



## KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Ochrona danych i kryptografia

### Przedmiot

Kierunek studiów

Informatyka

Studia w zakresie (specjalność)

Zaawansowane Technologie Internetowe

Poziom studiów

drugiego stopnia

Forma studiów

niestacjonarne

Rok/semestr

2/3

Profil studiów

ogólnoakademicki

Język oferowanego przedmiotu

polski

Wymagalność

obligatoryjny

### Liczba godzin

Wykład

15

Laboratoria

30

Inne (np. online)

Ćwiczenia

Projekty/seminaria

### Liczba punktów ECTS

3

### Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:

dr inż. Maciej Miłostan

Odpowiedzialny za przedmiot/wykładowca:

### Wymagania wstępne

Student powinien posiadać podstawową wiedzę z zakresu aplikacji internetowych, sieci komputerowych i programowania.

### 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. Zapoznania 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.

### Przedmiotowe efekty uczenia się

#### Wiedza

W wyniku przeprowadzonych zajęć student:

1. Zna podstawowe metody, techniki i narzędzia służące zapewnianiu należytego poziomu ochrony danych i badaniu zabezpieczeń informatycznych.
2. Pogłębia i systematyzuje wiedzę związaną z cyklem życia oprogramowania w kontekście zapewniania mechanizmów bezpieczeństwa w różnych fazach rozwoju systemu informatycznego, włącznie z fazą powdrożeniową.
3. Zdobywa wiedzę o trendach rozwojowych i nowych praktykach związanych z zapewnianiem ochrony systemów i aplikacji, w tym ochrony przed atakami cyberprzestępczymi.
4. Zdobywa podbudowaną teoretycznie szczegółową wiedzę związaną z praktycznym wykorzystaniem technik kryptograficznych i rozwiązań technicznych do szeroko pojętej ochrony danych i zapewniania ciągłości działania.
5. Ma pogłębioną i uporządkowaną wiedzę nt. zagrożeń związanych z przestępczością elektroniczną, rozumie specyfikę systemów krytycznych ze względu na bezpieczeństwo (ang. mission-critical systems).

#### Umiejętności

W wyniku przeprowadzonych zajęć student:

1. Potrafi zastosować w kontekście badania bezpieczeństwa systemów metody analityczne, symulacyjne i eksperymentalne.
2. Poprzez samodzielną realizację zadań laboratoryjnych rozwija umiejętność samokształcenia.
3. Poprzez tworzenie sprawozdań z zajęć student pogłębia umiejętność komunikacji w języku ojczystym i korzystania ze źródeł anglojęzycznych.
4. Potrafi pozyskiwać informacje dotyczące podatności systemów i aplikacji, zagrożeń cybernetycznych oraz możliwych luk w algorytmach kryptograficznych z publicznych baz danych, literatury oraz innych źródeł.
5. Przy analizach problemów z zakresu ochrony danych potrafi zastosować podejście systemowe i uwzględnić także aspekty pozatechniczne np. czynnik ludzki lub prawny.
6. Potrafi efektywnie uczestniczyć w inspekcji oprogramowania, w szczególności w podstawowym zakresie badać oprogramowanie pod kątem podatności na ataki.



7. Potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć (metod i narzędzi) oraz nowych produktów informatycznych.

8. Potrafi formułować i testować hipotezy związane z problemami inżynierskimi i prostymi problemami badawczymi.

9. Potrafi przeprowadzać analizę ryzyka związaną z aspektami bezpieczeństwa architektury systemu informatycznego.

#### Kompetencje społeczne

1. Potrafi odpowiednio określić priorytety służące realizacji zadania określonego przez siebie lub innych. Elementem niezbędnym do zaliczenia jest terminowa realizacja szeregu zadań praktycznych.

2. Ma świadomość odpowiedzialności za podejmowane decyzje – braki w realizacji zadań, nieterminowe ich wykonanie lub próby plagiatu wpływają na uzyskiwane oceny.

#### Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

##### 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 uzupełnienie 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 cząstkowych 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

Wykład:

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. Włamanie 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 użytkowania 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, konfiguracja programów i skryptów rozwiązujących zadane problemy, dyskusja zastosowanych rozwiązań i konstrukcji programistycznych

### 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) 5th edition, John Warsinske (editor), Wiley, 2019
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

Uzupełniająca

1. Mastering Regular Expressions, Jeffrey E.F. Friedl, O'Reilly Media, 2006
2. Sed & Awk, Dougherty and Arnold Robbins, O'Reilly and Associates, 1997

**Bilans nakładu pracy przeciętnego studenta**

	Godzin	ECTS
Łączny nakład pracy	75	3,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	30	1,2
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych, przygotowanie do kolokwium, wykonanie projektu) <sup>1</sup>	45	1,8

<sup>1</sup> niepotrzebne skreślić lub dopisać inne czynności