Karta (sylabus) przedmiotu

WM ***[Zarządzanie i Inżynieria produkcji]***

Studia drugiego stopnia o profilu: A ■ P □

Przedmiot: Ochrona danych i oprogramowania		**ZIP 2 S 0 1 11-0_0**
Status przedmiotu: obowiązkowy		
Język wykładowy: Polski		
Rok: I rok		**Semestr: 1**
Nazwa specjalności:		
Rodzaj zajęć i liczba godzin:	**Studia stacjonarne**	**Studia niestacjonarne**
Wykład	15	
Ćwiczenia		
Laboratorium		
Projekt	15	
Liczba punktów ECTS:	2	

Cel przedmiotu	
C1	Zdobycie wiedzy i umiejętności praktycznych z zakresu ochrony dokumentów elektronicznych przy wykorzystaniu narzędzi informatycznych ogólnodostępnych i specjalistycznych (kryptografia, podpis cyfrowy itp.)
C2	Zdobycie umiejętności bezpiecznego przesyłania danych w sieciach komputerowych (kablowych i bezprzewodowych)
C3	Zdobycie wiedzy z podstaw prowadzenia audytu bezpieczeństwa dla obiektów typu stacja robocza, serwer i lokalna sieć komputerowa oraz umiejętności przygotowania dokumentacji z nim związanej.

Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji	
1	Potrafi obsługiwać stację roboczą na poziomie podstawowym
2	Zna podstawowe elementy sieci komputerowej
3	Potrafi korzystać z poczty elektronicznej

Efekty kształcenia	
	W zakresie wiedzy:
EK 1	Ma pogłębioną wiedzę w zakresie niektórych zagadnień ogólnotechnicznych (w powiązaniu ze studiowaną specjalnością).
EK 2	Posiada wiedzę na temat najlepszych praktyk z zakresu inżynierii produkcji i zarządzania, w dziedzinach objętych programem studiów, zna zaawansowane metody, techniki, narzędzia itp. stosowane w poszczególnych obszarach działalności przedsiębiorstwa (w powiązaniu ze studiowaną specjalnością).
	W zakresie umiejętności:
EK3	Potrafi stosować w pracy lub nauce zaawansowaną i wyspecjalizowaną wiedzę z określonego obszaru nauk pokrewnych inżynierii produkcji i zarządzania (w powiązaniu ze specjalnością), wraz z dokonywaniem interpretacji i wyjaśnianiem zjawisk społecznych oraz wzajemnych relacji występujących między nimi.
EK4	Zna pakiety oprogramowania użytkowego w zakresie pozwalającym na ich zaawansowane stosowanie w pracy zawodowej oraz w życiu codziennym.

EK5	Projektuje i proponuje zmiany w organizacji i/lub jej wybranych obszarach z wykorzystaniem specjalistycznej wiedzy w różnych zakresach i formach oraz norm i standardów.

Treści programowe przedmiotu		
Forma zajęć – wykłady		
	Treści programowe	Liczba godzin
W1	Elementy bezpieczeństwa danych. informacja i dane, archiwizacja, *backup,* kopia zapasowa, replikacja, nośniki i urządzenia do przechowywania informacji, kompresja, digitalizacja, składowanie danych, Zarządzanie ryzykiem.	2
W2	Bezpieczeństwo kryptograficzne i transmisji. Podstawowe pojęcia, regulacje prawne, krótka historia kryptografii, steganografia, algotrytmy kryptograficzne – symetryczne i asymetryczne, funkcje hashujące, podpis cyfrowy, certyfikaty cyfrowe, HTTPS, OpenSSL.	2
W3	Bezpieczeństwo sieci. Sieci komputerowe - przypomnienie podstawowych informacji. Elementy bezpieczeństwa sieci – model OSI i PCT/IP, urządzenia sieciowe, Firewalle – typy, zasady konfiguracji, narzędzia, zagrożenia, topologie. Polityka bezpieczeństwa, dostępność, wydajność. Warstwy sieciowe L1…L5+, IDS, VPN – Spiec. Bezpieczeństwo WiFi	2
W4	Bezpieczeństwo WiFi, algorytmy, topologia SOHO, Enterprise, RADIUS, 802.1x , 802.1x&RADIUS.	2
W5	Bezpieczeństwo systemów operacyjnych. Usługi, uwierzytelnianie, ochrona lokalna, aktualizacje, kopie zapasowe, ochrona fizyczna nośników, weryfikacja możliwości odtworzenia.	2
W6	Bezpieczeństwo infrastruktury. RDBMS – dostępność, aktualizacje, metody uwierzytelniania, rozliczalność. Serwer aplikacyjny, HTTP, DNS.	1
W7	Bezpieczeństwo aplikacji. Aplikacje WWW, architektura, podatności techniczne i nietechniczne, testowanie. Ochrona środowiska, sieci L7 Firewall	1
W8	Polityka ochrony informacji. Planowanie polityki bezpieczeństwa, umowy o zachowaniu poufności, zabezpieczanie budynku i pomieszczeń, tworzenie procedur eksploatacji sprzętu i systemów, ochrona sieci przed programami szpiegującymi, zarządzanie dostępem użytkowników do systemu	2
	Suma godzin:	15
Forma zajęć – projekt		
	Treści programowe	Liczba godzin
P1	Analiza stacji roboczej, określenie poziomu bezpieczeństwa stacji roboczej na ataki lokalne i sieciowe przy wykorzystaniu standaryzowanej „paczki” wirusów.	2
P2	Analiza sieci lokalnej (dla połączeń kablowych i	2

	bezprzewodowych). konfiguracja zabezpieczeń sieciowych stacji roboczej – „firewalla” oraz weryfikacja skuteczności przy użyciu programów do ataku pasywnego.	
P3	Kodowanie danych. Wykorzystanie ogólnodostępnego i specjalistycznego oprogramowania do kryptografii i steganografii do ochrony poufności różnego typu plików, programów oraz partycji. Generowanie podpisu cyfrowego i jego wykorzystanie	2
P4	Projekt I systemu bezpieczeństwa dla wybranej jednostki organizacji o zasięgu lokalnym.	4
P5	Projekt II systemu bezpieczeństwa dla organizacji prowadzącej działalność przez sieć (np. sklep internetowy)	5
	Suma godzin:	15

Narzędzia dydaktyczne	
1	Wykład w prezentacją multimedialną
2	Metoda projektów (projekt praktyczny), praca w grupach, analiza przypadków,

Sposoby oceny	
Ocena formująca	
F1	Krótkie testy w trakcie trwania semestru, których wyniki są omawiane indywidualnie i w grupach
Ocena podsumowująca	
P1	Pisemnego egzaminu z zakresu materiału wykładowego (50% końcowej oceny),
P2	Pisemnego sprawdzianu z zakresu materiału podanego w programie ćwiczeń (30% końcowej oceny),
P3	Zadań projektowych samodzielnie wykonanych jako praca domowa (20% końcowej oceny).

Obciążenie pracą studenta	
Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
[Godziny kontaktowe z wykładowcą, realizowane w formie zajęć dydaktycznych – łączna liczba godzin w semestrze]	30
[Godziny kontaktowe z wykładowcą, realizowane w formie np. konsultacji w odniesieniu – łączna liczba godzin w semestrze]	2
[Przygotowanie się do laboratorium – łączna liczba godzin w semestrze]	10
[Przygotowanie się do zajęć – łączna liczba godzin w semestrze]	8
…	
Suma	50
Sumaryczna liczba punktów ECTS dla przedmiotu	2

Literatura podstawowa i uzupełniająca	
1	J. Stokłosa: Ochrona danych i zabezpieczenia w systemach teleinformatycznych / pod red. Janusza Stokłosy ; [aut. Krzysztof Chmiel et al.]. Wyd. Politechniki Poznańskiej, 2003
2	Serafin M. Sieci VPN : zdalna praca i bezpieczeństwo danych. Wyd. Helion 2008
3	M. Kutyłowski, W. B. Strothmastron: Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych. Wyd. RM 1999
4	W. Garbarczuk, A. Świć: Podstawy ochrony informacji. Wyd. PL 2006.
5	J. Stokłosa: Bezpieczeństwo danych w systemach informatycznych. Wyd. PP 2003

Macierz efektów kształcenia					
Efekt kształcenia	Odniesienie danego efektu kształcenia do efektów zdefiniowanych dla całego programu (PEK)	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposób ocen
EK 1	ZIP2A_W01(++)	C1,C2	W1,W2,W3,W8, P1,P2,P4	1,2	F1,P3
EK 2	ZIP2A_W02(+)	C1,C2	W1,W2,W3, W4,W5,W6,W7, W8, P1, P2,P4	1,2	F1, P3
EK 3	ZIP2A_U06(+++)	C1,C2,C3	W1,W2,W5,W7,W8, P1,P2,P3	1,2	F1,P2,P3
EK 4	ZIP2A_U08(+++)	C1, C2, C3	W1,W2,W3, W4, W5, W6,W7,P1, P2,P3	1,2	F1, P2,P3
EK 5	ZIP2A_U21(++)	C1,C2,C3	W2,W3,W4,W5,W6,W7,W 8, P4,P5	1,2	F1,P1,P2,P

Formy oceny – szczegóły				
	Na ocenę 2 (ndst)	Na ocenę 3 (dst)	Na ocenę 4 (db)	Na ocenę 5 (bdb)
EK 1	Nie potrafi zabezpieczyć stacji roboczej w stopniu podstawowym	Potrafi zainstalować oprogramowanie zabezpieczające stację roboczą na poziomie zaawansowanym	Potrafi zainstalować i skonfigurować poziomy zabezpieczeń na stacji roboczej	Potrafi skonfigurować konta pocztowe oraz specjalistyczne aplikacje na stacjach roboczych na bardzo wysokim poziomie bezpieczeństwa
EK 2	Nie potrafi wykorzystać metod detekcji podatności stacji i systemów	Potrafi wykorzystać wiedzę dotyczącą budowy SO do podniesienia ich bezpieczeństwa	Potrafi wykorzystać wiedzę z innych obszarów kształcenia do projektowania aplikacji	Potrafi zaprojektować bezpieczną aplikację sieciową zawierającą usługi zewnętrzne niezbędne w funkcjonowaniu organizacji
EK 3	Nie potrafi aplikować w rozwiązania informatyczne wiedzy technicznej	Potrafi wykorzystać podstawową wiedzę z nauk społecznych do podnoszenia poziomu bezpieczeństwa stacji roboczej	Potrafi wykorzystać wiedzę z nauk pokrewnych do projektowania i modelowania złożonych struktur podnoszących	Potrafi projektować złożone struktury uwzględniające rozwiązania nieprzewidywalne dotyczące stacji roboczej i sieci

			bezpieczeństwo sieci	
EK4	Nie potrafi korzystać z oprogramowania specjalistycznego	Potrafi korzystać z podstawowych funkcji oprogramowania dedykowanego	Potrafi korzystać z specjalistycznego oprogramowania i dostosowywać je do własnych potrzeb	Potrafi wykorzystać w pracy zaawansowane rozwiązania i modyfikować je wprowadzając własne funkcje
EK5	Nie potrafi tworzyć rozwiązań, które w sposób bezpośredni lub pośredni można zaaplikować w organizacji	Potrafi w swej działalności twórczej uwzględniać podstawowe zasady i normy obowiązujące w organizacji	Potrafi zaprojektować rozwiązania techniczne które mogą być wdrożone bezpośrednio do struktur informatycznych organizacji	Potrafi zaprojektować rozwiązania pozwalające w sposób interaktywny komunikować się z otoczeniem organizacji z zachowaniem standardów i norm obowiązujących środowisko.

Autor programu:	***dr Marek Błaszczak***
Adres e-mail:	m.blaszczak@pollub.pl
Jednostka organizacyjna:	***Instytut Technologicznych Systemów Informacyjnych***
Osoba, osoby prowadzące:	***dr Marek Błaszczak***