Załącznik nr 9
do Zarządzenia Rektora Nr 35/19
z dnia 12 czerwca 2019 r.

IV. Opis programu studiów

3. KARTA PRZEDMIOTU

Kod przedmiotu	**E-TD-02-s6**
Nazwa przedmiotu	**Cyberbezpieczeństwo 2**
Nazwa przedmiotu w języku angielskim	**Cybersecurity 2**
Obowiązuje od roku akademickiego	**2020/21**

USYTUOWANIE MODUŁU W SYSTEMIE STUDIÓW

Kierunek studiów	**Teleinformatyka**
Poziom kształcenia	**I stopień**
Profil studiów	**Praktyczny**
Forma i tryb prowadzenia studiów	**Studia stacjonarne**
Zakres	**Teleinformatyka**
Jednostka prowadząca przedmiot	**Katedra Informatyki, Elektroniki i Elektrotechniki**
Koordynator przedmiotu	**dr inż. Aleksandra Sikora, dr inż. Andrzej Stobiecki Michał Rajczykowski – Orange Polska**
Zatwierdził	**Dziekan Wydziału Elektrotechniki Automatyki i Informatyki Dr hab. inż. Antoni Różowicz, prof. PŚk**

OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów*	**Przedmiot kierunkowy**
Status przedmiotu*	**Obowiązkowy**
Język prowadzenia zajęć	**Polski**
Usytuowanie modułu w planie studiów - semestr	**Semestr VI**
Wymagania wstępne	**Cyberbezpieczeństwo 1**
Egzamin (TAK/NIE)	**Tak**
Liczba punktów ECTS	**5**

**pozostawić właściwe*

Forma prowadzenia zajęć	**wykład**	**ćwiczenia**	**laboratorium**	**projekt**	**Inne**
Liczba godzin w semestrze	**15**	**0**	**30**	**15**	**0**

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty kształcenia	Odniesienie do efektów kierunkowych
Wiedza	W01	Ma wiedzę na temat monitorowania bezpieczeństwa w systemach teleinformatycznych.	TI1_W07
	W02	Ma wiedzę na temat zwiększania bezpieczeństwa w sieci	TI1_W07 TI1_W12
	W03	Ma wiedzę o słabych punktach systemów teleinformatycznych	TI1_W12
Umiejętności	U01	Potrafi projektować proste systemy teleinformatyczne z uwzględnieniem zapewnienia ochrony przed zagrożeniami	TI1_U06
	U02	Potrafi rozwiązywać zastane proste problemy cyberbezpieczeństwa	TI1_U17
	U03	Posiada umiejętność określania zapotrzebowania na wykorzystanie technik cyberbezpieczeństwa	TI1_U18
Kompetencje społeczne	K01	Student rozumie potrzebę stałego uzupełniania wiedzy z obszaru cyberbezpieczeństwa	TI1_K03
	K02	Rozumie wagę problemów cyberbezpieczeństwa dla społeczeństwa.	TI1_K01

TREŚCI PROGRAMOWE

Forma zajęć*	Treści programowe
Wykład	1. Incydenty naruszenia polityki bezpieczeństwa. Wpływ ataków na bezpieczeństwo infrastruktury IT
	2. Sieciowe systemy bezpieczeństwa wdrożone na hoście, sieci lub chmurze na przykładzie rozwiązań klasy Firewall, IPS, AMP)
	3. Kwestie bezpieczeństwa w systemie operacyjnym Windows.(m.in. a procesy, wątki, przydział pamięci, rejestr systemu Windows, WMI, usługi)
	4. Kwestie bezpieczeństwa w rodzinie systemów operacyjnych Linux (m.in. procesy, uprawnienia, dowiązania symboliczne, daemony)
	5. Protokoły i usługi sieciowe. Infrastruktura sieci. Zasady bezpieczeństwa sieci.
	6. Charakterystyka popularnych ataków sieciowych oraz metody obrony. Charakterystyka popularnych ataków na aplikacje webowe.
	7. Wpływ powszechnie stosowanych algorytmów szyfrowania i bezpiecznych protokołów komunikacyjnych na bezpieczeństwo. Wpływ powszechnie stosowanych funkcji haszujących na bezpieczeństwo.
	8. Kryptografia i infrastruktura klucza publicznego. Metody ograniczania wpływu szkodliwego oprogramowania. Monitorowanie bezpieczeństwa, analiza danych wykorzystywanych w systemach monitorowania bezpieczeństwa. Jak reagować na incydenty bezpieczeństwa.

laboratorium	1. Badanie i analiza incydentów związanych z cyberbezpieczeństwem. Badanie i analiza słabości urządzeń IoT. Badanie i analiza słabości aplikacji IoT.
	2. Poznawanie procesów, wątków, uchwytów i rejestru systemu Windows. Windows PowerShell.
	3. Windows Task Manager. Nadzorowanie i zarządzanie zasobami systemu Windows.
	4. Bezpieczeństwo w systemie Linux. Linux Servers.
	5. Śledzenie trasy. Wireshark. Sprawdzanie ramek Ethernet. TCP 3-Way Handshake. Nmap. Analiza pakietów UDP DNS. Analiza pakietów TCP, UDP.
	6. Analiza protokołów HTTP and HTTPS.
	7. Łączność lokalna, lista kontroli dostępu. Identyfikacja przepływu pakietów.
	8. Malware (złośliwe oprogramowanie). Social engineering.
	9. Identyfikacja procesów uruchomionych na komputerze, używanego protokołu, lokalnych i zdalnych adresów. Badanie ruchu DNS.
	10. Atakowanie bazy danych mySQL. Analiza logów serwera. Rejestrowanie aktywności sieciowej.
	11. Szyfrowanie i deszyfrowanie danych przy użyciu OpenSSL. Szyfrowanie i deszyfrowanie danych za pomocą narzędzia hakerskiego. Badanie protokołó wTelnet i SSH za pomocą narzędzia Wireshark. Certyfikaty. Man-In-Middle.
	12. Multi-VM. Implementacja NetFlow. Logowanie z wielu źródeł.
	13. Rozwiązania IPS/IDS (na przykładzie Snort) Firewall. Wykorzystanie wyrażeń regularnych.
	14. Analiza plików PCAP. Interpretacja danych HTTP i DNS w celu odizolowania zagrożenia. Izolacja zaatakowanego hosta.
	15. Procedury obsługi incydentów związanych z bezpieczeństwem.
projekt	Celem projektów jest stworzenie systemu, programu lub algorytmu dotyczącego zagadnień cyberbezpieczeństwa, a w szczególności z zakresu: wykrywania, analizy oraz zapobiegania incydentom bezpieczeństwa. Projekty będą realizowane w zespołach dwu lub trzyosobowych osobowych. 1. Określenie zakresu realizacji projektu. 2. Przedstawienie schematu funkcjonalnego (jeżeli dotyczy) 3. Projekt algorytmu i jego opis (jeżeli dotyczy) 4. Analiza (jeżeli dotyczy) 5. Prezentacja rozwiązania oraz wnioski.

*) zostawić tylko realizowane formy zajęć

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów uczenia się					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01	x	x				x
W02	x	x				x
W03	x	x				x
U01				x		x
U02				x		x
U03				x		x
K01				x		x
K02				x		x

FORMA I WARUNKI ZALICZENIA

Forma zajęć*	Forma zaliczenia*	Warunki zaliczenia
Wykład	Egzamin	Uzyskanie co najmniej 50% punktów z egzaminu
Laboratorium	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów w trakcie zajęć
Projekt	zaliczenie z oceną	Wykonanie projektu ocenionego na ocenę pozytywną

*) zostawić tylko realizowane formy zajęć oraz wybrać formę zaliczenia

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS								
Lp.	**Rodzaj aktywności**	**Obciążenie studenta**					**Jednostka**
1.	Udział w zajęciach zgodnie z planem studiów	W	C	L	P	S	h
		15		30	15		
3.	Inne (konsultacje, egzamin)*	2		2	2		h
4.	**Razem przy bezpośrednim udziale nauczyciela akademickiego**	**66**					h
5.	**Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego**	**2.64**					ECTS
6.	**Liczba godzin samodzielnej pracy studenta**	**59**					h
7.	**Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy**	**2.36**					ECTS
8.	**Nakład pracy związany z zajęciami o charakterze praktycznym**	**45**					h
9.	**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym**	**1.80**					ECTS
10.	**Sumaryczne godzinowe obciążenie pracą studenta**	**125**					h
11.	**Punkty ECTS za moduł** *1 punkt ECTS=25 godzin obciążenia studenta*	**5**					

** wszelkie formy weryfikacji efektów, w tym egzaminy oraz nie więcej niż 2 godziny konsultacji dla każdej formy zajęć*

LITERATURA

1. Materiały zawarte na platformie NetAcad udostępniane studentom podczas zajęć dydaktycznych.
2. Wybrane aspekty cyberbezpieczeństwa w Polsce, Tomasz Hoffmann, Wydawnictwo FNCE sp. z o.o., Poznań 2018

Uwaga: wykaz literatury winien uwzględniać aktualne i dostępne publikacje