Wydziałowa Komisja Akredytacji Przedmiotów (WKAP)

**Autor***: dr hab. inż. Wojciech Mazurczyk*

# Bezpieczeństwo Komunikacji (BKOM)
# Network and Communications Security

**Poziom kształcenia:** I stopień
**Forma i tryb prowadzenia przedmiotu:** stacjonarna
**Kierunek studiów:** Cyberbezpieczeństwo
**Specjalność:**
**Grupa przedmiotów:**
**Poziom przedmiotu:** podstawowy
**Status przedmiotu:** obowiązkowy
**Język przedmiotu:** polski
**Semestr nominalny (tylko dla przedmiotów obowiązkowych): 5**
**Minimalny numer semestru: 5**
**Wymagania wstępne, zalecane przedmioty poprzedzające: n/d**
**Limit liczby studentów:** 60

**Powód zgłoszenia przedmiotu:** program studiów na nowym kierunku Cyberbezpieczeństwo

**Cel przedmiotu:**

Głównym celem przedmiotu BKOM jest wprowadzenie uczestników do dziedziny bezpieczeństwa komunikacji. W ramach tego przedmiotu omówione zostaną podstawowe zagadnienia dotyczące szeroko pojętego bezpieczeństwa komunikacji, w tym najpopularniejsze rozwiązania, systemy i protokoły wykorzystywane do jego zapewniania. Ponadto przedstawione zostaną dobre praktyki zabezpieczania sieci.

Sposób prowadzenia przedmiotu jest ukierunkowany na naukę praktyczną. Zajęcia wykładowe będą w dużym stopniu poświęcone analizie rzeczywistych sytuacji i przykładów, w których omawiane zagadnienia występują. Zajęcia laboratoryjne będą oparte o wykonywanie praktycznych zadań inżynierskich ilustrujących zagadnienia wykładowe. Celem laboratorium jest praktyczne wprowadzenie studentów do systemowego zapewniania bezpieczeństwa komunikacji w sieciach teleinformatycznych. Zadania laboratoryjne będą polegały na kształtowaniu umiejętności konfiguracji oraz obserwowaniu funkcjonowania systemów, protokołów i innych rozwiązań poprawiających bezpieczeństwo komunikacji. W ramach zajęć projektowych uczestnicy będą realizować zadania wykorzystujące wiedzę i umiejętności zdobyte w ramach wykładów oraz ćwiczeń laboratoryjnych, a które będą ściśle związane z tematyką zapewniania bezpieczeństwa w sieciach teleinformatycznych.

**Treść kształcenia:**

WYKŁADY:

1. **Wprowadzenie do bezpieczeństwa komunikacji (2 godz.)**
   Bezpieczeństwo komputerowe a bezpieczeństwo komunikacji w sieci, rodzaje atakujących sieci oraz narzędzia i techniki które wykorzystują, ataki aktywne/pasywne, wprowadzenie do treści wykładowej, projektowej i laboratoryjnej oraz sposobu oceny.

2. **Podstawowe zagrożenia bezpieczeństwa komunikacji (4 godz.)**
   Źródła zagrożeń / podatności / luk. Klasyfikacja ataków sieciowych. Charakterystyka głównych zagrożeń sieciowych w tym np. skanowania, malware (w tym ransomware), sieci botnet (w tym IoT botnets), ataków (D)DoS, ataków na DNS, Spoofing, Spam, phishing/spear-phishing, luki w TCP/IP, itp.

3. **Ukrywanie informacji w ruchu sieciowym (2 godz.)**
   Rola technik ukrywania informacji w cyberbezpieczeństwie, sposoby wykorzystania technik ukrywania informacji przez malware, klasyfikacja i charakterystyka metod ukrywania informacji, sposoby detekcji i przeciwdziałania rozwiązaniom opartym na ukrywaniu informacji.

4. **Systemy ochrony komunikacji: Firewalling (2 godz.)**
   Definicja firewallingu, filtrowanie Ingress/Egress, rodzaje firewalli: filtry pakietów (pasywne/aktywne), bramy na poziomie sesji, bramy na poziomie aplikacji (proxy nieprzezroczyste/przezroczyste), tworzenie filtrów, koncepcje pokrewne: rola Network Address Translation (NAT) oraz Port Address Translation (PAT), koncepcja Next-Generation Firewall oraz Web Application Firewall (WAF).

5. **Systemy ochrony komunikacji: Rozwiązania NIDS/NIPS (2 godz.)**
   Rola sieciowych systemów detekcji/prewencji włamań, rola NID/PS w porównaniu z firewallami, historia NID/PS, rodzaje NID/PS, komponenty NID/PS według Common Intrusion Detection Framework, omówienie funkcjonowania NID/PS na przykładzie konkretnego rozwiązania np. SNORT, SURICATA, BRO, itp.

6. **Rozwiązania Honeynet/Honeypot (2 godz.)**
   Rola systemów honeypot i honeynet w zapewnianiu bezpieczeństwa sieciowego, rodzaje i sposób działania systemów honeypot/honeynet, przykłady konkretnych systemów honeypot/honeynet wraz z przedstawieniem ich sposobu funkcjonowania.

7. **Protokoły zabezpieczeń komunikacji: SSL/TLS/IPSec/VPN (2 godz.)**
   Rola VPN w bezpieczeństwie komunikacji w tym IPSec (AH, ESP), rola rozwiązań protokołów SSL/TLS w zapewnianiu usług poufność i integralność transmisji danych, a także uwierzytelnienia (serwera, klienta).

8. **Protokoły kontroli dostępu i uwierzytelnienia (2 godz.)**
   Sposoby realizacji usług kontroli dostępu i uwierzytelnienia, rola AAA oraz omówienie jego najważniejsze protokoły tj. RADIUS, TACACS/TACACS+, DIAMETER, itp. Uwierzytelnienie sieciowe z wykorzystaniem Kerberos, czy mobilne używając OAuth, OpenID itp.

9. **Bezpieczeństwo web aplikacji (2 godz.)**
   Zabezpieczanie web aplikacji, sesje HTTP, ataki SQL Injection (SQLi), Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), itp. Rola rozwiązań typu Burp Suite w testowaniu bezpieczeństwa web aplikacji, rola WAF w zabezpieczaniu web aplikacji.

10. **Zapewnianie prywatności w sieci (2 godz.)**
    Istota zapewnienia prywatności użytkownika w sieci Internet, mechanizm HTTP cookies, device fingerprinting, rola rozwiązań typu Tor, DuckDuckGo, Tails w zapewnianiu prywatności w sieci Internet.

11. **Bezpieczeństwo komunikacji w sieci lokalnej (2 godz.)**
    W tym DHCP, STP, VLAN, WLAN, MAC address spoofing, MAC address table overflow, itp. bezpieczeństwo urządzeń końcowych oraz bezpieczeństwo IoT.

12. **Zabezpieczanie usług (2 godz.)**
    Sposoby zabezpieczania usług na przykładzie konkretnych usług np. VoIP, PGP, S/MIME, WLAN itp.

13. **Bezpieczeństwo komunikacji w sieci rozległej w tym sieci operatora (4 godz.)**
    Bezpieczeństwo routingu w tym BGP, ataki DDoS, itp. Sposoby obsługi incydentów, systemy SIEM (Security Incident Event Management), organizacja SOC (Security Operation Center), rola CERT (Computer Emergency Response Team) i wykorzystanie CTI (Cyber Threat Intelligence) w sieciach operatorskich itp. (w tym np. wycieczka do CERT/SOK).

ĆWICZENIA:
–

LABORATORIA:

W ramach projektu każdy student będzie miał do wykonania 5 ćwiczeń laboratoryjnych z wykorzystaniem materiałów instruktażowych oraz korzystając z pomocy Prowadzącego w zakresie:

- Analizy ruchu sieciowego pod katem incydentów bezpieczeństwa.
- Konfiguracji i badanie funkcjonowania rozwiązań typu VPN.
- Konfiguracji i badania działania systemów typu firewall.
- Konfiguracji, badania funkcjonowania i skuteczności systemów typu NID/PS.
- Konfiguracji i badanie sposobu działania systemów honeypot/honeynet.
- Konfiguracji i badanie funkcjonowania systemów zapewniających prywatność w sieci wraz z elementami ukrywania informacji z wykorzystaniem technik steganograficznych.
- Konfiguracji i analizy działania zabezpieczeń protokołów i usług dla sieci LAN/WAN.

Na każde ćwiczenie przewiduje się 3-4 godziny pracy studenta.

PROJEKT:

W ramach projektu zespoły 2-osobowe będą miały do wykonania zadania praktyczne, których wykonanie będzie możliwe poprzez wykorzystanie wiedzy i umiejętności zebranej w trakcie wykładów i laboratoriów. Zespoły otrzymają zadanie do rozwiązania z zakresu zapewniania bezpieczeństwa komunikacji w sieciach teleinformatycznych. Zadania projektowe będą wymagały wyszukania i analizy literatury naukowej.

ZAJĘCIA ZINTEGROWANE:

-

**Treść kształcenia - streszczenie w jęz. angielskim:**

The main objective of the BKOM course is to present to the student the most important aspects of the network and communications security field.

This course identify and introduce the most fundamental concepts related to communication networks security. First the network threats are presented and then based on this background the students are getting acquainted with main defensive solutions i.e. with the most important security systems and protocols which are used in current communication networks. Moreover, specific challenges related to different networks' sizes are discussed and outlined. Finally, by participating in the BKOM course, the students are acquainted with the main guidelines related to developing and maintaining secure communication networks which are important to every future cybersecurity engineer i.e. graduate of the Cybersecurity programme.

**Egzamin: tak**

**Literatura i oprogramowanie:**

Materiały do zajęć stanowią slajdy, instrukcje laboratoryjne, wytyczne wykonania projektu, opracowania, artykuły naukowe.

1. D. Denning, Wojna Informacyjna i bezpieczeństwo informacji, WNT 1999
2. W. Stallings, Kryptografia i bezpieczeństwo sieci komputerowych, Helion 2012
3. Alfred J. Muniz, A. Lakhani, Kali Linux - Testy penetracyjne, Helion 2013
4. J. Hutchens, Skanowanie sieci z Kali Linux - Receptury, Helion 2013
5. Bruce Schneier, Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C, WNT, Warszawa, 2002
6. Sebastian Zander, Grenville Armitage, Philip Branch, A Survey of Covert Channels and Countermeasures in Computer Network Protocols, IEEE Communications Surveys & Tutorials, 3rd Quarter 2007
7. William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin, Firewalls and Internet Security - Repelling the Wily Hacker, Addison-Wesley, ISBN:0-201-63466-X, 2003.

8. E. Bou-Harb, M. Debbabi, C. Assi, Cyber Scanning: A Comprehensive Survey, IEEE Communications Surveys & Tutorials, pp. 1496 - 1519, Vol. 16, Iss. 3, 2014
9. W. Mazurczyk, S. Wendzel, S. Zander, A. Houmansadr, K. Szczypiorski - Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures, IEEE Press Series on Information and Communication Networks Security, IEEE Press-Wiley, April 2016, ISBN-10: 1118861698

Oprogramowanie:
1. Systemy operacyjne Windows, Linux – wersje zarówno klienckie jak i serwerowe.
2. Oprogramowanie open-source i komercyjne do realizacji zadań praktycznych w ramach zajęć laboratoryjnych i projektowych:
   - narzędzia związane z systemami bezpieczeństwa sieciowego,
   - narzędzia do analizy oraz detekcji zagrożeń sieciowych,
   - narzędzia do monitoringu aktywności sieciowych,
   - narzędzia do przeprowadzania testów bezpieczeństwa sieci.

| **Wymiar godzinowy zajęć:** | W | C | L | P |
|---|---|---|---|---|
| | 30 | – | 15 | 15 |

**Przewidywane formy kształcenia i organizacja przedmiotu**

Realizacja przedmiotu obejmuje następujące formy zajęć:
- wykład prowadzony w wymiarze 2 godz. tygodniowo,
- zajęcia laboratoryjne; w ramach tych zajęć student, korzystając z oprogramowania i sprzętu będzie realizował wskazane zadania związane z zapewnianiem i testowaniem bezpieczeństwa sieci teleinformatycznych,
- zajęcia projektowe; w ramach tych zajęć studenci będą wykonywali w 2 osobowych grupach będą wykonywali zadania związane z praktycznymi aspektami zapewniania bezpieczeństwa w sieciach teleinformatycznych i testowaniem tych zabezpieczeń oraz prezentowali wynikające z tych czynności wyniki i wnioski. W ramach projektu niezbędne będzie także przeprowadzenie studium literaturowego związanego z zapewnianiem bezpieczeństwa sieci teleinformatycznych.

Sprawdzanie założonych efektów kształcenia realizowane jest przez:
- ocenę wiedzy i umiejętności wykazanych na egzaminie pisemnym o charakterze problemowym,
- ocenę wiedzy i umiejętności związanych z realizacją zadań laboratoryjnych – ocenę sprawozdań z realizacji zadań,
- ocenę wiedzy i umiejętności związanych z realizacją zadań projektowych – ocena prezentacji i raportu z przeglądu literatury.

**Wymiar w jednostkach ECTS:** 4 pkt.

**Liczba godzin pracy studenta związanych z osiągnięciem efektów kształcenia (opis):**

1. liczba godzin kontaktowych – **60 godzin**, w tym
   - obecność na wykładach: **30 godzin**,
   - obecność na zajęciach laboratoryjnych: **16 godzin**,

- obecność na egzaminie: **2 godzin**,
- obecność na zajęciach projektowych (zajęcia wprowadzające): **2 godzin**,
- udział w konsultacjach związanych z realizacją przedmiotu: **10 godzin.**

2. praca własna studenta – **60 godzin**, w tym
   - analiza literatury i materiałów wykładowych związana z przygotowaniem do kolejnych wykładów: **5 godzin**,
   - analiza literatury i innych materiałów (w tym wykładowych) związanych z przygotowaniem do laboratorium: **20 godzin**,
   - realizacja projektu: **25 godzin**,
   - przygotowanie do egzaminu: **10 godzin.**

**Łączny nakład pracy studenta wynosi 120 godzin, co odpowiada 4 pkt. ECTS.**

**Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich**: 2 pkt. ECTS, co odpowiada 60 godzinom kontaktowym.

**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym:** 2.5 pkt. ECTS, co odpowiada 23 + 45 = 68 godzinom realizacji projektu oraz laboratorium.

## EFEKTY KSZTAŁCENIA/UCZENIA SIĘ

| **efekty kształcenia/uczenia się**<br>student, który zaliczył przedmiot: | **forma zajęć/ technika kształcenia** | **sposób weryfikacji (oceny)*** | **odniesienie do efektów uczenia się dla programu** |
|---|---|---|---|
| WIEDZA | | | |
| W1: ma wiedzę dotyczącą fundamentalnych pojęć z zakresu bezpieczeństwa komunikacji | wykład + projekt + laboratorium | projekt, laboratorium, egzamin | W07<br>W09<br>W12 |
| W2: ma podstawową wiedzę o głównych zagrożeniach w sieciach teleinformatycznych | wykład + projekt + laboratorium | projekt, laboratorium, egzamin | W07 |
| W3: ma podstawową wiedzę z zakresu sposobu funkcjonowania systemów bezpieczeństwa sieciowego | wykład + projekt + laboratorium | projekt, laboratorium, egzamin | W07 |
| W4: ma podstawową wiedzę z zakresu sposobu funkcjonowania protokołów bezpieczeństwa sieciowego | wykład + projekt + laboratorium | projekt, laboratorium, egzamin | W07 |
| W5: ma wiedzę z zakresu analizy ruchu sieciowego pod kątem incydentów bezpieczeństwa | wykład + laboratorium + projekt | laboratorium, egzamin | W07 |
| W6: ma wiedzę z zakresu zapewniania prywatności w sieciach teleinformatycznych | wykład + laboratorium | laboratorium, egzamin | W07<br>W09<br>W12 |
| W7: ma podstawową wiedzę z zakresu ukrywania informacji w ruchu sieciowym | wykład + projekt + laboratorium | projekt, laboratorium, egzamin | W07 |
| W8: ma podstawową wiedzę z obszaru środków technicznych zapewniających bezpieczeństwo komunikacji w sieci teleinformatycznej | wykład + laboratorium + projekt | projekt, laboratorium, egzamin | W07<br>W12 |
| W9: ma podstawową wiedzę z zakresu zapewniania bezpieczeństwa w sieciach różnej skali (LAN, sieć operatora) | wykład + laboratorium + projekt | projekt, laboratorium, egzamin | W07 |
| UMIEJĘTNOŚCI | | | |
| U1: potrafi w podstawowym zakresie definiować zagrożenia występujące w sieci teleinformatycznej | wykład + laboratorium | laboratorium | U03 |
| U2: potrafi wykorzystywać podstawowe narzędzia | wykład + laboratorium | laboratorium | U03 |

| | | | |
|---|---|---|---|
| do testowania zabezpieczeń sieci teleinformatycznych | | | |
| U3: potrafi stworzyć dokumentację z przeprowadzonych badań zgodnie z założoną metodyką i wymaganiami | wykład + laboratorium + projekt | laboratorium + projekt | U03<br>U10 |
| U4: potrafi wykorzystywać podstawowe narzędzia do zapewniania prywatności w sieci teleinformatycznej | wykład + laboratorium | laboratorium | U03 |
| U5: potrafi ocenić funkcjonowanie sieci w przypadku wystąpienia zagrożeń i przewidzieć ich skutki oraz zaproponować sposoby zabezpieczeń | wykład + projekt | projekt | U04<br>U07 |
| U6: potrafi stosować środki techniczne zapewniające bezpieczeństwo komunikacji w sieci | wykład + laboratorium | laboratorium | U08 |
| U7: potrafi w podstawowym zakresie wykorzystywać systemy i protokoły zabezpieczeń do zapewniania bezpieczeństwa w sieci teleinformatycznej | wykład + laboratorium | laboratorium | U05<br>U07 |
| U8: potrafi rozwiązywać zadania formułowane na bieżąco, komunikować wnioski i opinie, prowadzić na ich temat dyskusję i przekonywać innych | projekt | projekt | U09<br>U11 |
| U9: potrafi przeprowadzić krytyczną ocenę bezpieczeństwa przykładowej sieci teleinformatycznej | wykład + laboratorium + projekt | egzamin, projekt | U02<br>U06 |
| U10: potrafi krytycznie analizować dostępną literaturę z dziedziny bezpieczeństwa komunikacji | projekt | projekt | U01<br>U12 |
| KOMPETENCJE SPOŁECZNE | | | |
| KS1: ma świadomość konieczności ciągłego udoskonalania swoich umiejętności, uczenia się i podnoszenia kompetencji w zakresie zapewniania bezpieczeństwa komunikacji | wykład + projekt | n/d | KS01 |
| KS2: ma świadomość etyki cyberbezpieczeństwa, w tym odnajdowania podatności i obsługi incydentów bezpieczeństwa oraz znaczenia wiedzy w rozwiązywaniu problemów bezpieczeństwa sieciowego | wykład + projekt + laboratorium | projekt + laboratorium | KS03 |
| KS3: ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy | wykład + projekt + laboratorium | projekt + laboratorium | KS05 |

**Uwagi:**

**Data i podpis autora (kierownika zespołu autorskiego):**