	5	ocena	8	8		16
Razem:		60		121	71	8	200

W – Wykład,
Ć – Ćwiczenia,
ĆL – Ćwiczenia laboratoryjne,
R – Razem,

Realizowane przedmioty z podziałem na poszczególne semestry

Przedmioty realizowane w 1 semestrze							
Lp.	**Zakres tematyczny**	**Punkty ECTS**	**Forma zaliczenia**	**W**	**Ć**	**ĆL**	**R**
1	**2**	**3**	**4**	**5**	**6**	**7**	**9**
1.	Infrastruktura krytyczna dawniej i dziś	2	zaliczenie	2			2
2.	Zasady identyfikacji infrastruktury krytycznej i europejskiej infrastruktury krytycznej	2	zaliczenie	2	-		2
3.	Zagadnienia organizacyjno–prawne ochrony infrastruktury krytycznej	3	ocena	10			10
4.	Zagrożenia infrastruktury krytycznej na wybranych przykładach. Współzależność infrastruktur krytycznych względem siebie	4	ocena	10	4		14
5.	Alokacja systemu infrastruktury krytycznej w systemie zarządzania kryzysowego	3	zaliczenie	4	6		10
6.	Rola podmiotów odpowiedzialnych za ochronę infrastruktury krytycznej	6	ocena	16	6		22
7.	Analiza ryzyka	2	zaliczenie	6			6
8.	Systemy infrastruktury krytycznej	5	ocena	11	9		20
9.	Współpraca na rzecz ochrony infrastruktury krytycznej	3	zaliczenie	6	4		10
10.	Metodologie ochrony infrastruktury krytycznej w innych państwach	2	zaliczenie	4	2		6
11.	Programy i plany w ochronie infrastruktury krytycznej	4	zaliczenie	6	8		14
Razem:		36		77	39	0	116
Przedmioty realizowane w 2 semestrze							
Lp.	**Zakres tematyczny**	**Punkty ECTS**	**Forma zaliczenia**	**W**	**Ć**	**ĆL**	**R**

1.	Działania na rzecz zapewnienia bezpieczeństwa infrastruktury krytycznej	3	zaliczenie	4	6		10
2.	Problemy infrastruktury krytycznej w praktyce	2	zaliczenie	4	2		6
3.	Ćwiczenia na rzecz ochrony infrastruktury krytycznej. MTD.	4	zaliczenie	6	-	8	14
4.	Budowa i wdrożenie systemu zarządzania ciągłością działania w organizacji	2	ocena	8	-		8
5.	Zarządzanie ryzykiem ukierunkowanym na zarządzanie ciągłością działania (Analiza wpływu na Biznes – Business Impact Analysis)	6	ocena	10	14		24
6.	Strategia zarządzania ciągłością działania w organizacji	2	zaliczenie	4	2		6
7	Zasady testowania, przeglądu i audytu wewnętrznego i zewnętrznego systemu zarządzania ciągłością działania	5	ocena	8	8		16
Razem:		24		44	32	8	84

2. Ramowy opis zakresu przedmiotów

2.1. Infrastruktura krytyczna dawniej i dziś

Geneza infrastruktury krytycznej. Infrastruktura krytyczna z różnych perspektyw badawczych. Początki ochrony infrastruktury na świecie i w Polsce. Działania NATO w zakresie ochrony infrastruktury krytycznej. Komunikat „Ochrona infrastruktury krytycznej w walce z terroryzmem”. Zielona księga w sprawie europejskiego programu ochrony infrastruktury krytycznej. Dyrektywa Rady Europy w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie jej ochrony. Infrastruktura krytyczna jako kontynuacja nauk z przeszłości. Nauki techniczne i ścisłe jako podstawa elementów infrastruktury krytycznej. Rola nauk humanistycznych i społecznych a ochrona infrastruktury krytycznej. Podejście inter- i transdyscyplinarne. Infrastruktura krytyczna w dobie

globalizacji. Ogólnoświatowy przepływ dóbr i usług. Możliwości i potrzeby reorganizacji narodowych systemów bezpieczeństwa w struktury ponadnarodowe. Globalna wioska krytyczna.

2.2. Zasady identyfikacji infrastruktury krytycznej i europejskiej infrastruktury krytycznej

Obowiązki państw członkowskich Unii Europejskiej. Metodologia wyznaczania infrastruktury krytycznej. Kryteria sektorowe i przekrojowe. Rodzaje skutków powodowanych dysfunkcją Infrastruktur krytycznych mających kluczowe znaczenie dla gospodarek państw, sprawnego funkcjonowania rządu i pomyślnego bytu społeczeństw. Definicje europejskiej infrastruktury krytycznej. Zasady wyznaczania europejskiej infrastruktury krytycznej. Europejski Program Ochrony Infrastruktury Krytycznej (EPOIK). Definicje infrastruktur krytycznych w poszczególnych krajach.

2.3. Zagadnienia organizacyjno – prawne ochrony infrastruktury krytycznej

Infrastruktura krytyczna w prawie Unii Europejskiej oraz w prawodawstwie krajowym. Pojęcie infrastruktury krytycznej i jej ochrony. Systemy infrastruktury krytycznej. Podejścia kompleksowe w ramach współtworzenia Europejskiego Programu Ochrony Infrastruktury Krytycznej. Korelacje aktów prawnych dotyczących infrastruktur krytycznych z rozwiązaniami już funkcjonującymi. Podmioty dokonujące kwalifikacji obiektów wymagających szczególnej i obowiązkowej ochrony.

2.4. Zagrożenia infrastruktury krytycznej na wybranych przykładach.

Współzależność infrastruktur krytycznych względem siebie**.** Zagrożenia wewnątrzsystemowe i międzysystemowe. Atak terrorystyczny na WTC i związane z tym konsekwencje dla infrastruktury krytycznej w USA. Blackout – Szczecin 2008. Cyberatak – Estonia 2007. Szacowanie wartości strat. Wpływ dysfunkcji jednego systemu na pozostałe. Ścieżki propagacji zagrożeń. Efekt domino. Budowa map domino. Przechodzenie od map domino do dotkliwości skutków i szacowanie wartości strat.

2.5. Alokacja systemu infrastruktury krytycznej w systemie zarządzania kryzysowego

Ochrona infrastruktury krytycznej jako subelement systemu zarządzania kryzysowego – zalety i wady. Dopełnienie istniejących środków sektorowych. Korelacja z innymi systemami ochrony. Realizacja zadań w zakresie ochrony infrastruktury krytycznej na potrzeby planów zarządzania kryzysowego. Cykl ochrony infrastruktury krytycznej. Ochrona ludności przed skutkami awarii infrastruktury krytycznej. Rozwiązania sektorowe w zakresie ochrony infrastruktury krytycznej. Identyfikacja rozwiązań na rzecz ochrony infrastruktury krytycznej. Analiza SWOT. Ustalenie poziomu zabezpieczeń (organizacyjnych, proceduralnych, technicznych). Adaptacja rozwiązań międzynarodowych do warunków krajowych.

2.6. Rola podmiotów zaangażowanych w ochronę infrastruktury krytycznej

Podmioty właściwe w sprawach ochrony infrastruktury krytycznej. Obowiązki właścicieli i operatorów infrastruktury krytycznej. Rola Dyrektora Rządowego Centrum Bezpieczeństwa. Udział Szefa Agencji Bezpieczeństwa Wewnętrznego w realizacji zadań z zakresu przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym. Uprawnienia ministra do spraw Skarbu Państwa oraz ich wykonywanie w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorze energii elektrycznej, ropy naftowej i paliw gazowych. Obowiązki spółek kapitałowych lub grup kapitałowych prowadzących działalność w sektorze energii elektrycznej, ropy naftowej i paliw gazowych. Możliwości wykorzystania Sił Zbrojnych Rzeczypospolitej Polskiej do wykonywania zadań z zakresu zarządzania kryzysowego. Ministrowie i centralne organy administracji rządowej – obowiązki w zakresie ochrony infrastruktury krytycznej. Dysfunkcje w sferze administracji publicznej i wynikające z tego konsekwencje. Podstawy prawne przekazania do dyspozycji wojewody pododdziałów lub oddziałów Sił Zbrojnych Rzeczypospolitej Polskiej do wykonywania zadań z zakresu zarządzania kryzysowego. Rola Państwowej Straży Pożarnej, Policji, Straży Gminnych, Straży Granicznej oraz Służby Celnej na rzecz ochrony infrastruktury krytycznej.

2.7. Analiza ryzyka

Analiza ryzyka – podstawowe pojęcia. Metody analizy ryzyka. Szacowanie podatności i skutków wystąpienia zdarzenia. Metodyka oceny ryzyka w administracji

publicznej. Matryca ryzyka sytuacji kryzysowych. Ocena ryzyka wystąpienia zagrożeń mogących powodować dysfunkcje infrastruktury krytycznej.

2.8. Systemy infrastruktury krytycznej

- Efektywność branży paliwowo – energetycznej. Przemysł elektroenergetyczny i jego struktura. Zapasy obowiązkowe paliw. Rola Urzędu Regulacji Energetyki. Skutki zależności polityczno – ekonomicznych. Surowce energetyczne Polski. Formy zabezpieczania infrastruktury krytycznej sieciowej. Zdolność systemów infrastruktury krytycznej do funkcjonowania w warunkach narastającej destabilizacji. Alternatywne kierunki zasilania w produkty, dobra i usługi. Rozwiązania międzypaństwowe na rzecz ochrony krajowych infrastruktur krytycznych. Wymiary bezpieczeństwa energetycznego. Dywersyfikacja źródeł dostaw energii. Bezpieczeństwo przesyłu, dystrybucji oraz sprzedaży energii.
- Łączność w zarządzaniu kryzysowym. Wymogi użytkowników systemu łączności. Potrzeby i wymagania stawiane systemom łączności województwa do działania w sytuacjach nadzwyczajnych zagrożeń. Podsystem łączności stacjonarnej. Wykorzystanie rankingowych sieci łączności ruchomej. System Cyfrowej Łączności Dyspozytorskiej.
- E-government. Informacja jako produkt. Bezpieczeństwo informacji w sieci. Przepływ informacji a działalność gospodarcza. Cyberterroryzm. Elementy składowe krytycznej infrastruktury teleinformatycznej i właściwy system. Przykładowe zagrożenia i sposoby im zapobiegania, a także systemy krytycznej infrastruktury teleinformatycznej. Programy ochrony cyberprzestrzeni.
- Zagrożenia dla systemu finansowego wynikające z kryzysu ogólnoświatowego. Finanse bezgotówkowe. Bezpieczeństwo walutowe państwa. System finansowy jako jeden z kluczowych systemów IK. Ryzyko inwestycji. Fundusze ubezpieczeniowe. Rola Narodowego Banku Polskiego jako banku banków. Ubezpieczenie jako forma transferu ryzyka.
- Bezpieczeństwo produkcji i dostaw. Zanieczyszczenia środowiska a jakość żywności. Żywność genetycznie modyfikowana. Terroryzm żywnościowy. Bezpieczeństwo żywności w państwach Unii Europejskiej. Systemy

zapewnienia bezpieczeństwa zdrowotnego żywności. Nadzór nad bezpieczeństwem żywności. System szybkiego ostrzegania o niebezpiecznych produktach żywnościowych RASFF. Rosnące ceny żywności a bezpieczeństwo państwa.

- Gospodarowanie wodami. Instalacje wodno – kanalizacyjne. Zanieczyszczenia wody. Stacje uzdatniania wody. Gospodarka ściekowa. Zbiorowe zaopatrzenie w wodę. Zagrożenia systemu zaopatrzenia w wodę na przykładzie m.st. Warszawy. Wpływ zaopatrzenia w wodę na inne systemy. Cechy specyficzne systemu zaopatrzenia w wodę i właściwa analiza niezawodności. GIS w informatyzacji przedsiębiorstw wodnych.
- Finansowanie Narodowego Funduszu Zdrowia. Analiza ekonomiczna problemów służby zdrowia. System opieki zdrowotnej – słabości, potrzeby, możliwości. Ocena ryzyka i ochrona infrastruktury krytycznej w obiektach opieki zdrowotnej. Redukowanie społecznej podatności. Katalog zagrożeń.
- System transportowy w systemie logistycznym Polski. Rodzaje transportu – szanse i zagrożenia. Położenie Polski a transformacja zagrożeń. Przewóz towarów niebezpiecznych. Transport rurociągowy. Infrastruktura transportowa. Przyczyny niskiego poziomu bezpieczeństwa na drogach. Cechy i funkcje przedmiotowego systemu. Inwestycyjne działania infrastrukturalne. Scenariusze zagrożeń.
- Infrastruktura ratownicza. Numer alarmowy 112. Organizacja ratownictwa podczas dużych zdarzeń masowych. Służby mundurowe w systemie ochrony ludności. Efektywność funkcjonowania służb. Wsparcie sprzętem specjalistycznym w operacjach ratowniczych. Krajowy System Ratowniczo – Gaśniczy jako podejście kompleksowe do ochrony ludności. Problematyka ochrony ludności. Edukacja społeczeństwa.

2.9. Współpraca na rzecz ochrony infrastruktury krytycznej

Współpraca w ochronie infrastruktury krytycznej na poziomie strategicznym, operacyjnym, zarządczy. Relacja publiczno-prywatna. Forum ochrony infrastruktury krytycznej. Mechanizm ochrony infrastruktury krytycznej. Bieżąca wymiana informacji w ramach ochrony infrastruktury krytycznej. Kanały wymiany informacji. Szkolenia, doradztwo, konferencje.

2.10. Metodologie ochrony infrastruktury krytycznej w innych państwach

Rozwiązania systemowe w państwach Europy Zachodniej i w USA. Ochrona kompleksowa na poziomie strategicznym i operacyjnym. Przykłady sukcesów i niepowodzeń w przyjmowanych wariantach ochrony infrastruktury krytycznej. Ochrona hierarchiczna sektorów infrastruktury krytycznej w zależności od spełnianej prze nią roli.

2.11. Programy i plany w ochronie infrastruktury krytycznej

Narodowy Program Ochrony Infrastruktury Krytycznej. Wizja rządu dotycząca ochrony kluczowych składników infrastruktury państwa. Sposób realizacji obowiązków i współpracy w zakresie Narodowego Programu Ochrony Infrastruktury Krytycznej przez organy administracji publicznej i służby odpowiedzialne za bezpieczeństwo narodowe. Procedura opracowania Narodowego Programu Ochrony Infrastruktury krytycznej. Elementy składowe Narodowego Programu Ochrony Infrastruktury Krytycznej. Plany ochrony infrastruktury krytycznej. Sposób tworzenia, aktualizacji planów ochrony infrastruktury krytycznej. Warunki i tryb uznania spełnienia obowiązku posiadania planu odpowiadającego wymogom planu ochrony infrastruktury krytycznej. Elementy struktury planu ochrony infrastruktury krytycznej. Wykaz podmiotów zobligowanych do opracowania planu ochrony infrastruktury krytycznej. Korelacja z planami zarządzania kryzysowego i planami ciągłości działania.

2.12. Działania na rzecz zapewnienia bezpieczeństwa infrastruktury krytycznej

Zapewnienie bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego, prawnego oraz plany ciągłości działania i odbudowy. Gwaranty skutecznych działań na rzecz ochrony infrastruktury krytycznej. Model zarządzania ryzykiem dla infrastruktury krytycznej oraz model zarządzania ciągłością działania infrastruktury krytycznej. Partnerstwo publiczno – prywatne.

2.13. Problemy infrastruktury krytycznej w praktyce

Forum wymiany informacji. Dublowanie prowadzonych działań. Brak unifikacji metodologii w określaniu elementów infrastruktury krytycznej. Braki w zakresie możliwości ochrony infrastruktury krytycznej. Potrzeba szczegółowej oceny

sposobów ochrony infrastruktury krytycznej. Projektowanie map zagrożeń wywołujących dysfunkcję infrastruktur krytycznych wewnątrz jednego systemu oraz w relacji międzysystemowej. Inwestowanie w ochronę infrastruktury krytycznej – inicjatywy demobilizujące. Wartość rynku ochrony infrastruktury krytycznej. Korelacja między wzrostem na dobra i usługi a kosztem zabezpieczeń. Zasady wzrostu wrażliwości infrastruktur krytycznych na zagrożenia asymetryczne. Uczestnicy rynku zabezpieczeń infrastruktury krytycznej – beneficjenci czy przegrani? Poziom zaangażowania uczestników ochrony infrastruktury krytycznej a mechanizmy zachęt.

2.14. Ćwiczenia na rzecz ochrony IK. MTD

Ćwiczenia na poziomie krajowym, systemowym, regionalnym, lokalnym. Organizatorzy ćwiczeń. Uczestnicy ćwiczeń. Metodyczne wymogi organizacji ćwiczeń. Rodzaje ćwiczeń. Koncepcja wykorzystania Multimedialnego Treningu Decyzyjnego. Kontrola przygotowania podmiotów ochrony infrastruktury krytycznej.

2.15. Budowa i wdrożenie systemu zarządzania ciągłością działania w organizacji

Zarys zarządzania ciągłością działania. Istota ciągłości działania. Przepisy, standardy, normy i źródła dobrych praktyk. Klasyczny cykl zarządzania ciągłością działania. Zrozumienie organizacji. Analiza Wpływu na Biznes (Business Impact Analysis). Wprowadzenie do zarządzania ryzykiem. Strategia ciągłości działania. Plany Ciągłości Działania i Plany Awaryjne. Testowanie i utrzymanie systemu. Model dojrzałości organizacji w obszarze zarządzania ciągłością działania. Korzyści z wdrożenia systemu zarządzania ciągłością działania.

2.16. Zarządzanie ryzykiem ukierunkowanym na zarządzanie ciągłością działania (Analiza wpływu na Biznes – Business Impact Analysis)

Standardy zarządzania ryzykiem. Planowanie reakcji na ryzyko. Identyfikacja ryzyka (budowanie mapy ryzyka/zagrożeń). Pomiar ryzyka. Przeprowadzanie jakościowej analizy ryzyka. Przeprowadzenie ilościowej analizy ryzyka. Limitowanie ryzyka. Monitorowanie ryzyka. System kontroli wewnętrznej. System ograniczania ryzyka operacyjnego.

2.17. Strategia zarządzania ciągłością działania w organizacji

Metody opracowania strategii zapewnienia ciągłości działania w organizacji. Identyfikowanie zadań i zasobów ułatwiających przywrócenie działalności organizacji - krytycznym procesy i zasoby. Zasady opracowania i budowy skutecznego planu reagowania (pierwsza reakcja na sytuację kryzysową, plan zarządzania kryzysowego, zasady współpracy ze służbami pracującymi w trybie ciągłym). Zasady i wytyczne do opracowania działań o krytycznym z uwzględnieniem dostawców i partnerów zewnętrznych. Zasady opracowania planu zarządzania kontaktami komunikacją wewnętrzną i zewnętrzną oraz instytucjami nadzorczymi.

2.18. Zasady testowania, przeglądu i audytu wewnętrznego i zewnętrznego systemu zarządzania ciągłością działania

Zarządzanie ciągłością działania w perspektywie technicznej (kwestia niezawodności technicznej), biznesowej (kwestia ciągłości biznesu), społecznej (kwestia reagowania na kataklizmy naturalne, kryzysy społeczne i terroryzm). Zasady i dobre praktyki w budowie scenariuszy przeprowadzenia testów ciągłości działania. Zasady współpracy ze służbami publicznymi w planowaniu testów (WCZK, PSP, Policja, podmioty systemu PRM). Podstawowe cele, sposoby planowania i przeprowadzania testów ciągłości działania w organizacji. Rodzaje testów. Zasady opracowania programu, scenariuszy i planów testowania na różnych poziomach działalności (zarządzanie kryzysowe, komunikacja kryzysowa, procesy biznesowe, zasoby techniczne). Raporty z testów. Rola audytu wewnętrznego i zewnętrznego w systemie zarządzania ciągłością działania. Cykl audytowy. Zasady przygotowania raportu z audytu w oparciu o wymagania prawne i dobre praktyki. Egzamin na audytora wewnętrznego systemu zarządzania ciągłością działania. Uwarunkowania i zasady prowadzenia ewakuacji przedsiębiorstwa. Egzamin z zakresu prowadzenia ewakuacji przedsiębiorstwa.

IV. EFEKTY KSZTAŁCENIA DLA STUDIÓW PODYPLOMOWYCH OCHRONA INFRASTRUKTURY KRYTYCZNEJ

Zarządzanie ciągłością działania infrastruktury krytycznej wpisuje się w obszar inżynierii bezpieczeństwa w ramach prowadzonego przez WIBC SGSO kierunku studiów inżynieria bezpieczeństwa.

1. Wykaz efektów kształcenia

Kod efektu	Nazwa efektu kształcenia	Odniesienie
WIEDZA		
ZCDIK_W01	Ma wiedzę z zakresu identyfikacji, analizy, oceny, hierarchizacji ryzyka w inżynierii bezpieczeństwa, analizy niezawodności, i skuteczności elementów systemów bezpieczeństwa	K_W07
ZCDIK _W02	Ma podstawową wiedzę w zakresie prawa krajowego i międzynarodowego w przedmiocie ochrony ludności, zarządzania i reagowania kryzysowego, zarządzania ciągłością działania, działań ratowniczych, ochrony przeciwpożarowej, ochrony środowiska, współpracy z administracją publiczną oraz międzynarodowej współpracy ratowniczej	K_W09
ZCDIK _W03	Posiada wiedzę na temat zasad funkcjonowania PSP oraz KSRG i innych systemów ratowniczych	K_W11
ZCDIK _W04	Ma wiedzę z zakresu budowy i działania technicznych systemów zabezpieczeń obiektów, obszarów i infrastruktury technicznej oraz infrastruktury krytycznej, a także wiedzę o materiałach i zasadach ich doboru do zastosowań technicznych	K_W12
ZCDIK _W05	Ma wiedzę na temat metodologii prowadzenia szkoleń i organizacji ćwiczeń i zajęć terenowych	K_W14
ZCDIK _W06	Ma podstawową wiedzę o aspektach prawnych, ekonomicznych i organizacyjnych pracy w sektorze gospodarczym, z zakresu praw i obowiązków, a także odpowiedzialności za bezpieczeństwo powierzonego mienia osób trzecich	K_W15
UMIEJĘTNOŚCI		
ZCDIK _U01	Potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł, powiązać ich treści ze sobą, dokonywać ich krytycznej analizy i interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie	K_U01
ZCDIK _U02	Posiada umiejętności pracy indywidualnej i zespołowej, potrafi stosować terminologię i język techniczny, korzystać z metod symulacyjnych, porozumiewać się z wykorzystaniem nowoczesnych technologii informacyjnych	K_U02
ZCDIK _U03	Potrafi stosować podstawowe metody analityczne, techniki i narzędzia służące rozwiązywaniu zadań inżynierskich związanych z bezpieczeństwem konstrukcji, urządzeń i instalacji	K_U03
ZCDIK _U04	Ma umiejętność samokształcenia się m.in. w celu podnoszenia kompetencji zawodowych	K_U04
ZCDIK _U05	Potrafi korzystać z wiedzy w życiu zawodowym, aktywnie uczestniczyć w pracy grupowej i kierować podwładnymi pracownikami	K_U07
ZCDIK _U06	Potrafi wykonywać analizy bezpieczeństwa i ryzyka, a także w oparciu o nie zarządzać bezpieczeństwem i ryzykiem	K_U08
ZCDIK _U07	Dysponuje wiedzą na temat rozpoznawania i identyfikowania zagrożeń pożarami, wybuchami, awariami przemysłowymi i klęskami żywiołowymi, oraz na temat modeli rozprzestrzeniania się zagrożeń	K_U11
ZCDIK _U08	Potrafi opracować dokumentacje związane z planami i organizacją działań ratowniczych, operacyjno-technicznym zabezpieczeniem terenu i obiektów, organizacją szkoleń i ćwiczeń, zarządzaniem ciągłością działania, a także identyfikować systemy bezpieczeństwa technicznego obiektów, obszarów i infrastruktury krytycznej, w tym systemy zarządzania	K_U16

	ciągłością działania i ich elementy	
KOMPETENCJE SPOŁECZNE		
ZCDIK _K01	Rozumie potrzebę i zna możliwości dokształcania się – podnoszenia kompetencji zawodowych i społecznych	K_K01
ZCDIK _K02	Potrafi odpowiednio określić priorytety czynności i decyzji służbowych	K_K03
ZCDIK _K03	Potrafi myśleć i działać w sposób przedsiębiorczy	K_K04
ZCDIK _K04	Ma świadomość roli społecznej absolwenta uczelni technicznej, a zwłaszcza rozumie potrzebę przekazywania społeczeństwu, w szczególności poprzez środki masowego przekazu, informacji i opinii dotyczących osiągnięć techniki i innych aspektów działalności inżynierskiej; podejmuje starania, aby przekazać takie informacje i opinie w sposób powszechnie zrozumiały	K_K05
ZCDIK _K05	Ma świadomość ważności podejmowania decyzji podczas wykonywania obowiązków służbowych	K_K07
ZCDIK _K06	Potrafi odpowiednio określić priorytety czynności i podejmowanych decyzji podczas wykonywania obowiązków służbowych	K_K08

Wykaz skrótów:
ZCDIK – akronim od pełnej nazwy kierunku studiów
W - kategoria wiedzy
U – kategoria umiejętności
K - kategoria kompetencji społecznych
01, 02,…- numery kolejnych efektów kształcenia

2. Efekty kształcenia dla poszczególnych przedmiotów

Nr	Nazwa	Efekty kształcenia	ECTS
1.	Infrastruktura krytyczna dawniej i dziś	ZCDIK_W01, ZCDIK_W04, ZCDIK_U01, ZCDIK_U05, ZCDIK_U04, ZCDIK_K01, ZCDIK _K05	**2**
2.	Zasady identyfikacji infrastruktury krytycznej i europejskiej infrastruktury krytycznej	ZCDIK_W06, ZCDIK_U01, ZCDIK_K01, ZCDIK_K02, ZCDIK _K04, ZCDIK _UK6	**2**
3	Zagadnienia organizacyjno – prawne ochrony infrastruktury krytycznej	ZCDIK_W06, ZCDIK_U01, ZCDIK _K01	**3**
4.	Zagrożenia infrastruktury krytycznej na wybranych przykładach. Współzależność infrastruktur krytycznych względem siebie	ZCDIK_W04, ZCDIK_W06, ZCDIK_U01, ZCDIK_U02, ZCDIK_U07, ZCDIK_U01, ZCDIK _K02, ZCDIK _K03	**4**
5.	Alokacja systemu infrastruktury krytycznej w systemie zarządzania kryzysowego	ZCDIK _W06, ZCDIK_U01, ZCDIK_U02, ZCDIK_U06, ZCDIK_U07, ZCDIK_K02, ZCDIK_K05, ZCDIK_K06	**3**
6.	Rola podmiotów zaangażowanych w ochronę infrastruktury krytycznej	ZCDIK_W06, ZCDIK_U01, ZCDIK_U02, ZCDIK_U03, ZCDIK_U04, ZCDIK_U05, ZCDIK_U08, ZCDIK_K01, ZCDIK_K02, ZCDIK_K05, ZCDIK_K06	**6**
7.	Analiza ryzyka	ZCDIK_W01,ZCDIK_W02, ZCDIK_W06, ZCDIK _U01,	**2**

		ZCDIK _U03, ZCDIK _U06, ZCDIK _U08, ZCDIK _K03,	
8.	Systemy infrastruktury krytycznej	ZCDIK_W01, ZCDIK_W03, ZCDIK_W05, ZCDIK_W06, ZCDIK_U01, ZCDIK_U02, ZCDIK_U01, ZCDIK_U02, ZCDIK_U03, ZCDIK_U04, ZCDIK_U06, ZCDIK_U07, ZCDIK_K02, ZCDIK_K03	**5**
9.	Współpraca na rzecz ochrony infrastruktury krytycznej	ZCDIK_W01, ZCDIK _W03, ZCDIK _W03, ZCDIK _U05, ZCDIK _K02, ZCDIK _K03, ZCDIK _K05, ZCDIK _K06	**3**
10.	Metodologie ochrony infrastruktury krytycznej w innych państwach	ZCDIK_W06, ZCDIK_U01, ZCDIK_U06, ZCDIK_U07, ZCDIK_U08, ZCDIK_K01	**2**
11.	Programy i plany w ochronie infrastruktury krytycznej	ZCDIK_W01, ZCDIK_W02, ZCDIK_W06, ZCDIK_U01, ZCDIK_U02, ZCDIK_K01, ZCDIK_K07	**4**
12.	Działania na rzecz zapewnienia bezpieczeństw infrastruktury krytycznej	ZCDIK_W01, ZCDIK_W03, ZCDIK_W05, ZCDIK_W06, ZCDIK_U02, ZCDIK_U03, ZCDIK_U04, ZCDIK_K01, ZCDIK_K02, ZCDIK_K04, ZCDIK_K05, ZCDIK_K06, ZCDIK_K07	**3**
13.	Problemy infrastruktury krytycznej w praktyce	ZCDIK_W04, ZCDIK_W06, ZCDIK_U01, ZCDIK_U07, ZCDIK_K04	**2**
14.	Ćwiczenia na rzecz ochrony IK. MTD	ZCDIK_W01, ZCDIK _W03, ZCDIK _W05, ZCDIK _U08, ZCDIK _K05, ZCDIK _K06	**4**
15.	Budowa i wdrożenie systemu zarządzania ciągłością działania w organizacji	ZCDIK_W01, ZCDIK _W02, ZCDIK _W04, ZCDIK _W06, ZCDIK _U01, ZCDIK _U02, ZCDIK _K03	**2**
16.	Zarządzanie ryzykiem ukierunkowanym na zarządzanie ciągłością działania (Analiza wpływu na Biznes – Business Impact Analysis)	ZCDIK_W01, ZCDIK _W02, ZCDIK _W03, ZCDIK _W04, ZCDIK _W06, ZCDIK _U01, ZCDIK _U02, ZCDIK _U03, ZCDIK _U06, ZCDIK _U07, ZCDIK _U08, ZCDIK _K02, ZCDIK _K06	**6**
17.	Strategia zarządzania ciągłością działania w organizacji	ZCDIK_W01, ZCDIK _W02, ZCDIK _W06, ZCDIK _U01, ZCDIK _U02, ZCDIK _U06, ZCDIK _U08, ZCDIK _K02, ZCDIK _K03, ZCDIK _K05, ZCDIK _K06	**2**
18.	Zasady testowania, przeglądu i audytu wewnętrznego i zewnętrznego systemu zarządzania ciągłością działania	ZCDIK _W02, ZCDIK _W03, ZCDIK _W04, ZCDIK _W05, ZCDIK _W06, ZCDIK _U01, ZCDIK _U02, ZCDIK _U03, ZCDIK _U07, ZCDIK _U08	**5**