	Nazwa modułu. **Blok przedmiotów wybieralnych**						Kod modułu: M23
Wypełnia Zespół Kierunku	Nazwa przedmiotu: **Przedmiot wybieralny II** **Bezpieczeństwo systemu LINUX**						Kod przedmiotu:
	Nazwa jednostki prowadzącej przedmiot / moduł: **INSTYTUT INFORMATYKI STOSOWANEJ**						
	Nazwa kierunku: **INFORMATYKA**						
	Forma studiów: **stacjonarne**		Profil kształcenia: **PRAKTYCZNY**				Specjalność: **Administracja systemów i sieci komputerowych**
	Rok / semestr: **3/6**		Status przedmiotu /modułu: **wybieralny**				Język przedmiotu / modułu: **polski**
	Forma zajęć	wykład	ćwiczenia	ćwiczenia laboratoryjne	konwersatorium	seminarium	inne (wpisać jakie)
	Wymiar zajęć	**15**		**30**			

Koordynator przedmiotu / modułu	**mgr inż. Mariusz Bagiński**
Prowadzący zajęcia	**mgr inż. Mariusz Bagiński**
Cel przedmiotu / modułu	Wyposażenia studenta w praktyczną wiedzę umożliwiającą bezpieczne korzystanie z systemu operacyjnego Linux w charakterze stacji roboczej i serwera w sieci Internet.
Wymagania wstępne	Znajomość zagadnień teoretycznych z zakresu działania sieci komputerowych oraz podstawy obsługi systemu Linux. Biegle na poziomie użytkownika, w zakresie podstawowym na poziomie administratora.

Nr	**EFEKTY KSZTAŁCENIA**	Odniesienie do efektów dla **programu**
	Wiedza	
01	Zna rodzaje zagrożeń występujących w sieciach komputerowych i Internecie.	K_W05, K_W08, K_W16 K_W17
02	Wie jak chronić systemy, sieci i dane przed różnymi zagrożeniami.	K_W04
03	Zna narzędzia zapewniające poufność i integralność danych.	K_W08, K_W12
	Umiejętności	
04	Potrafi skonfigurować zaporę sieciową w systemie Linux.	K_U05, K_U10, K_U13
05	Wykorzystuje szyfrowanie asymetryczne do ochrony plików, katalogów, poczty elektronicznej. Zarządza kluczami. Wykorzystuje podpis cyfrowy.	K_U05, K_U10
06	Bezpiecznie loguje się do systemu, monitoruje stan jego bezpieczeństwa i korzysta z niego z sieci zewnętrznej.	K_U05, K_U06, K_U10, K_U14, K_U22
07	Generuje certyfikaty cyfrowe i wykorzystuje w bezpiecznej komunikacji WWW i FTP.	K_U05, K_U10
	Kompetencje społeczne	
08	Przestrzega etyki zawodowej, w tym poszanowania praw autorskich.	K_K03
09	Chroni dane osobowe i firmowe.	K_K03

TREŚCI PROGRAMOWE

Forma zajęć - WYKŁAD

1. Rodzaje zagrożeń w sieciach komputerowych.
2. Podstawowe bezpieczeństwo systemu: BIOS, GRUB, AppArmor, TCP Wrapper, arpwatch, chroot.
3. Narzędzia kopii zapasowych.
4. Firewall w systemie Linux. Strefa DMZ.
5. Funkcje skrótu: MD5 i SHA1.
6. Szyfrowanie symetryczne i niesymetryczne. GPG.
7. Certyfikaty cyfrowe. Podpis elektroniczny.
8. Ochrona poczty elektronicznej na serwerze i stacji roboczej.
9. OpenSSL. Certyfikaty w usługach: HTTPS, FTPS.

10. SSH, SFTP, certyfikaty w SSH. Tunele SSH.
11. Bezpieczne używanie tradycyjnych i rozszerzonych praw dostępu.
12. Oprogramowanie antywirusowe na serwerze i stacji roboczej Linux.
13. Logi systemowe - Syslog. Analiza logów. Rotacja logów.
14. Automatyczna analiza logów z użyciem pakietu oprogramowania OSSEC. (Trend Micro).
15. Systemy IDS/IPS. Implementacja systemu IPS z użyciem OSSEC i SNORT.

Forma zajęć - LABORATORIUM

1. Konfiguracja podstawowego bezpieczeństwa systemu.
2. Tworzenie kopii zapasowych w systemie Linux.
3. Konfiguracja zapory sieciowej – IPTABLES.
4. Obliczanie funkcji skrótu: sum, md5sum, XCSC, sha1sum.
5. Tworzenie certyfikatów SSL.
6. Uruchamianie usług HTTPS i FTPS.
7. GPG (GNU Privacy Guard) – szyfrowanie plików i katalogów, podpis cyfrowy.
8. GPG (GNU Privacy Guard) - szyfrowanie poczty elektronicznej, podpis cyfrowy poczty.
9. Ochrona poczty elektronicznej: POP3S, IMAPS, spam, antywirusy. Konfiguracja klienta w systemie Linux.
10. Szyfrowanie plików i partycji systemowych z użyciem narzędzia TrueCrypt.
11. Zarządzanie usługą SSH i SFTP, logowanie z użyciem certyfikatów.
12. Aplikacje: Nmap, Nessus, Wireshark, tcpdump i inne.
13. Bezpieczna manipulacja tradycyjnymi i rozszerzonymi listami kontroli dostępu (współdzielenie plików i katalogów, pliki systemowe, inne prawa dostępu).
14. Analiza logów systemowych („ręczna" i automatyczna – OSSEC).
15. Implementacja systemu IPS z użyciem SNORT i OSSEC.

Metody kształcenia	Wprowadzenie, wykonywanie zadanych konfiguracji na maszynach wirtualnych.

Metody weryfikacji efektów kształcenia	Nr efektu kształcenia z sylabusa
Kolokwium zaliczeniowe (wykład).	01-03
Wykonanie zadanej konfiguracji na maszynie wirtualnej + odpowiedź ustna (lab.).	04-09

Forma i warunki zaliczenia	Kolokwium zaliczeniowe z teorii bezpieczeństwa i odpowiednich poleceń systemu Linux (wykład), wykonanie zadania na maszynie wirtualnej + odpowiedź ustna (lab.), odpowiednie wagi: 50% wykład, 50% lab., obecności.
Literatura podstawowa	1. „Linux – bezpieczeństwo. Receptury", autor: D.J. Barrett i inni, Helion 2003. 2. „Bezpieczeństwo sieci w Linuksie. Wykrywanie ataków i obrona przed nimi za pomocą iptables, psad, fwsnort", autor: Michale Rash, Helion 2008. 3. Strony podręcznika systemowego: man, info.
Literatura uzupełniająca	Źródła internetowe.

NAKŁAD PRACY STUDENTA:

	Liczba godzin
Udział w wykładach	15
Samodzielne studiowanie tematyki wykładów	5
Udział w ćwiczeniach audytoryjnych i laboratoryjnych*	30
Samodzielne przygotowywanie się do ćwiczeń*	20
Przygotowanie projektu / eseju / itp. *	
Przygotowanie się do egzaminu / zaliczenia	
Udział w konsultacjach	5
Inne	
ŁĄCZNY nakład pracy studenta w godz.	75
Liczba punktów ECTS za przedmiot	**3 ECTS**
Obciążenie studenta związane z zajęciami praktycznymi*	50 **2 ECTS**
Obciążenie studenta na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich	50 **2 ECTS**