ZAGADNIENIA DO EGZAMINU INŻYNIERSKIEGO 2026/2027 - CYBERBEZPIECZEŃSTWO

sem/specj.	nazwa kursu	Zagadnienia do egzaminu inżynierskiego
I	Matematyka 1	1. Działania na liczbach i zbiorach. 2. Rozwiązywanie równań i nierówności. 3. Podstawowe własności funkcji. 4. Ciągi liczbowe (ciąg arytmetyczny i ciąg geometryczny, ciągi rekurencyjne). 5. Algebra wektorów (iloczyn skalarny, wektorowy, działania na wektorach).
I	Organizacja i architektura komputerów	1. Architektury procesorów CISC i RISC. 2. Jednostka wykonawcza procesora, jej działanie. 3. Procesor i jego komponenty. 4. Pamięć komputera. 5. Magistrale i interfejsy. 6. Układy wejścia/wyjścia. 7. Struktura komputera.
I	Podstawy programowania	1. Podstawowe elementy języka C++. Typy danych, deklaracje zmiennych i stałych, operatory, wyrażenia, priorytety operatorów oraz podstawowa struktura programu w języku C++. 2. Kompilacja, preprocesor i standardowe wejście/wyjście. Proces kompilacji programu, wybrane dyrektywy preprocesora, obsługa standardowego wejścia i wyjścia oraz śledzenie wykonania programu. 3. Instrukcje sterujące i organizacja kodu. Instrukcje przypisania, instrukcje warunkowe, instrukcje wyboru, pętle oraz instrukcje skoku. Zasady formatowania kodu źródłowego i stosowania komentarzy. 4. Funkcje w języku C++. Deklarowanie, definiowanie i wywoływanie funkcji, parametry i argumenty funkcji, zmienne lokalne, przekazywanie parametrów przez wartość i przez referencję, przeciążanie funkcji, funkcje inline, funkcje lambda oraz funkcje rekurencyjne. 5. Tablice, wektory, napisy i podstawowe struktury danych. Tablice jednowymiarowe i dwuwymiarowe, wektory, ciągi tekstowe w stylu C oraz klasa string. Podstawowe operacje na danych przechowywanych w tych strukturach. 6. Pamięć, wskaźniki i referencje. Model pamięci programu, przestrzenie nazw, wskaźniki, referencje, dynamiczna alokacja pamięci, tablice dynamiczne, wskaźniki do tablic oraz podstawowe problemy związane z zarządzaniem pamięcią. 7. Struktury, pliki i argumenty programu. Struktury, wskaźniki do struktur, tablice struktur, funkcje operujące na strukturach, odczytywanie i zapisywanie plików tekstowych oraz obsługa argumentów wiersza poleceń.

ZAGADNIENIA DO EGZAMINU INŻYNIERSKIEGO 2026/2027 - CYBERBEZPIECZEŃSTWO

sem/specj.	nazwa kursu	Zagadnienia do egzaminu inżynierskiego
I	Teoretyczne podstawy informatyki	1. Klasyczne liczbowe systemy pozycyjne. Porównanie systemu binarnego z systemem U1 i U2. Format zmiennoprzecinkowy IEEE 754. 2. Gramatyki bezkontekstowe. 3. Automaty skończone. Maszyna Turinga. 4. Hierarchia Chomsky'ego języków formalnych. 5. Złożoność czasowa algorytmu? Przykłady problemów o różnej złożoności. 6. Pojęcia ilości informacji oraz entropii. 7. Porównanie źródeł bezpamięciowych oraz źródeł Markowa.
I	*Języki hipertekstowe i tworzenie stron WWW**	1. Struktura i działanie internetu (HTTP/HTTPS, klient–serwer 2. Front-end vs back-end 3. Semantyczne znaczniki HTML5 4. Podstawy CSS (selektory, właściwości) 5. Współpraca HTML, CSS i JavaScript
I	*Systemy CMS**	1. Środowisko i protokół HTTP/HTTPS 2. Rodzaje i zastosowanie technologii webowych 3. Standardy dostępności 4. CMS – budowa, zastosowanie, funkcjonalności 5. Bezpieczeństwo i ochrona danych osobowych
II	Matematyka 2	1. Tautologie i kontrtautologie klasycznego rachunku zdań oraz klasycznego rachunku kwantyfikatorów. 2. Funkcje zdaniowe. 3. Indukcja matematyczna i jej zastosowania. 4. Relacje. Relacje równoważności oraz klasy abstrakcji. Relacje porządku. 5. Funkcja jako relacja - własności funkcji (np. injekcja, surjekcja, bijekcja, składanie funkcji). 6. Kombinatoryka i rachunek prawdopodobieństwa. 7. Zmienna losowa.

ZAGADNIENIA DO EGZAMINU INŻYNIERSKIEGO 2026/2027 - CYBERBEZPIECZEŃSTWO

sem/specj.	nazwa kursu	Zagadnienia do egzaminu inżynierskiego
II	Algorytmy i struktury danych	1. Złożoność obliczeniowa algorytmów i notacja asymptotyczna. Analiza złożoności czasowej i pamięciowej algorytmów. Notacja O oraz notacja Θ. Porównywanie efektywności algorytmów. 2. Algorytmy rekurencyjne. Pojęcie rekurencji, warunek zakończenia, stos wywołań oraz przykłady algorytmów rekurencyjnych, takich jak obliczanie silni, ciągu Fibonacciego, algorytm Euklidesa, przeszukiwanie drzewa czy sortowanie przez scalanie. 3. Algorytmy wyszukiwania i sortowania. Podstawowe algorytmy wyszukiwania danych oraz klasyczne algorytmy sortowania. Zasada działania, warunki stosowania oraz porównanie złożoności wybranych metod. 4. Podstawowe struktury danych. Tablice, listy z dowiązaniami, stosy, kolejki i kopce. Podstawowe operacje wykonywane na tych strukturach oraz przykłady ich zastosowań. 5. Tablice z haszowaniem. Idea haszowania, funkcje haszujące, kolizje oraz podstawowe metody ich rozwiązywania. Operacje wyszukiwania, wstawiania i usuwania elementów. 6. Drzewa i ich zastosowania. Drzewa binarne, drzewa wyszukiwań binarnych, drzewa zrównoważone oraz B-drzewa. Podstawowe operacje na drzewach i przykłady zastosowań. 7. Grafy i podstawowe algorytmy grafowe. Podstawowe pojęcia dotyczące grafów, sposoby reprezentacji grafów oraz wybrane algorytmy grafowe, w szczególności przeszukiwanie grafu i wyznaczanie najkrótszych ścieżek.
II	Wprowadzenie do sieci komputerowych	1. Topologie sieci (fizyczne i logiczne) 2. Media transmisyjne (miedziane, światłowodowe, bezprzewodowe) 3. Enkapsulacja i dekapsulacja 4. Podział na sieci i podsieci (subnetting) 5. Różnice IPv4 vs IPv6
II	Języki i narzędzia programowania obiektowego	1. Pojęcie klasy i obiektu na przykładzie języka C++. 2. Dziedziczenie klas i polimorfizm w C++. 3. Wskaźniki i referencje oraz dynamiczne zarządzanie pamięcią w języku C++. 4. Przeciążenie operatorów, przeciążenie funkcji 5. Konstruktory i destruktory w C++. 6. Biblioteka STL w języku C++.
II	Środowisko cyberbezpieczeństwa	1. Proszę scharakteryzować środowisko cyberbezpieczestwa pastwa. 2. Proszę wymienić podmioty wchodzące w skład Krajowego Systemu Cyberbezpieczestwa (zgodnie z ustawą z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczestwa). 3. Proszę scharakteryzować 3 wybrane zasady prawa międzynarodowego publicznego, które znajdują zastosowanie w cyberprzestrzeni. 4. Proszę omówić temat rywalizacji między podmiotami w cyberprzestrzeni w zakresie: militarnym, technologicznym i społecznym. 5. Proszę scharakteryzować współpracę międzynarodową państw w obszarze cyberbezpieczeństwa, uwzględniając jej cele, mechanizmy oraz główne wyzwania.

ZAGADNIENIA DO EGZAMINU INŻYNIERSKIEGO 2026/2027 - CYBERBEZPIECZEŃSTWO

sem/specj.	nazwa kursu	Zagadnienia do egzaminu inżynierskiego
II	Teoria organizacji i zarządzania	1. Teoretyczne podstawy organizacji i zarządzania pod kątem cyberbezpieczeństwa oraz odpowiednich standardów. 2. Zarządzanie incydentami związanymi z bezpieczeństwem informacji. 3. Zasady gromadzenia informacji dla systemu wykrywania i blokowania ataków. 4. Polityka cyberbezpieczeństwa informacji. 5. Systemy zarządzania bezpieczeństwem informacji.
III	Matematyka 3	1. Rachunek różniczkowy funkcji jednej zmiennej rzeczywistej. 2. Rachunek całkowy funkcji jednej zmiennej rzeczywistej. 3. Zastosowania pochodnych. 4. Zastosowania całek. 5. Liczby zespolone. 6. Macierze i wyznaczniki. 7. Zastosowania macierzy do rozwiązania układu równań liniowych.
III	Wprowadzenie do systemów operacyjnych	1. Zarządzanie pamięcią i jej rodzaje; 2. Urządzenia wejścia/wyjścia i sposoby interakcji jednostki centralnej z nimi; Sposoby zarządzania urządzeniami wejścia/wyjścia; 3. System plików: organizacja logiczna i fizyczna; 4. Synchronizacja procesów: poziom sprzętowy, poziom systemu operacyjnego; 5. Zakleszczenia i metody postępowania w przypadku ich wystąpienia; 6. Strumienie standardowe oraz ich przekierowanie; Praca w systemie operacyjnym z użyciem konsoli; 7. Analiza usterek systemowych i sprzętowych – diagnostyka uszkodzeń w systemach Windows i Linux;
III	Ochrona danych osobowych	1. Wymień trzy podstawowe atrybuty bezpieczeństwa informacji i krótko omów każdy z nich. 2. Przedstaw system ochrony danych osobowych w Polsce (organ nadzorczy, odpowiedzialność i funkcje na poziomie jednostek organizacyjnych). 3. Omów różnicę pomiędzy zwykłymi danymi osobowymi a szczególnymi kategoriami danych osobowych i wskaż po 3 przykłady obydwóch rodzajów danych. 4. Wymień i krótko omów przesłanki legalnego przetwarzania zwykłych danych osobowych. 5. Omów trzy wybrane zasady przetwarzania danych osobowych.

ZAGADNIENIA DO EGZAMINU INŻYNIERSKIEGO 2026/2027 - CYBERBEZPIECZEŃSTWO

sem/specj.	nazwa kursu	Zagadnienia do egzaminu inżynierskiego
IV	Bazy danych (1 i 2)	1. Relacyjny model danych i podstawowe elementy bazy danych. 2. Modelowanie danych za pomocą diagramów ER i EER. 3. Normalizacja i denormalizacja baz danych. 4. Język SQL – konstruowanie zapytań prostych i złożonych. 5. Widoki, procedury składowane, funkcje i wyzwalacze. 6. Indeksy i optymalizacja zapytań SQL. 7. Transakcje, właściwości ACID i problemy współbieżności. 8. Bezpieczeństwo i ochrona danych w systemach bazodanowych. 9. Skalowalność, partycjonowanie, replikacja i wysoka dostępność. 10. Relacyjne bazy danych, NoSQL, NewSQL i twierdzenie CAP.
IV	Bezpieczeństwo aplikacji internetowych (1 i 2)	1. Ataki typu SQL Injection (SQLi) i metody ochrony. 2. XSS mechanizmy ataku i ochrony. 3. Atak typu CSRF i mechanizmy zabezpieczeń. 4. Ataki typu Session Hijacking a nowoczesne metody uwierzytelniania. 5. Techniki ataków typu DoS i DDoS.
IV	Bezpieczeństwo sieci komputerowych (1 i 2, 3)	1. Bezpieczeństwo protokołu HTTP oraz mechanizmy ochrony komunikacji WWW. 2. Podatności protokołu FTP oraz bezpieczne metody przesyłania plików. 3. Bezpieczeństwo systemu DNS i zagrożenia związane z jego działaniem. 4. Uwierzytelnianie, autoryzacja i kontrola dostępu w sieciach komputerowych. 5. Rola podstawowych urządzeń sieciowych w zapewnianiu bezpieczeństwa sieci komputerowej. 6. Zabezpieczanie routerów przed nieautoryzowanym dostępem i atakami sieciowymi. 7. Zabezpieczanie przełączników sieciowych, w tym ochrona portów i kontrola dostępu. 8. Bezpieczeństwo punktów dostępowych oraz sieci bezprzewodowych. 9. Bezpieczeństwo routingu w sieciach komputerowych. 10. Protokoły routingu RIP i OSPF oraz sposoby ich zabezpieczania. 11. Algorytmy routingu i ich znaczenie w zarządzaniu ruchem sieciowym. 12. Sieci VLAN jako mechanizm segmentacji i zwiększania bezpieczeństwa sieci. 13. Zagrożenia związane z sieciami VLAN oraz sposoby ich ograniczania. 14. Rodzaje zagrożeń sieciowych: DoS/DDoS, spoofing, phishing, podsłuchiwanie i przechwytywanie danych. 15. Podstawowe mechanizmy zabezpieczające sieci komputerowe: firewall, VPN oraz IDS/IPS.

ZAGADNIENIA DO EGZAMINU INŻYNIERSKIEGO 2026/2027 - CYBERBEZPIECZEŃSTWO

sem/specj.	nazwa kursu	Zagadnienia do egzaminu inżynierskiego
IV	Programowanie niskopoziomowe	1. Struktura programu w asemblerze x86 (NASM) 2. Architektura x86 (32 i 64-bitowa) procesora (rejestry, instrukcje, pamięć i adresacja) 3. Kompilacja kodu (GCC i NASM) oraz analiza programu za pomocą debugera GDB (GNU Debugger) 4. Mechanizmy zarządzania pamięcią w programach C/C++: analiza dynamicznej alokacji (malloc(), new) oraz dealokacji (free(), delete), konwersja wskaźników wysokopoziomowych na adresy fizyczne w pamięci 5. Stos: obszar pamięci i zasada jego działania oraz wykorzystania w programach
IV	Programowanie skryptowe	1. Typty danych i operatory w języku Python. 2. Składnia i semantyka instrukcji sterujących w języku Python (instrukcje warunkowe i iteracyjne), instrukcje match-case. 3. Struktura programu oraz funkcje w języku Python, wbudowane funkcje w języku Python. 4. Kolekcje w języku Python (słowniki, krotki, zbiory listy). 5. Obsługa plików w języku Python, wyrażenia regularne, rekurencja w języku Python.
IV	Teoria informacji i kodowania	1. Model systemu komunikacyjnego. 2. Pojęcie informacji i entropii. 3. Modele źródeł informacji. 4. Kodowanie źródeł dyskretnych. 5. Kody korekcyjne w systemach transmisji danych.
IV	Zarządzanie kryzysowe w cyberbezpieczeństwie	1. System zarządzania kryzysowego w Polsce – mocne i słabe strony z perspektywy cyberbezpieczeństwa. 2. Fazy zarządzania kryzysowego - przykłady działań. 3. Postępowanie z incydentem cybernetycznym w zarządzaniu kryzysowym – przykłady i ocena proces incident response. 4. Infrastruktura krytyczna i jej ochrona przed zagrożeniami cybernetycznymi – rola i współdziałanie poszczególnych podmiotów. 5. Narzędzia i technologie użyteczne podczas zapobiegania, przygotowania, reagowania i odbudowy.
IV	Biały wywiad	1. Istota i znaczenie białego wywiadu (OSINT) we współczesnym środowisku informacyjnym 2. Metody i narzędzia pozyskiwania oraz weryfikacji informacji w OSINT 3. Aspekty prawne, etyczne i bezpieczeństwa w działalności OSINT
V	Bezpieczeństwo infrastruktury krytycznej i systemów sterowania przemysłowego IoT	1. Architektura sieci przemysłowych, Model Purdue oraz różnice między środowiskami IT a OT 2. Modelowanie zagrożeń i ocena ryzyka w cyberbezpieczeństwie 3. Monitorowanie sieci, systemy wykrywania intruzów oraz reagowanie na incydenty w OT 4. Utwardzanie (hardening) urządzeń końcowych oraz bezpieczeństwo Przemysłowego Internetu Rzeczy 5. Infrastruktura jako kod (IaC), konteneryzacja i orkiestracja w nowoczesnych systemach

ZAGADNIENIA DO EGZAMINU INŻYNIERSKIEGO 2026/2027 - CYBERBEZPIECZEŃSTWO

sem/specj.	nazwa kursu	Zagadnienia do egzaminu inżynierskiego
V	Kryptografia	1. Podstawowe elementy kryptografii: Podstawowe pojęcia; Proste szyfry; Szyfrowanie z kluczem; Szyfrowanie symetryczne i asymetryczne. 2. Tryby działań algorytmów symetrycznych: ECB; CBC; CFB; OFB; Zastosowania; Zalety; Wady. 3. Algorytm kryptograficzny DES, Triple DES i RSA: Schemat i opis; Procedura szyfrowania i odszyfrowania. Stosowanie 4. Podpis cyfrowy: Uogólniony schemat; ElGamala; Ślepe podpisy cyfrowe; Niezaprzeczalne podpisy cyfrowe. 5. Techniki i metody kryptoanalityczne: Kryptoanaliza; Techniki łamania szyfrów.
V	Sprzętowe aspekty cyberbezpieczeństwa	1. Pojęcie bezpieczeństwa sprzętowego oraz rola sprzętu jako root of trust. 2. Hierarchia sprzętu elektronicznego: PCB, układ scalony, SoC, mikroprocesor. 3. Globalizacja łańcucha dostaw a zagrożenia dla integralności sprzętu. 4. Sprzętowe mechanizmy ochrony: implementacje kryptograficzne, kontrola dostępu, odporność na manipulację, wykrywanie włamań. 5. Bezpieczeństwo systemów wbudowanych i IoT oraz ograniczenia projektowe.
V	Wykrywanie anomalii sieciowych z użyciem uczenia maszynowego	1. Pojęcie anomalii w systemach komputerowych oraz ich klasyfikacja (point, contextual, collective). 2. Reprezentacja danych i inżynieria cech w detekcji anomalii (cechy statystyczne, czasowe, behawioralne). 3. Metody uczenia maszynowego w detekcji anomalii (modele nadzorowane, nienadzorowane i półnadzorowane). 4. Problem niezbalansowanych danych oraz metryki oceny modeli (PR-AUC, TPR/FPR, wybór progu decyzyjnego). 5. Zastosowanie metod detekcji anomalii w cyberbezpieczeństwie (IDS/IPS, wykrywanie ataków sieciowych).
V	Wojny informacyjne	1. Dezinformacja jako element wojen hybrydowych. 2. Podstawowe metody i środki prowadzenia działań w ramach wojen informacyjnych. 3. Ataki socjotechniczne jako narzędzie wojen informacyjnych oraz ich klasyfikacja. 4. Rola białego wywiadu (OSINT) w wojnach informacyjnych oraz podstawowe narzędzia OSINT. 5. Rola sztucznej inteligencji (AI) we współczesnych wojnach informacyjnych oraz jej zastosowania.
V	Podstawy prawne cyberbezpieczeństwa	1. Wymień podstawowe elementy cyberprzestrzeni. 2. Wymień trzy podstawowe elementy krajowego systemu cyberbezpieczeństwa (tzw. zespoły reagowania na incydenty komputerowe) i krótko omów ich właściwość. 3. Wymień trzy wybrane akty prawne i trzy instytucje na poziomie Unii Europejskiej właściwe w zakresie cyberbezpieczeństwa. 4. Wymień cztery podstawowe rodzaje cyberprzestępstw określonych w Konwencji Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r. (Dz.U. 2015 poz. 728). 5. Wymień podmioty, które obejmuje krajowy system cyberbezpieczeństwa (na podstawie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j. Dz. U. z 2026 r., poz. 20 z późn. zm.).

ZAGADNIENIA DO EGZAMINU INŻYNIERSKIEGO 2026/2027 - CYBERBEZPIECZEŃSTWO

sem/specj.	nazwa kursu	Zagadnienia do egzaminu inżynierskiego
V	Zarządzanie strategiczne w cyberbezpieczeństwie	1. Omów znaczenie cyberbezpieczeństwa jako elementu zarządzania strategicznego współczesnej organizacji. Wskaż wpływ zagrożeń cybernetycznych na realizację celów biznesowych. 2. Scharakteryzuj klasyczny proces zarządzania strategicznego oraz wskaż, które jego elementy mogą zostać zaadaptowane do zarządzania cyberbezpieczeństwem organizacji. 3. Przedstaw strategiczne konsekwencje wdrożenia regulacji prawnych dotyczących cyberbezpieczeństwa i ochrony danych osobowych, ze szczególnym uwzględnieniem RODO oraz dyrektywy NIS2. 4. Wyjaśnij rolę identyfikacji i mapowania aktywów informacyjnych w procesie zarządzania cyberbezpieczeństwem oraz podejmowaniu decyzji strategicznych. 5. Opisz proces doboru strategii cyberbezpieczeństwa do profilu ryzyka organizacji. Wskaż czynniki wpływające na wybór odpowiednich mechanizmów ochrony.
V	*Komunikacja i zarządzanie projektami **	1. Modele komunikacji w zespołach projektowych. 2. Zarządzanie projektami informatycznymi (Scrum, Kanban, Waterfall). 3. Rola interesariuszy i zarządzanie wymaganiami. 4. Dokumentacja projektowa i jej znaczenie w procesie wytwórczym. 5. Narzędzia wspomagające zarządzanie projektami (Jira, Trello).
V	*Metody badawcze w informatyce i projektach inżynierskich**	1. Podejścia badawcze (ilościowe, jakościowe, mieszane) 2. Typy badań (podstawowe, stosowane, eksperymentalne) 3. Plan badawczy – organizacja przebiegu badan 4. Powtarzalność badań 5. Etyka w badaniach naukowych
V	*Programowanie aplikacji mobilnych**	1. Proces tworzenia aplikacji mobilnej od pomysłu po wdrożenie 2. Podejścia do tworzenia aplikacji mobilnych – natywne i cross-platformowe 3. Budowa aplikacji Flutter, widgety i zarządzanie stanem 4. Bezpieczna komunikacja z API i przetwarzanie danych 5. Persystencja danych i bezpieczne przechowywanie informacji
V	*Tworzenie aplikacji internetowych**	1. Środowisko i protokół HTTP/HTTPS 2. Rodzaje i zastosowanie technologii webowych 3. Standardy wymiany danych (XML, JSON) 4. Analiza potrzeb użytkownika 5. Bezpieczeństwo, ochrona danych osobowych i dostępność

ZAGADNIENIA DO EGZAMINU INŻYNIERSKIEGO 2026/2027 - CYBERBEZPIECZEŃSTWO

sem/specj.	nazwa kursu	Zagadnienia do egzaminu inżynierskiego
VII	Analiza malware	1. Klasyfikacja i charakterystyka złośliwego oprogramowania 2. Statyczna analiza malware 3. Dynamiczna analiza malware 4. Techniki ukrywania i utrudniania analizy malware 5. Wykrywanie, ocena zagrożenia i dokumentowanie analizy malware
VII	Bezpieczeństwo systemów operacyjnych (1 i 2)	1. IDS, HIDS, NIDS , IPS 2. Filtrowanie pakietów w jadrze systemu 3. Szyfrowanie dyskow 4. Utwardzanie jądra systemu 5. Certyfikowanie kluczy publicznych i PKI 6. Algorytmy kryptograficzne i funkcje skrótu 7. VPN i IPSec 8. Uwierzytelnianie i Autoryzacja 9. Utwardzanie systemu (Hardening) 10. Bezpieczeństwo Protokołów Sieciowych (SSH, TLS, HTTP/S)
VII	Metodyki testów penetracyjnych	1. Omów prawidłową strukturę raportu z testów penetracyjnych oraz dobre praktyki jego prezentacji. 2. Jakie kluczowe kwestie formalno-prawne i organizacyjne należy uzgodnić przed rozpoczęciem testów penetracyjnych? 3. Omów klasę podatności typu Injection: wyjaśnij mechanizm jej powstawania, potencjalne skutki ataku oraz skuteczne metody mitygacji. 4. Czym różni się horyzontalna eskalacja uprawnień od wertykalnej i jakie potencjalne zagrożenia niesie ze sobą każda z nich? 5. Jaką rolę w procesie testów penetracyjnych odgrywa skanowanie sieci i jakich narzędzi najczęściej używa się do mapowania infrastruktury?
VII	Wykrywanie incydentów	1. Źródła danych wykorzystywane w wykrywaniu incydentów bezpieczeństwa 2. Metody wykrywania i klasyfikacji incydentów 3. Postępowanie po wykryciu incydentu
VII	*Analiza informacji**	1. Pozyskiwanie i przygotowanie danych do analizy. 2. Eksploracyjna analiza danych oraz weryfikacja i korelacja informacji. 3. Analiza tekstu, ekstrakcja informacji z dostępnych źródeł. 4. Metody statystyczne, uczenie maszynowe w aspekcie wykrywania anomalii, zastosowanie narzędzi AI. 5. Ocena wyników analizy i raportowanie

ZAGADNIENIA DO EGZAMINU INŻYNIERSKIEGO 2026/2027 - CYBERBEZPIECZEŃSTWO

sem/specj.	nazwa kursu	Zagadnienia do egzaminu inżynierskiego
VII	*Metody eksploracji danych**	1. Eksploracja danych w cyberbezpieczeństwie. Cele eksploracji danych, podstawowe etapy analizy oraz typowe źródła danych: logi systemowe, logi sieciowe, alerty bezpieczeństwa, dane aplikacji internetowych i dane OSINT. 2. Przygotowanie danych do analizy. Czyszczenie danych, obsługa braków, duplikatów i wartości odstających, kodowanie zmiennych kategorycznych oraz agregacja danych według czasu, użytkownika, adresu IP lub hosta. 3. Eksploracyjna analiza danych i wizualizacja. Statystyki opisowe, analiza rozkładów, analiza częstości, korelacje oraz podstawowe wykresy wykorzystywane do wykrywania wzorców i nietypowych obserwacji. 4. Klasyfikacja i ocena modeli w cyberbezpieczeństwie. Zastosowanie klasyfikacji do wykrywania zagrożeń, podział danych na zbiór uczący i testowy oraz ocena modeli za pomocą macierzy pomyłek, accuracy, precision, recall i F1-score. 5. Grupowanie i wykrywanie anomalii. Idea uczenia bez nadzoru, podstawowe metody grupowania i detekcji anomalii oraz ich zastosowanie do analizy alertów, logowań, ruchu sieciowego i nietypowej aktywności użytkowników.

**Kurs do wyboru!*