

KARTA OPISU MODUŁU KSZTAŁCENIA		
Nazwa modułu/przedmiotu Ochrona danych i kryptografia		Kod 1010515331010510513
Kierunek studiów Informatyka	Profil kształcenia (ogólnoakademicki, praktyczny) ogólnoakademicki	Rok / Semestr 2 / 3
Ścieżka obieralności/specjalność Zaawansowane technologie internetowe	Przedmiot oferowany w języku: polski	Kurs (obligatoryjny/obieralny) obligatoryjny
Stopień studiów: II stopień	Forma studiów (stacjonarna/niestacjonarna) niestacjonarna	
Godziny Wykłady: 16 Ćwiczenia: - Laboratoria: 18 Projekty/seminaria: -		Liczba punktów 4
Status przedmiotu w programie studiów (podstawowy, kierunkowy, inny) kierunkowy		(ogólnouczelniany, z innego kierunku) z danego kierunku
Obszar(y) kształcenia i dziedzina(y) nauki i sztuki nauki techniczne		Podział ECTS (liczba i %) 4 100%
Odpowiedzialny za przedmiot / wykładowca:		
dr inż. Maciej Miłostan email: maciej.milostan@put.poznan.pl tel. 616652978 Wydział Informatyki ul. Piotrowo 3 60-965 Poznań		
Wymagania wstępne w zakresie wiedzy, umiejętności, kompetencji społecznych:		
1	Wiedza:	Student rozpoczynający ten moduł powinien posiadać podstawową wiedzę z zakresu matematyki, uporządkowaną i podbudowaną teoretycznie wiedzę z zakresu systemów operacyjnych, technologii sieciowych, języków i paradygmatów programowania oraz szczegółową wiedzę dotyczącą programowania aplikacji internetowych. Ponadto wskazane jest posiadanie wiedzy z zakresu ustawy o ochronie danych osobowych.
2	Umiejętności:	W zakres wymaganych umiejętności zalicza się umiejętność rozwiązywania podstawowych problemów algorytmicznych i dokonywania analizy ich złożoności, umiejętność wyszukiwania informacji oraz umiejętność efektywnego uczestnictwa w inspekcji oprogramowania.
3	Kompetencje społeczne	Ponadto w zakresie kompetencji społecznych student musi prezentować takie postawy, jak uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, kultura osobista, szacunek dla innych ludzi.
Cel przedmiotu:		
1. Zapoznanie studentów z wieloaspektową naturą problemu zapewniania bezpieczeństwa systemów informatycznych i zachowania ciągłości procesów biznesowych. 2. Pogłębienie wiedzy studentów z zakresu praktycznego zastosowania technik kryptograficznych, w szczególności z zakresu infrastruktury klucza publicznego i wykorzystywanych w tej infrastrukturze algorytmów asymetrycznych. Pogłębienie wiedzy z zakresu praktycznego wykorzystania algorytmów symetrycznych. 3. Zapoznanie studentów z technologiami stosowanymi w zapewnianiu ciągłości procesów biznesowych i bezpieczeństwa tj. sposobami tworzenia kopii zapasowych (z uwzględnieniem środowisk zwirtualizowanych) i odtwarzaniem danych po awarii, macierzami RAID, mechanizmem deduplikacji. 4. Wskazanie najczęściej popełnianych błędów programistycznych przy tworzeniu aplikacji, ze szczególnym uwzględnieniem aplikacji internetowych. 5. Pogłębienie wiedzy z zakresu ochrony sieci komputerowej. 6. Zapoznanie studentów z zagadnieniem reagowania na incydenty sieciowe.		
Efekty kształcenia i odniesienie do kierunkowych efektów kształcenia		
Wiedza:		

1. Zdobywa podbudowaną teoretycznie szczegółową wiedzę związaną z praktycznym wykorzystaniem technik kryptograficznych i rozwiązań technicznych do szeroko pojętej ochrony danych i zapewnienia ciągłości działania. - [K2st_W3]
2. Zdobywa wiedzę o trendach rozwojowych i nowych praktykach związanych z zapewnianiem ochrony systemów i aplikacji, w tym ochrony przed atakami cyberprzestępczymi. - [K2st_W4]
3. Poglębia i systematyzuje wiedzę związaną z cyklem życia oprogramowania w kontekście zapewniania mechanizmów bezpieczeństwa w różnych fazach rozwoju systemu informatycznego, włącznie z fazą powdrożeniową. - [K2st_W5]
4. Zna podstawowe metody, techniki i narzędzia służące zapewnianiu należytego poziomu ochrony danych i badaniu zabezpieczeń informatycznych. - [K2st_W6]
5. Ma wiedzę nt. zasad, do których należy się stosować w przypadku badań wymagających przetwarzania danych osobowych lub weryfikowania zabezpieczeń systemów informatycznych. - [K2st_W7]

Umiejętności:

1. Potrafi pozyskiwać informacje dotyczące podatności systemów i aplikacji, zagrożeń cybernetycznych oraz możliwych luk w algorytmach kryptograficznych z publicznych baz danych, literatury oraz innych źródeł - [K2st_U1]
2. Poprzez tworzenie sprawozdań z zajęć student pogłębia umiejętność komunikacji w języku ojczystym i korzystania ze źródeł anglojęzycznych. - [K2st_U12]
3. Poprzez samodzielną realizację zadań laboratoryjnych rozwija umiejętność samokształcenia. - [K2st_U16]
4. Potrafi zastosować w kontekście badania bezpieczeństwa systemów metody analityczne, symulacyjne i eksperymentalne. - [K2st_U4]
5. Przy analizach problemów z zakresu ochrony danych potrafi zastosować podejście systemowe i uwzględnić także aspekty pozatechniczne np. czynnik ludzki lub prawny. - [K2st_U5]
6. Potrafi przeprowadzać analizę ryzyka związaną z aspektami bezpieczeństwa architektury systemu informatycznego. - [K2st_U8]
7. Potrafi współdziałać w zespole adresując problemy związane z ochroną danych i bezpieczeństwem systemów teleinformatycznych. - [K2st_U15]
8. Potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć (metod i narzędzi) oraz nowych produktów informatycznych. - [K2st_U6]
9. Potrafi efektywnie uczestniczyć w inspekcji oprogramowania, w szczególności w podstawowym zakresie badań oprogramowanie pod kątem podatności na ataki. - [K2st_U8]

Kompetencje społeczne:

1. Rozumie, że w kontekście ochrony danych i zapewniania bezpieczeństwa część wiedzy i umiejętności bardzo szybko staje się przestarzała lub nieadekwatna do nowych zagrożeń - [K2st_K1]
2. Z perspektywy ochrony danych rozumie znaczenie stosowania najnowszych technik kryptograficznych w badaniach - [K2st_K2]
3. Prawidłowo identyfikuje i rozstrzyga dylematy związane z wykonywaniem zawodu. - [K2st_K4]
4. Ma świadomość roli społecznej absolwenta uczelni technicznej i potrzeby komunikatywnego przekazywania treści, zwłaszcza w kontekście zagrożeń związanych z cyberprzestępczością. - [K2st_K3]

Sposoby sprawdzenia efektów kształcenia

Ocena formująca

a) w zakresie wykładów weryfikowanie założonych efektów kształcenia realizowane jest przez:

- odpowiedzi na pytania dotyczące materiału omówionego na poprzednich wykładach

b) w zakresie laboratoriów / ćwiczeń weryfikowanie założonych efektów kształcenia realizowane jest przez:

- ocenę umiejętności związanych z realizacją ćwiczeń laboratoryjnych
- ocenę sprawozdań przygotowywanych częściowo w trakcie zajęć, a częściowo po ich zakończeniu
- ocenę i obronę zrealizowanych przez studenta ćwiczeń laboratoryjnych

Ocena podsumowująca

a) w zakresie wykładów weryfikowanie założonych efektów kształcenia realizowane jest przez:

- ocenę wiedzy i umiejętności wykazanych na egzaminie pisemnym w formie testu zawierającego zarówno pytania z możliwością wyboru odpowiedzi jak i pytania problemowe wymagające uzupełnienia brakujących elementów wyrażen i definicji. Test zaliczeniowy będzie się składał z min. 19 pytań, lista pytań nie będzie udostępniana studentom, udostępniana będzie tylko informacja o zakresie egzaminu. W celu uzyskania oceny 3.0 należy zdobyć 70% maksymalnej liczby punktów. Dopuszcza się możliwość przeprowadzenia egzaminu poprawkowego w formie ustnej.

- omówienie wyników egzaminu

b) w zakresie laboratoriów / ćwiczeń weryfikowanie założonych efektów kształcenia realizowane jest przez:

- zestawienie ocen wystawionych w trakcie semestru w postaci średniej ważonej ocen częściowych uzyskanych ze sprawozdań z ćwiczeń laboratoryjnych. Do uzyskania zaliczenia wymagane jest pozytywne zaliczenie co najmniej 75% bloków ćwiczeń laboratoryjnych.

Aktywność podczas zajęć premiowana jest dodatkowymi punktami, w szczególności za:

- omówienie dodatkowych aspektów zagadnienia,
- efektywność zastosowania zdobytej wiedzy podczas rozwiązywania zadanego problemu,
- uwagi prowadzące do udoskonalenia materiałów dydaktycznych lub procesu dydaktycznego.

Treści programowe

Program wykładu obejmuje następujące zagadnienia.

Wykład 1-2.: Informacje wprowadzające dotyczące przebiegu procesu kształcenia. Wprowadzenie studentów w wieloaspektową naturę problemu zapewniania bezpieczeństwa systemów informatycznych i zachowania ciągłości procesów biznesowych. Omówienie aspektów bezpieczeństwa pod kątem technicznym, logistycznym, fizycznych oraz danych. Omówienie spektrum zagrożeń dla bezpieczeństwa systemów, usług i aplikacji, oraz sposobów ich adresowania w kontekście strategii dogłębnej ochrony (ang. defense in depth). W szczególności, w toku wykładów przybliżone zostaną ataki na aplikacje. Poruszona zostanie również kwestia ataków typu odmowa obsługi (DoS i DDoS). Zostaną przedstawione podstawowe środki zapobiegawcze adresujące omówione zagrożenia. Proponowane środki uwzględniają wielowarstwową charakterystykę środowiska aplikacyjnego. Ponadto dla lepszego zrozumienia cyklu zapewniania bezpieczeństwa poruszony będzie aspekt ekonomiczny tego procesu i kosztu wdrażania zabezpieczeń.

Wykład 3-4.: Omówienie systemów kryptograficznych symetrycznych i asymetrycznych. Systemy kryptograficzne bezwarunkowo i obliczeniowo bezpieczne. Usługi kryptograficzne. Funkcja Eulera i wykorzystanie jej własności w arytmetyce modularnej. Algorytm potęgowania modulo. Algorytm DES, 3DES i AES jako przykłady standardowe szyfry symetryczne. RSA i ElGamal jako przykłady algorytmów asymetrycznych. Znajdywanie liczb pierwszych i testy pierwszości liczb (sita, test Millera-Rabina, test AKS). Funkcje skrótu. Wybrane zastosowania funkcji skrótu i algorytmów asymetrycznych ? m.in. omówienie mechanizmu podpisu elektronicznego.

Wykład 5-6: Bezpieczeństwo sieci i odtwarzanie po awarii. Zastosowanie i rodzaje zapór sieciowych. Segmentacja sieci i strefa zdemilitaryzowana. Personalizacja dostępu i protokół IEEE802.1X. Dobre praktyki w zakresie aktualizacji systemów. Włamania oraz systemy detekcji intruzów i anomalii. Kopie zapasowe, archiwizacja i odtwarzanie po awarii.

Wykład 7-8: Badanie architektury systemów informatycznych pod kątem możliwych wektorów ataków i związanego z nimi ryzyka (model STRIDE, ocena DREAD). Reagowanie na incydenty w świetle obowiązujących ustaw ? wybrane aspekty.

Ćwiczenia laboratoryjne prowadzone są w formie ośmiu dwugodzinnych zajęć odbywających się w laboratorium komputerowym. Pierwsze zajęcia są częściowo przeznaczone na zapoznanie studentów z zasadami użytkownika laboratorium i zaliczania zadań. Program laboratoriów jest następujący: Laboratorium 1. Ataki na system operacyjny przy dostępie fizycznym do atakowanego systemu. Filtracja pakietów - reguły stanowe i bezstanowe (iptables), proste skanery sieciowe i aplikacje monitorujące (nmap, tcpdump, iptraf, wireshark). Laboratorium 2. Biblioteki Openssl i GnuPG a infrastruktura klucza publicznego (ang. PKI): pozyskiwanie certyfikatów, podpisywanie i szyfrowanie wiadomości, integracja GnuPG z klientem pocztowym. Laboratorium 3 i 4. OWASP WebGoat - ataki na aplikacje internetowe, ćwiczenia praktyczne. Laboratorium 5 i 6. Ataki na serwery usług ? próba wykorzystania podatnych na atak serwerów usług w celu uzyskania dostępu do niezaktualizowanego systemu. Zapoznanie ze źródłami informacji o podatnościach. Wykorzystywanie narzędzi automatycznych i baz ?exploitów? do testowania bezpieczeństwa (np. Metasploit, Nessus). Laboratorium 7 i 8. Filtracja w warstwie aplikacji, firewall nowej generacji (NGN firewalls).

Cześć wymienionych wyżej treści programowych realizowana jest w ramach pracy własnej studenta.

Metody dydaktyczne:

1. Wykład: prezentacja multimedialna wedle potrzeby ilustrowana dodatkowymi przykładami podawanymi na tablicy
2. Ćwiczenia laboratoryjne: ćwiczenia praktyczne przy komputerze realizowane według podanego scenariusza, implementacja programów i skryptów rozwiązujących zadane problemy, dyskusja zastosowanych rozwiązań i konstrukcji programistycznych.

Literatura podstawowa:

1. Official (ISC)2 (R) Guide to The CISSP (R) CBK (R) second edition, Harold F. Tipton (editor), CRC Press, 2009
2. Cryptography and Network Security: Principles and Practice (5th Edition), Stallings W, Prentice Hall, 2010 (lub Ochrona danych w sieci i intersieci - w teorii i praktyce, William Stallings, WNT, 1997)
3. Practical Cryptography, Niels Ferguson and Bruce Schneier, John Wiley&Sons, 2003 (lub Kryptografia w praktyce, Niels Ferguson and Bruce Schneier (Tłumaczenie: Tomasz Żmijewski), Helion, 2004)
4. Modelowanie zagrożeń, Frank Swiderski, Window Snyder, A.P.N. Promise, 2005
5. Bezpieczeństwo danych w systemach informatycznych, Stokłosa J., Bilski T., Pankowski T., Wydawnictwo Naukowe PWN, Warszawa - Poznań, 2001
6. Wykrywanie intruzów, Amoroso E, Wydawnictwo RM, Warszawa, 1999

Literatura uzupełniająca:

1. Understanding the Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations, Adams C., Lloyd S., Kent S, New Riders Publishing, 1999
2. Rethinking Public Key Infrastructures and Digital Certificates, Brands S.A., MIT Press, 2000
3. Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure, Housley R., Polk T, John Wiley & Sons, 2001
4. Polityka bezpieczeństwa i ochrony informacji, Kifner T, Helion, Gliwice, 1999
5. Information Security Management Handbook, Fourth Edition, Krause M.(Editor), Tipton H.F.(Editor), CRC Press - Auerbach Publications, 1999
6. Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych, Kutylowski M., Strothmann W-B, Read Me, Warszawa, 1999
7. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, Schneier B, John Wiley & Sons, 1995
8. Internet Cryptography, Smith R.E, Addison-Wesley Pub Co, 1997
9. Internet Firewalls. Tworzenie zapór ogniowych, Zwicky E.D., Cooper S., Chapman B., Wydawnictwo RM, Warszawa, 2001
10. Cryptography in C and C++, Welschenbach M., APress, 2001

Bilans nakładu pracy przeciętnego studenta

Czynność	Czas (godz.)
1. Udział w wykładach:	16
2. Udział w zajęciach laboratoryjnych / ćwiczeniach:	18
3. Przygotowanie do ćwiczeń laboratoryjnych:	8
4. Dokończenie (w ramach pracy własnej) sprawozdań z ćwiczeń laboratoryjnych:	8
5. Udział w konsultacjach związanych z realizacją procesu kształcenia, w szczególności ćwiczeń laboratoryjnych (dopuszcza się możliwość konsultacji zdalnych)	2
6. Zapoznanie się ze wskazaną literaturą / materiałami dydaktycznymi	26
7. Przygotowanie do egzaminu i obecność na egzaminie: 17 godz. + 1 godz.	18
8. Omówienie wyników egzaminu	1

Obciążenie pracą studenta

forma aktywności	godzin	ECTS
Łączny nakład pracy	97	4
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	38	2
Zajęcia o charakterze praktycznym	32	1