CyberAgent

Co-funded by the European Union

D3.1 MODUŁY SZKOLENIOWE DLA STUDENTÓW SZKÓŁ WYŻSZYCH

CYBERAGENT 01.2025

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Pakiet roboczy 3: CyberAgent Tworzenie zasobów edukacyjnych

Produkt 3.1: Moduły szkoleniowe dla studentów szkół wyższych

Lider WP3 – TIMTAL. Lider D3.1 – VU.

TREŚĆ

WPROWADZENIE

Zgodnie z raportem D2.2, MŚP borykają się z poważnym niedoborem wykwalifikowanych specjalistów ds. cyberbezpieczeństwa, a obecni pracownicy często nie posiadają systemowej wiedzy niezbędnej do odpowiedniego reagowania na coraz bardziej złożone cyberzagrożenia. Dlatego też w szkolnictwie wyższym szczególnie ważne jest przygotowanie specjalistów, którzy będą potrafili zastosować swoją wiedzę w środowisku MŚP – zarówno w obszarze technicznym, jak i zarządczym. W związku z tym w dokumencie D2.3 stworzono ścieżkę kształcenia opartą na kompetencjach, podzieloną na różne obszary tematyczne i skoncentrowaną na rozwoju praktycznych umiejętności.

Niniejszy dokument przedstawia jeden z głównych rezultatów projektu – moduły szkoleniowe dla studentów szkół wyższych (D3.1). Celem tego działania jest stworzenie programów szkoleniowych dla instytucji szkolnictwa wyższego (HEI), które obejmują kluczowe obszary wiedzy, umiejętności i kompetencji w zakresie cyberbezpieczeństwa istotne dla małych i średnich przedsiębiorstw (MŚP).

Moduły te są wynikiem konsekwentnej pracy opartej na szczegółowej analizie potrzeb (D2.2), podczas której przeprowadzono ankietę wśród przedstawicieli MŚP, instytucji kształcenia i szkolenia zawodowego (VET) oraz instytucji szkolnictwa wyższego, a także jasno określonej strukturze ścieżki edukacyjnej (D2.3).

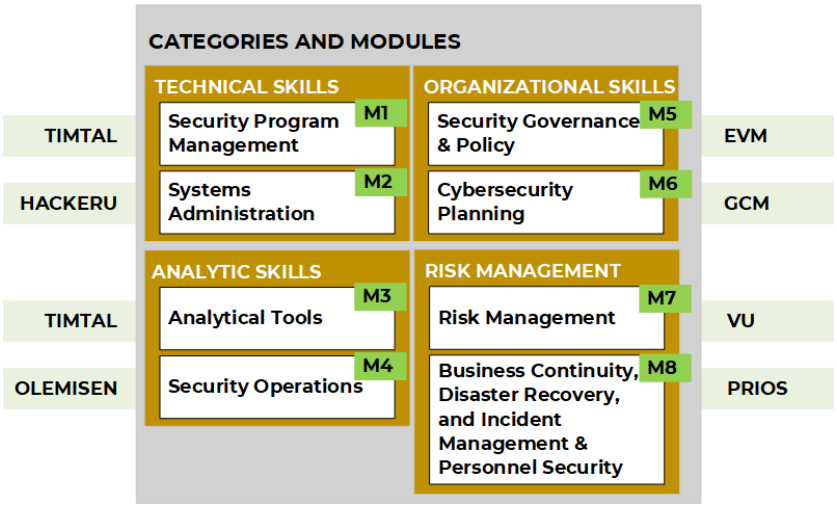
Program szkoleniowy, odpowiadający poziomom 5–6 Europejskich Ram Kwalifikacji (EQF), jest przeznaczony dla studentów szkół wyższych i zaawansowanych pracowników MŚP. Składa się z ośmiu modułów podstawowych i jednego modułu inspirującego, obejmujących cztery podstawowe obszary kompetencji:

- **Umiejętności techniczne** (zarządzanie programami bezpieczeństwa, administracja systemami).
- **Umiejętności analityczne** (narzędzia analityczne, operacje bezpieczeństwa).
- **Umiejętności organizacyjne** (zarządzanie bezpieczeństwem i polityka bezpieczeństwa, planowanie cyberbezpieczeństwa).
- **Zarządzanie ryzykiem** (zarządzanie ryzykiem i ograniczanie ryzyka, ciągłość działania, odzyskiwanie danych po awarii oraz zarządzanie incydentami i bezpieczeństwo personelu).

Każdy moduł jest wart 3 punktów ECTS (odpowiadających 75 godzinom pracy studenta), jest zgodny z zasadami obszaru szkolnictwa wyższego i przestrzega zaleceń metodologicznych określonych w D2.3: edukacja opiera się na aktywnych metodach uczenia się (np. studia przypadków, uczenie się oparte na projektach) i samokształceniu, a efekty uczenia się są wyraźnie rozróżnione na poziomie wiedzy, umiejętności i kompetencji.

Każdy moduł o wartości 3 punktów ECTS został opracowany przez różnych partnerów konsorcjum, wykorzystujących swoją specyficzną wiedzę i doświadczenie zawodowe.

Opracowane moduły obejmują następujące kluczowe obszary, uznane za niezwykle ważne w raporcie D2.2:



1. M1: ZARZĄDZANIE PROGRAMAMI BEZPIECZEŃSTWA

Tytuł modułu	Kod modułu
ZARZĄDZANIE PROGRAMEM BEZPIECZEŃSTWA	

Wykładowca (wykładowcy)	Instytucja lub wydział, w którym realizowany jest moduł

Sposób realizacji	Język
Stacjonarne, online, hybrydowe	*Angielski, fiński, turecki, norweski, litewski, rumuński, francuski, polski, hiszpański*

Wymagania wstępne
Brak

Liczba przyznanych punktów ECTS	Obciążenie pracą studenta	Godziny zajęć kontaktowych	Indywidualne godziny pracy
3	75 godzin	50 godzin	25 godzin

Cel i efekty modułu

Po ukończeniu tego kursu studenci będą dysponować umiejętnościami pozwalającymi skutecznie zarządzać programami bezpieczeństwa w odpowiedzi na zagrożenia cyberbezpieczeństwa. Opracują strategie obrony przed aktualnymi zagrożeniami, takimi jak phishing, oprogramowanie ransomware i ataki DDoS, w ramach zarządzania projektami i zasobami. Ponadto studenci nauczą się stosować wskaźniki bezpieczeństwa i metody zapewnienia jakości, zdobywając umiejętność optymalizacji programów bezpieczeństwa, efektywnego zarządzania zasobami i zwiększania bezpieczeństwa organizacji poprzez wykorzystanie odpowiednich narzędzi przeciwko ewoluującym zagrożeniom. Kurs ten pozwoli również rozwinąć kompetencje w zakresie oceny zagrożeń, raportowania i komunikacji, umożliwiając skuteczne wdrażanie strategii cyberbezpieczeństwa w swoich organizacjach.

Efekty kształcenia modułu	Metody nauczania i uczenia się	Metody oceny
Wiedza: Uczestnicy zdobędą praktyczną wiedzę na temat najnowszych zagrożeń dla cyberbezpieczeństwa, w tym phishingu, oprogramowania ransomware i ataków DDoS, oraz sposobów zarządzania nimi poprzez skuteczne zarządzanie projektami i zasobami oraz wdrażanie środków zapewnienia i kontroli jakości.	Do wyboru przez wykładowcę z części 1.3. [Metody nauczania, np. wykłady teoretyczne, prelegenci gościnni, quizy, gry, zadania praktyczne/laboratoria, nauczanie i uczenie się między rówieśnikami, samokształcenie itp.	Testy samooceny Test sprawdzający wiedzę

Umiejętności: Uczestnicy zdobędą umiejętności korzystania z narzędzi i oprogramowania służących do ochrony przed ewoluującymi zagrożeniami cybernetycznymi oraz stosowania solidnych praktyk bezpieczeństwa w zarządzaniu projektami i zasobami w celu poprawy ogólnych wskaźników bezpieczeństwa i kontroli jakości w swoich organizacjach.	Do wyboru przez wykładowcę z części 1.3. [Metody nauczania, np. zadania praktyczne/laboratoria, ćwiczenia praktyczne, symulowane środowiska, quizy, gry, studia przypadków itp.] z D2.3 „Struktura ścieżki kształcenia agentów zmian w zakresie cyberbezpieczeństwa w MŚP”	Oceny praktyczne
Kompetencje: Uczestnicy będą potrafili oceniać i łagodzić potencjalne zagrożenia bezpieczeństwa, skutecznie komunikować kwestie związane z cyberbezpieczeństwem oraz dokładnie zgłaszać zagrożenia i naruszenia za pośrednictwem odpowiednich kanałów w ramach swojej organizacji.	Do wyboru przez wykładowcę, z części 1.3. [Metody nauczania, np. symulowane środowiska, konkursy typu „zdobądź flagę”, 5E, CBL, CL, POGIL, PBL itp.] z D2.3 „Struktura ścieżki edukacyjnej dla agentów zmian w zakresie cyberbezpieczeństwa w MŚP”	Symulacje Zawody

Zawartość modułu: podział tematów	**Godziny pracy kontaktowej**					**Indywidualne godziny pracy i zadania**	
	Wykłady (HEI)	Konsultacje	Praktyka (HEI)	Testy	**Wszystkie**	**Praca**	**Zadania**
Zarządzanie projektami • Planowanie projektów • Określanie celów projektu • Określenie zakresu i wymagań projektu • Przygotowanie harmonogramu projektu • Narzędzia zarządzania projektami • Aktualne zagrożenia dla cyber-bezpieczeństwa (ataki DDoS, oprogramowa-nie ransomware, złośliwe oprogramowanie, phishing, ataki typu zero-day, ataki na urządzenia IoT itp. • Modelowanie zagrożeń i analiza podatności • Plany reagowania na sytuacje awaryjne i incydenty	8	0,5	3	0,5	**12**	**6**	• Zaplanuj projekt pod-noszenia świadomości w zakresie cyber-bezpieczeństwa dla pracowników MŚP. • Określ jasne cele pro-jektu podnoszenia świadomości w zakresie cyberbezpieczeństwa, aby zwiększyć zro-zumienie poten-cjalnych zagrożeń bezpieczeństwa wśród pracowników MŚP.

• Zgłaszanie zagrożeń i incydentów związanych z cyberbezpieczeństwem							• Określ zakres i wymagania projektu podnoszenia świadomości w zakresie cyberbezpieczeństwa dla pracowników MŚP, w tym tematy szkoleń i niezbędne zasoby. • Przygotuj harmonogram projektu podnoszenia świadomości w zakresie cyberbezpieczeństwa dla pracowników MŚP. • Wykorzystaj narzędzia do zarządzania projektami, aby monitorować postępy i wykorzystanie zasobów w ramach projektu podnoszenia świadomości w zakresie cyberbezpieczeństwa skierowanego do pracowników MŚP. • Zbadaj aktualne zagrożenia dla cyberbezpieczeństwa i zestaw wyniki w raporcie. • Stwórz uproszczony model zagrożeń, aby pomóc pracownikom MŚP w identyfikacji potencjalnych luk w zabezpieczeniach w ich codziennej działalności. • Znajdź i przejrzyj przykłady planów reagowania na sytuacje awaryjne i incydenty. • Jakie kroki należy rozważyć podczas przygotowywania raportu dotyczącego zgłaszania zagrożeń i incydentów związanych z cyberbezpieczeństwem? Zbadaj i podsumuj.
Zarządzanie zasobami • Zarządzanie zasobami ludzkimi (zespoły projektowe) • Świadomość bezpieczeństwa i szkolenia zespołów	8	0,5	3	0,5	**12**	**6**	• Opracuj strategię zarządzania zasobami, aby zapewnić efektywne wykorzystanie zasobów

• Zarządzanie zasobami sprzętowymi i oprogramowaniem • Narzędzia i oprogramowanie zabezpieczające • Efektywne wykorzystanie zasobów technologicznych • Budżet i alokacja zasobów							w fikcyjnej firmie z sektora MŚP. • Stwórz przykładowy plan tematyczny szkolenia z zakresu świadomości cyberbezpieczeństwa. • Przygotuj spis sprzętu i oprogramowania dla fikcyjnej firmy z sektora MŚP. • Zbadaj powszechnie stosowane narzędzia i oprogramowanie zabezpieczające. • Stwórz przykładowy budżet i plan alokacji zasobów dla hipotetycznego MŚP.
Wskaźniki bezpieczeństwa • Wskaźniki bezpieczeństwa i techniki pomiarowe • Gromadzenie danych za pomocą SIEM • Analiza wskaźników bezpieczeństwa • Monitorowanie projektu i ocena wydajności • Przegląd działań i dostosowanie projektu • Raportowanie wskaźników bezpieczeństwa	8	0,5	4	0,5	**13**	**6**	• Zbadaj wskaźniki bezpieczeństwa stosowane do oceny stanu cyberbezpieczeństwa w małych i średnich przedsiębiorstwach. • Zbadaj źródła, z których oprogramowanie SIEM pobiera logi. • Skonfiguruj i sprawdź oprogramowanie SIEM typu open source. • Przeanalizuj wskaźniki bezpieczeństwa, zbierając logi za pomocą oprogramowania SIEM. • Przedstaw wyniki analizy wskaźników bezpieczeństwa za pomocą wykresów i elementów wizualnych.
Zapewnienie jakości i kontrola jakości • Zarządzanie jakością • Standardy jakości w cyberbezpieczeństwie • Audyty zgodności i jakości • Techniki testowania i walidacji • Ocena i zalecenia dotyczące ulepszeń	8	0,5	4	0,5	**13**	**7**	• W jaki sposób należy zaplanować procesy zapewnienia jakości i kontroli jakości, aby zwiększyć skuteczność aplikacji cyberbezpieczeństwa w MŚP? Przeprowadź badania i podsumuj wyniki. • Zbadaj elementy kontroli zawarte w

							załączniku A do normy ISO/IEC 27001:2022. • Zbadaj i przedstaw, czym są techniki testowania i walidacji. • Jakie korzyści dla MŚP płyną z ciągłego przeglądu i doskonalenia procesów jakości?
Razem	**32**	**2**	**14**	**2**	**50**	**25**	

Strategia oceny	**Porównawczy procent wagowy**	**Kryteria oceny**
Test samooceny I	10	10 punktów – 96–100% poprawnych odpowiedzi. 9 punktów – 91–95% poprawnych odpowiedzi. 8 punktów – 86–90% poprawnych odpowiedzi. 7 punktów – 80–85% poprawnych odpowiedzi. 6 punktów – 70–79% poprawnych odpowiedzi. 5 punktów – 60–69% poprawnych odpowiedzi. 4 punkty – 50–59% poprawnych odpowiedzi. 3 punkty – 40–49% poprawnych odpowiedzi. 2 punkty – 30–39% poprawnych odpowiedzi. 1 punkt – 0–29% poprawnych odpowiedzi.
Test samooceny II	10	
Test samooceny III	10	
Test samooceny IV	10	
Test sprawdzający wiedzę	60	

Materiały do nauki *(Nazwisko, inicjał imienia. (Rok, miesiąc, dzień). Tytuł artykułu. Tytuł czasopisma/dziennika/gazety, numer tomu (numer wydania), numery stron całego artykułu, wydawca, adres URL)*

Lektury obowiązkowe

Lektury zalecane

https://sansorg.egnyte.com/dl/RFrVIbX2oc
https://edwps.com/wp-content/uploads/2018/04/Cyber-PMO-U.S.-Cyber-Magazine.pdf
https://healthybyte.net/cybersecurity/what-is-a-security-program-management

2. M2: ADMINISTRACJA SYSTEMÓW

Nazwa modułu	**Kod modułu**
ADMINISTRACJA SYSTEMÓW	

Wykładowca (wykładowcy)	**Instytucja lub wydział, w którym realizowany jest moduł**

Sposób realizacji	Język
Stacjonarne, online, mieszane	*Angielski, fiński, turecki, norweski, litewski, rumuński, francuski, polski, hiszpański*

Wymagania wstępne
Brak

Liczba przyznanych punktów ECTS	Obciążenie pracą studenta	Godziny zajęć kontaktowych	Indywidualne godziny pracy
3	75	50	25

Cel i efekty modułu		
Po ukończeniu tego kursu studenci będą potrafili w sposób ciągły zarządzać (identyfikować, analizować, oceniać, szacować, łagodzić) ryzykiem związanym z cyberbezpieczeństwem infrastruktur, systemów i usług ICT poprzez planowanie, stosowanie, raportowanie i komunikowanie analizy ryzyka, oceny i postępowania. Studenci poznają podstawy sieciowe, aby właściwie zarządzać urządzeniami sieciowymi, obsługiwać serwery Linux i Windows oraz zarządzać nimi i zabezpieczać je. Bardzo przydatna będzie również wiedza na temat chmury i sztucznej inteligencji w kontekście cyberbezpieczeństwa, która pozwoli im odpowiednio przyspieszyć wykonywanie zadań oraz przeprowadzać automatyzację i skalowanie. Studenci dowiedzą się również, jak wzmocnić systemy, wykrywać zagrożenia i zapewnić dostępność serwerów (akronim z triady CIA).		
Efekty kształcenia modułu	**Metody nauczania i uczenia się**	**Metody oceny**

Wiedza: Uczestnicy zdobędą wiedzę z zakresu administracji sieciami, systemów operacyjnych, podstaw sieci, narzędzi do administracji sieciami, bezpieczeństwa urządzeń sieciowych, administracji systemami Linux, administracji systemami Windows, wirtualizacji, przetwarzania w chmurze z wykorzystaniem sztucznej inteligencji do procedur sieciowych i cyberbezpieczeństwa, procedur cyberbezpieczeństwa, wykrywania zagrożeń, analizy zagrożeń, reagowania na zagrożenia, usuwania zagrożeń, podstaw cyberbezpieczeństwa, ochrony organizacji przed atakami, bezpieczeństwa infrastruktury i sieci, monitorowania i analizy sieci oraz postępowania w przypadku incydentów. Będą potrafili ustanowić i opisać skuteczne procedury administrowania systemami oraz procedury operacyjne dostosowane do konkretnych potrzeb miejsc pracy w MŚP zgodnie z normami zgodności.	Wybrane przez wykładowcę: zajęcia na żywo, nagrania wideo, prezentacje, urządzenia wirtualne (jeśli dotyczy), analiza literatury, prelegenci gościnni, nauczanie i uczenie się między rówieśnikami, mentoring.	Testy samooceny i testy sprawdzające wiedzę.
Umiejętności: Uczestnicy zdobędą umiejętności korzystania z metodologii i narzędzi do projektowania i wdrażania bezpiecznych architektur systemowych, w tym systemów operacyjnych, baz danych, sieci i infrastruktur chmurowych dla miejsc pracy w małych i średnich przedsiębiorstwach.	Do wyboru przez wykładowcę: zajęcia na żywo, nagrania wideo, prezentacje, urządzenia wirtualne (jeśli dotyczy), analiza literatury, prelegenci gościnni, nauczanie i uczenie się między rówieśnikami, mentoring.	Testy samooceny i testy sprawdzające wiedzę
Kompetencje: Uczestnicy kursu zdobędą kompetencje w zakresie opracowywania i wdrażania strategicznych ram cyberbezpieczeństwa dla administracji systemowej, kierowania projektami i zespołami w celu zwiększenia odporności i dostępności systemów oraz podejmowania etycznych decyzji dotyczących utrzymania solidnych praktyk w zakresie cyberbezpieczeństwa w różnych obszarach administracyjnych w miejscach pracy w małych i średnich przedsiębiorstwach.	Do wyboru przez wykładowcę: zajęcia na żywo, nagrania wideo, prezentacje, urządzenia wirtualne (jeśli dotyczy), analiza literatury, prelegenci gościnni, nauczanie i uczenie się między rówieśnikami, mentoring.	Testy samooceny i testy sprawdzające wiedzę

Treść modułu: podział tematów	Godziny pracy kontaktowej					Indywidualne godziny pracy i zadania	
	Wykłady (HEI)	Konsultacje	Ćwiczenia (HEI)	Testy	**Wszystkie**	**Praca indywidualna**	**Zadania**
Administracja systemem operacyjnym • Systemy operacyjne • Związek między sprzętem a oprogramowaniem • Pliki binarne, liczenie szesnastkowe • Bity i bajty • Wiersz poleceń w systemie operacyjnym • Polecenia systemu Windows i Linux • Klient i serwer Windows • Aplikacje, procesy i usługi w systemie Windows • Rozszerzenia i typy plików • Klucze i wartości rejestru • Ustawienia panelu sterowania • Użytkownicy i grupy • Struktura domeny i menedżer serwera • AD i GPO • Interfejsy i jądro systemu Linux • Procesy w systemie Linux • Konwencje nazewnictwa plików i katalogów • Powłoki systemu Linux i składnia poleceń • Manipulowanie plikami i folderami • Praca z poleceniami monitorowania systemu i potokami • Zarządzanie procesami i kontrolą zadań • Zarządzanie usługami	4	0,5	2	0,5	**7**	**3,5**	Liczenie szesnastkowe Ćwiczenie poleceń systemu Windows Ćwiczenie poleceń systemu Linux Ćwiczenie korzystania z Menedżera zadań Tworzenie plików i zarządzanie nimi Modyfikowanie i przeglądanie kluczy i wartości rejestru Modyfikowanie ustawień Panelu sterowania Zarządzanie użytkownikami i grupami Zarządzanie strukturą domeny Tworzenie i usuwanie obiektów usługi Active Directory Zarządzanie procesami w systemie Linux Manipulowanie plikami i folderami Praca z potokami Polecenia monitorowania systemu Zarządzanie usługami systemu Linux
Administracja systemem baz danych • Repozytoria i listy źródeł • Zarządzanie serwerem WWW	4	0,5	2	0,5	**7**	**3,5**	Zarządzanie repozytoriami i listami źródeł

• Dzienniki systemowe i monitorowanie dzienników • Planowanie zadań w systemie Linux • Rozwiązywanie problemów z serwerem i siecią • Kopia zapasowa i odzyskiwanie • Zabezpieczanie GRUB • Zapory sieciowe • Zarządzanie obiektami Active Directory i obiektami GPO • DNS i DHCP • Podstawy PowerShell • Microsoft BitLocker, AppLocker i zapora sieciowa • LDAP i Kerberos • NTLM • Zasady dotyczące haseł i blokowania • Uwierzytelnianie i kontrola dostępu • Protokół ICMP (Internet Control Message Protocol) • TCP a UDP • NetBIOS i SMB • SSL i TLS • Certyfikaty • Protokoły Telnet i Secure Shell (SSH) • HTTP i HTTPS • Protokoły systemów pocztowych • Protokół systemu nazw domenowych (DNS) • FTP i RDP • Kapsułkowanie a dekapitulacja • Sniffery sieciowe i Wireshark • TCP/UDP • DHCP, DNS							Zarządzanie serwerem WWW Weryfikacja i zarządzanie logami systemowymi oraz monitorowanie logów Planowanie zadań w systemie Linux Rozwiązywanie problemów z serwerem Przywracanie kopii zapasowych Zabezpieczanie GRUB Zarządzanie usługami baz danych Konfigurowanie zasad dotyczących haseł Konfigurowanie zasad blokowania kont Konfigurowanie uwierzytelniania i kontroli dostępu
Administracja siecią • Typy sieci i sieci bezprzewodowe • Sieci i topologie • Tożsamość urządzeń i urządzenia dostępowe • Infrastruktura i urządzenia zabezpieczające • Urządzenia specjalistyczne i architektura sieci • Sieci wirtualne • Adresy fizyczne i logiczne • Modele OSI i sieci • Kapsułkowanie i dekapsułkowanie danych	4	0,5	2	0,5	**7**	**3,5**	Tworzenie topologii sieci Zarządzanie urządzeniami sieciowymi Budowanie sieci Zabezpieczanie urządzeń sieciowych Tworzenie sieci wirtualnych Konfigurowanie protokołów sieciowych i numerów portów Praca z Cisco Packet Tracer

• Protokoły sieciowe i numery portów • Nośniki sieciowe i kable • Technologie bezprzewodowe • Narzędzia do administrowania siecią • Cisco Packet Tracer • Klasy sieciowe i podsieci • Protokół rozdzielania adresów (ARP) • Adresowanie statyczne a dynamiczne • Translacja adresów sieciowych (NAT) • Przełączniki i Cisco IOS • Zabezpieczenia portów przełączników i interfejsy routerów • Konfiguracja sieci VLAN i DTP • Routing między sieciami VLAN • Wprowadzenie do list ACL • Rozwiązywanie problemów sieciowych							Praca z protokołem rozdzielania adresów (ARP) Planowanie sieci Konfigurowanie statycznego i dynamicznego adresowania IP Konfigurowanie DHCP i NAT Praca z Cisco IOS Konfigurowanie sieci VLAN Rozwiązywanie problemów sieciowych
Administracja chmurą • Hypervisory i maszyny wirtualne • Kontenery • Zabezpieczanie środowisk wirtualnych • Kopia zapasowa i odzyskiwanie • Przetwarzanie w chmurze i dostawcy usług chmurowych • Czym są modele usług w chmurze • Rodzaje wdrożeń chmury • Sieci wirtualne • Usługi obliczeniowe AWS • Amazon Elastic Compute Cloud (EC2) • Narzędzia do monitorowania chmury • Narzędzia do automatyzacji i koordynacji • Zagrożenia i luki w zabezpieczeniach chmury • Zarządzanie tożsamością i dostępem (IAM) • Kontrola dostępu oparta na rolach (RBAC) • Uwierzytelnianie wieloskładnikowe (MFA) • Szyfrowanie danych w chmurze • Wirtualna chmura prywatna (VPC) • Docker i Kubernetes	4	0,5	2	0,5	**7**	**3,5**	Tworzenie maszyn wirtualnych Konfigurowanie kontenerów Zabezpieczanie środowisk wirtualnych Praca z kopiami zapasowymi Zarządzanie siecią w chmurze Konfigurowanie sieci wirtualnych Praca z narzędziami do monitorowania chmury Wdrażanie automatyzacji i koordynacji Wykrywanie zagrożeń i luk w zabezpieczeniach chmury Konfigurowanie zarządzania tożsamością i dostępem (IAM) Wdrażanie szyfrowania danych w chmurze Praca z Dockerem i Kubernetes

Administracja systemami cyberfizycznymi • Kontrola bezpieczeństwa i dostępu • Rodzaje uwierzytelniania • TACACS+ i RADIUS • Konfiguracja AAA • Cele zarządzania ryzykiem • Szyfrowanie i deszyfrowanie • Hashowanie i tabele tęczy • Spoofing adresów MAC i zatruwanie ARP • Skakanie po sieciach VLAN i nieautoryzowane DHCP • Flood ICMP • Flooding TCP i UDP • Przejęcie sesji • Spoofing DNS • Obrona w głębi (DID) i Zero Trust • Strefy zdemilitaryzowane (DMZ) • Honeypoty i wzmocnienie sieci • Najlepsze praktyki dotyczące bezpiecznej sieci • VPN • SSH i VNC • Zapory stanowe a zapory bezstanowe • Zapory oparte na hoście a zapory oparte na sieci • Zapory sprzętowe a zapory programowe • Zapora sieciowa aplikacji internetowych (WAF) • Sztuczna inteligencja w zaporach sieciowych • IDS i IPS • NIDS i HIDS • Snort • tcpdump	4	0,5	2	0,5	**7**	**3,5**	Konfiguracja infrastruktury Główne komponenty Wdrażanie zabezpieczeń Praca z TACACS+ i RADIUS Konfiguracja AAA Korzystanie z szyfrowania i deszyfrowania Analiza typowych ataków i technik obronnych Konfiguracja stref zdemilitaryzowanych (DMZ) Badanie honeypotów Wzmacnianie bezpieczeństwa poprzez najlepsze praktyki dla bezpiecznej sieci Instalowanie VPN Praca z Secure Shell (SSH) Praca z Virtual Network Computing (VNC) Techniki pracy z zaporą ogniową Wdrażanie sztucznej inteligencji w zaporach sieciowych Wykorzystanie Snort i tcpdump do ochrony i wykrywania
Wzmocnienie systemu • Techniki GenAI • Generowanie kodu • Zarządzanie kontami użytkowników i kontrola dostępu • Wykrywanie anomalii i rozwiązywanie problemów • Rozwiązywanie błędów usługi Apache2 • Zarządzanie poprawkami i aktualizacjami • Automatyczne tworzenie kopii zapasowych i odzyskiwanie danych	4	0,5	2	0,5	**7**	**3,5**	Praca z technikami GenAI Zarządzanie kontami użytkowników i kontrola dostępu Wykrywanie anomalii i rozwiązywanie problemów Rozwiązywanie błędów usługi Apache2 za pomocą GenAI Konfigurowanie zarządzania poprawkami i aktualizacjami

• Zarządzanie zasobami IT i inwentaryzacja • Odzyskiwanie usuniętych plików za pomocą GenAI • Procedury bezpieczeństwa cybernetycznego • Wykrywanie i analiza zagrożeń • Reagowanie na zagrożenia i usuwanie skutków • Wykorzystanie sztucznej inteligencji do wykrywania zagrożeń w czasie rzeczywistym • Weryfikacja i testowanie modeli GenAI • Ramy zarządzania i regulacji • Konfiguracja i bezpieczeństwo DNS • Konfiguracja i bezpieczeństwo DHCP • Podstawy PowerShell • Zabezpieczenia portów przełączników • System podstawowych operacji wejścia/wyjścia sieci (NetBIOS) • Protokół SMB (Server Message Block) • Protokół SSL (Secure Sockets Layer) i TLS (Transport Layer Security) • Certyfikaty bezpieczeństwa • Protokoły systemów pocztowych • Protokół systemu nazw domenowych (DNS) • Protokół transferu plików (FTP) • Protokół zdalnego pulpitu (RDP) • Planowanie zadań w systemie Linux • Rozwiązywanie problemów z serwerem • Rozwiązywanie problemów z siecią • Tworzenie kopii zapasowych i odzyskiwanie danych • Zabezpieczanie GRUB • Konfiguracja i zabezpieczanie zapór sieciowych							Konfiguracja automatycznego tworzenia kopii zapasowych i odzyskiwania danych Zarządzanie zasobami IT Odzyskiwanie usuniętych plików za pomocą GenAI Wdrażanie zabezpieczeń DNS i DHCP Praca z Microsoft BitLocker i Microsoft AppLocker Konfiguracja zapory Microsoft Firewall Konfigurowanie zabezpieczeń portów przełącznika Zabezpieczanie protokołu FTP Zabezpieczanie protokołu zdalnego pulpitu (RDP) Planowanie zadań związanych z bezpieczeństwem w systemie Linux Zabezpieczanie programu GRUB Konfiguracja i zabezpieczenie zapór sieciowych (iptables)
Dostępność • IR a SOC • Zdarzenia i incydenty • Wykrywanie alertów i ich klasyfikacja • Dokumentacja i raportowanie • Czym są ataki internetowe?	4	0,5	3	0,5	**8**	4	Wykrywanie zdarzeń i incydentów Przeprowadzanie selekcji alertów Sporządzanie dokumentacji i odpowiednich raportów

• DoS i DDoS • Wstrzyknięcie kodu SQL i XSS • Wstrzyknięcie poleceń i lokalne włączenie plików (LFI) • Cross-Site Request Forgery (CSRF) • Brute-Force i Credential Stuffing • Przekazywanie skrótu i przekazywanie biletu • Rozpoznanie LDAP • Uszkodzona kontrola dostępu • Oprogramowanie ransomware • Wirusy komputerowe i robaki • Trojan i oprogramowanie reklamowe • Keylogger i kryptojacking • Złośliwe oprogramowanie bezplikowe • Zrozumienie rozprzestrzeniania się złośliwego oprogramowania • Statyczna i dynamiczna analiza złośliwego oprogramowania • Bezpieczna analiza złośliwego oprogramowania • Analiza hybrydowa Badanie złośliwego oprogramowania • Przeprowadzanie statycznej i dynamicznej analizy złośliwego oprogramowania • Zarządzanie wskaźnikami IOC i zasadami dotyczącymi haseł • Zasady dopuszczalnego użytkowania (AUP) • Zasady dotyczące korzystania z własnych urządzeń (BYOD) • Zasady dotyczące zdalnego dostępu							Wdrażanie działań po incydencie Wykonanie i ochrona przed atakami DoS i DDoS Wykrywanie ataków internetowych i rozprzestrzeniania się złośliwego oprogramowania Przeprowadzanie bezpiecznej statycznej i dynamicznej analizy złośliwego oprogramowania Zarządzanie wskaźnikami IOC Konfigurowanie zasad dotyczących haseł Konfigurowanie zasad dotyczących korzystania z własnych urządzeń (BYOD) Konfigurowanie zasad zdalnego dostępu
Całkowita	**28**	**3,5**	**15**	**3,5**	**50**	**25**	

Strategia oceny	**Porównawczy procent wagowy**	**Kryteria oceny**
Test samooceny (1)	5%	10 punktów – 90–100% poprawnych odpowiedzi. 9 punktów – 80–90% poprawnych odpowiedzi. 8 punktów – 70–80% poprawnych odpowiedzi. 7 punktów – 60–70% poprawnych odpowiedzi. 6 punktów – 50–60% poprawnych odpowiedzi. 5 punktów – 50–60% poprawnych odpowiedzi. 4 punkty – 40–50% poprawnych odpowiedzi. 3 punkty – 30–40% poprawnych odpowiedzi. 2 punkty – 20–30% poprawnych odpowiedzi.
Test samooceny (2)	5%	
Test samooceny (3)	5%	
Test samooceny (4)	5	
Test samooceny (5)	5	
Test samooceny (6)	5	
Test samooceny (7)	5	
Test sprawdzający wiedzę	65%	

		1 punkt – 10–20% poprawnych odpowiedzi.

3. M3: NARZĘDZIA ANALITYCZNE

Nazwa modułu	Kod modułu
NARZĘDZIA ANALITYCZNE	

Wykładowca (wykładowcy)	Instytucja lub wydział, na którym realizowany jest moduł

Sposób realizacji	Język
Stacjonarne, online, hybrydowe	*Angielski, fiński, turecki, norweski, litewski, rumuński, francuski, polski, hiszpański*

Wymagania wstępne
Brak

Liczba przyznanych punktów ECTS	Obciążenie pracą studenta	Godziny zajęć kontaktowych	Indywidualne godziny pracy
3	75	50	25

Cel i efekty modułu		
Po ukończeniu tego kursu studenci będą dysponować umiejętnościami niezbędnymi do ochrony zasobów organizacji przy użyciu wskaźników wydajności, analizy danych i informacji dotyczących bezpieczeństwa. Nauczą się skutecznie stosować narzędzia analityczne w celu identyfikacji potencjalnych zagrożeń i słabych punktów w zakresie cyberbezpieczeństwa, wykorzystywać wnioski oparte na danych do ulepszania środków bezpieczeństwa oraz stosować wskaźniki wydajności związane z hasłami, korzystaniem z przeglądarek, pocztą elektroniczną i aplikacjami do przetwarzania danych. Pod koniec modułu uczestnicy będą potrafili oceniać i ograniczać potencjalne zagrożenia bezpieczeństwa przy użyciu odpowiednich narzędzi oraz zgłaszać wszelkie zagrożenia lub zakłócenia do właściwych organów regulacyjnych.		
Efekty uczenia się modułu	**Metody nauczania i uczenia się**	**Metody oceny**

Wiedza: Uczestnicy zdobędą praktyczną wiedzę na temat stosowania pomiarów wydajności, analizy danych i informacji dotyczących bezpieczeństwa w celu ochrony zasobów organizacji.	Wybrane przez wykładowcę z części 1.3. [Metody nauczania, np. wykłady teoretyczne, prelegenci zewnętrzni, quizy, gry, zadania praktyczne/laboratoria, nauczanie i uczenie się między rówieśnikami, samokształcenie itp.] z D2.3 „Struktura ścieżki edukacyjnej dla agentów zmian w zakresie cyberbezpieczeństwa w MŚP".	Testy samooceny Test sprawdzający wiedzę
Umiejętności: Uczestnicy kursu nabędą umiejętności korzystania z narzędzi analitycznych w celu identyfikacji potencjalnych zagrożeń i słabych punktów w zakresie cyberbezpieczeństwa, stosowania wniosków opartych na danych w celu wzmocnienia praktyk cyberbezpieczeństwa oraz wykorzystywania wskaźników wydajności do oceny i poprawy bezpieczeństwa haseł, przeglądania stron internetowych, poczty elektronicznej i przetwarzania danych.	Do wyboru przez wykładowcę z części 1.3. [Metody nauczania, np. zadania praktyczne/laboratoria, ćwiczenia praktyczne, symulowane środowiska, quizy, gry, studia przypadków itp.] z D2.3 „Struktura ścieżki kształcenia agentów zmian w zakresie cyberbezpieczeństwa w MŚP".	Oceny praktyczne
Kompetencje: Uczniowie będą potrafili oceniać i łagodzić potencjalne zagrożenia bezpieczeństwa za pomocą narzędzi analitycznych, dokładnie zgłaszając zagrożenia i naruszenia odpowiednim kanałom w swojej organizacji.	Do wyboru przez wykładowcę, z części 1.3. [Metody nauczania, np. symulowane środowiska, konkursy typu „zdobądź flagę", 5E, CBL, CL, POGIL, PBL itp.] z D2.3 „Struktura ścieżki kształcenia agentów zmian w zakresie cyberbezpieczeństwa w MŚP"	Symulacje Zawody

Zawartość modułu: podział tematów	**Godziny pracy kontaktowej**	**Indywidualne godziny pracy i zadania**

	Wykłady (HEI)	Konsultacje	Praktyka (HEI)	Testy	**Wszystkie prace**	**Praca indywidualna**	**Zadania**
Pomiar wydajności (wskaźniki) • Metryki wydajności • Monitorowanie systemu i sieci • Monitorowanie wskaźników wydajności • Mapowanie sieci • Skanowanie podatności • Analiza ruchu sieciowego	10	0,5	5	0,5	**16**	**8,5**	• Przeprowadź badania dotyczące wskaźników wydajności i narzędzi. Porównaj narzędzia do monitorowania wydajności i określ ich różnice. • Zakończ instalację Zabbix i przeprowadź podstawową konfigurację. • Stworzyć aplikację do monitorowania wskaźników wydajności za pomocą Zabbix. • Zidentyfikuj luki w zabezpieczeniach systemu docelowego za pomocą oprogramowania do mapowania sieci (takiego jak nmap, rustscan itp.). • Przeprowadzić skanowanie podatności w systemie docelowym przy użyciu oprogramowania Nessus. Przygotować raport z testów podatności. • Przeprowadź analizę ruchu sieciowego przy użyciu Wireshark.
Analiza danych • Gromadzenie danych • Czyszczenie i wstępne przetwarzanie danych • Analiza danych • Wizualizacja danych • Narzędzia analityczne • Zastosowania analizy danych w cyberbezpieczeństwie	10	0,5	5	0,5	**16**	**8,5**	• Przeprowadź czyszczenie danych i przetwarzanie wstępne zbioru danych związanych z kwestiami cyberbezpieczeństwa przygotowanego dla hipotetycznego MŚP. • Przeanalizuj oczyszczony i wstępnie przetworzony zbiór danych z hipotetycznego MŚP i zwizualizuj wyniki. • Jakie są przykłady zastosowań analizy danych w cyberbezpieczeństwie?

							Proszę poszukać informacji.
Wywiad bezpieczeństwa • Zrozumienie wywiadu bezpieczeństwa • Źródła wywiadu bezpieczeństwa • Metody gromadzenia danych wywiadowczych dotyczących zagrożeń • Struktury wywiadu zagrożeń • Platformy wywiadu bezpieczeństwa oparte na sztucznej inteligencji • Studia przypadków dotyczące zastosowań wywiadu bezpieczeństwa	10	0,5	7	0,5	**18**	**8**	• Zbadaj, w jaki sposób wywiad bezpieczeństwa przyczynia się do proaktywnych strategii bezpieczeństwa małych i średnich przedsiębiorstw. • Jakie są najczęstsze źródła pozyskiwania informacji dotyczących bezpieczeństwa? Jak ocenia się wiarygodność tych źródeł? • Określ zalety i ograniczenia każdej metody gromadzenia informacji wywiadowczych dotyczących zagrożeń. • Wyjaśnij podstawowe cechy struktur wywiadu zagrożeń, takich jak MITRE ATT&CK i Cyber Kill Chain. • Przeanalizuj prawdziwe studium przypadku, w którym wykorzystano dane wywiadowcze dotyczące bezpieczeństwa. Opisz metody gromadzenia danych wywiadowczych zastosowane w tym studium przypadku.
Razem	**30**	**1,5**	**17**	**1,5**	**50**	**25**	

Strategia oceny	Porównawczy procent wagowy	Kryteria oceny
Test samooceny I	15	10 punktów – 96–100% poprawnych odpowiedzi. 9 punktów – 91–95% poprawnych odpowiedzi. 8 punktów – 86–90% poprawnych odpowiedzi. 7 punktów – 80–85% poprawnych odpowiedzi. 6 punktów – 70–79% poprawnych odpowiedzi. 5 punktów – 60–69% poprawnych odpowiedzi. 4 punkty – 50–59% poprawnych odpowiedzi. 3 punkty – 40–49% poprawnych odpowiedzi. 2 punkty – 30–39% poprawnych odpowiedzi. 1 punkt – 0–29% poprawnych odpowiedzi.
Test samooceny II	15	
Test samooceny III	15	
Test sprawdzający wiedzę	55	

Materiały do nauki *(Nazwisko, inicjał imienia. (Rok, miesiąc, dzień). Tytuł artykułu. Tytuł czasopisma/dziennika/gazety, numer tomu (numer wydania), numery stron całego artykułu, wydawca, adres URL)*
Lektura obowiązkowa
…
Lektura zalecana
https://brainstation.io/career-guides/what-tools-do-cybersecurity-analysts-use **https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it** **https://medium.com/@jcm3/wireshark-traffic-analysis-part-1-tryhackme-walkthrough-a9bec11d94d9** **https://www.kali.org/tools/nmap/** **https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/** **https://www.varonis.com/blog/cyber-kill-chain** **https://www.youtube.com/watch?v=kVnvIBNiC58**

4. M4: OPERACJE BEZPIECZEŃSTWA

Nazwa modułu	Kod modułu
OPERACJE BEZPIECZEŃSTWA	

Wykładowca (wykładowcy)	Instytucja lub wydział, w którym realizowany jest moduł

Sposób realizacji	Język
Stacjonarne, online, mieszane, konsultacje	*Angielski, fiński, turecki, norweski, litewski, rumuński, francuski, polski, hiszpański*

Wymagania wstępne
Brak

Liczba przyznanych punktów ECTS	Obciążenie pracą studenta	Godziny zajęć kontaktowych	Indywidualne godziny pracy
3	75	50	25

Cel i efekty modułu

Po ukończeniu tego kursu studenci będą potrafili skutecznie zarządzać operacjami bezpieczeństwa w ramach infrastruktur, systemów i usług ICT. Zdobędą umiejętności monitorowania, wykrywania, reagowania i usuwania skutków incydentów związanych z cyberbezpieczeństwem poprzez stosowanie najlepszych praktyk, narzędzi i ram odpowiednich dla operacji bezpieczeństwa.

Efekty kształcenia modułu	Metody nauczania i uczenia się	Metody oceny
Wiedza: Uczestnicy zdobędą zaawansowaną wiedzę na temat operacji związanych z bezpieczeństwem, w tym monitorowania, wykrywania, reagowania na incydenty i przywracania sprawności. Będą potrafili ustanowić i opisać skuteczne procedury operacyjne w zakresie cyberbezpieczeństwa dostosowane do konkretnych potrzeb miejsc pracy w MŚP zgodnie z normami cyberbezpieczeństwa.	Do wyboru przez wykładowcę, z części 1.3. [Metody nauczania, np. wykłady teoretyczne, analiza literatury, prelegenci zewnętrzni, nauczanie i uczenie się między rówieśnikami, mentoring itp.	Testy samooceny Test sprawdzający wiedzę

Umiejętności: Uczestnicy zdobędą umiejętności w zakresie stosowania zaawansowanych metodologii i narzędzi do wykonywania zadań związanych z bezpieczeństwem, projektowania i wdrażania skutecznych strategii monitorowania, reagowania na incydenty oraz opracowywania solidnych procedur operacyjnych dostosowanych do potrzeb małych i średnich przedsiębiorstw.	Wybrane przez wykładowcę z części 1.3. [*Metody nauczania, np. wykłady teoretyczne, analiza literatury, prelegenci zewnętrzni, nauczanie i uczenie się między rówieśnikami, mentoring itp.]* z D2.3 *„Struktura ścieżki edukacyjnej dla agentów zmian w zakresie cyberbezpieczeństwa w MŚP*".	Testy samooceny Test sprawdzający wiedzę
Kompetencje: Uczestnicy będą potrafili opracowywać i wdrażać strategiczne polityki i procedury dotyczące bezpieczeństwa w miejscach pracy w MŚP.	Do wyboru przez wykładowcę, z części 1.3. [*Metody nauczania, np. wykłady teoretyczne, analiza literatury, prelegenci gościnni, nauczanie i uczenie się między rówieśnikami, mentoring itp.]* z D2.3 *„Struktura ścieżki kształcenia agentów zmian w zakresie cyberbezpieczeństwa w MŚP*".	Testy samooceny Test sprawdzający wiedzę

Zawartość modułu: podział tematów	**Godziny pracy kontaktowej**					**Indywidualne godziny pracy i zadania**	
	Wykłady (HEI)	Konsultacje	Ćwiczenia praktyczne	Testy	Wszystkie	Praca indywidualna	Zadania

Podstawy operacji bezpieczeństwa - Zrozumienie operacji bezpieczeństwa i SOC (centrum operacji bezpieczeństwa) - Role i obowiązki w operacjach bezpieczeństwa - Przegląd narzędzi i technologii związanych z operacjami bezpieczeństwa	6	0,5	2	0,5	**9**	6	Rozpoznawanie i zrozumienie struktury i funkcji SOC, analiza różnych ról w ramach operacji bezpieczeństwa, badanie narzędzi wykorzystywanych w operacjach bezpieczeństwa oraz analiza studium przypadku.
Konwergencja bezpieczeństwa - Zrozumienie konwergencji bezpieczeństwa - Podstawy bezpieczeństwa fizycznego (zasady bezpieczeństwa fizycznego, ochrona aktywów fizycznych, polityki) - Studium przypadku podkreślające zasady konwergencji bezpieczeństwa	8	0,5	4	0,5	**13**	6	Przejrzyj definicję i zasady konwergencji bezpieczeństwa, uznaj znaczenie integracji fizycznych i cyfrowych operacji bezpieczeństwa, zidentyfikuj i oceń ryzyko w domenach cybernetycznych i fizycznych.

Zarządzanie informacjami i zdarzeniami dotyczącymi bezpieczeństwa - Przegląd zasad monitorowania bezpieczeństwa - Wdrażanie rozwiązań SIEM	8	0,5	4	0,5	**13**	6	Wprowadzenie do monitorowania bezpieczeństwa i wdrażania SIEM. Podstawowe zasady, takie jak typy logów, metody wykrywania i cykl życia monitorowania. Praktyczne aspekty wdrażania SIEM, w tym architektura, gromadzenie danych, tworzenie reguł i zarządzanie alertami.
Praktyki w zakresie operacji bezpieczeństwa - Identyfikacja źródeł danych i optymalizacja gromadzenia logów - Centralizacja alertów za pomocą SIEM - Testowanie systemu SIEM	4	0,5	10	0,5	**15**	7	Kompleksowy i zorientowany na praktykę program szkoleniowy obejmujący niezbędną wiedzę i praktyczne umiejętności w zakresie zarządzania logami, konfiguracji SIEM oraz wykrywania zagrożeń w różnych środowiskach IT.
Razem	**26**	**2**	**20**	**2**	**50**	**25**	

Strategia oceny	**Porównawczy procent wagowy**	**Kryteria oceny**
Test samooceny (1)	10%	10 punktów – 96–100% poprawnych odpowiedzi. 9 punktów – 91–95% poprawnych odpowiedzi. 8 punktów – 86–90% poprawnych odpowiedzi. 7 punktów – 80–85% poprawnych odpowiedzi. 6 punktów – 70–79% poprawnych odpowiedzi. 5 punktów – 60–69% poprawnych odpowiedzi. 4 punkty – 50–59% poprawnych odpowiedzi. 3 punkty – 40–49% poprawnych odpowiedzi. 2 punkty – 30–39% poprawnych odpowiedzi. 1 punkt – 0–29% poprawnych odpowiedzi.
Test samooceny (2)	10%	
Test samooceny (3)	10%	
Test samooceny (4)	10%	
Test sprawdzający wiedzę	60%	

Certyfikacja HEI/VET -> Test samodzielny I + ...+ Test samodzielny n + Test sprawdzający wiedzę
Certyfikacja MŚP/samokształcenie -> Samokontrola I + ...+ Samokontrola n + Test sprawdzający wiedzę
Mikromoduły, mikrosekcje -> Samokontrola I (opcjonalnie), Samokontrola n (opcjonalnie)

Materiały do nauki *(Nazwisko, inicjał imienia. (Rok, miesiąc, dzień). Tytuł artykułu. Tytuł czasopisma/dziennika/gazety, numer tomu (numer wydania), numery stron całego artykułu, wydawca, adres URL)*
Lektura obowiązkowa
Cybellium (2024). *Przewodnik po centrach operacji bezpieczeństwa (SOC): Kompleksowy przewodnik po centrach operacji bezpieczeństwa (SOC)* Muniz, J. (2021). *Nowoczesne centrum operacji bezpieczeństwa*. Pearson Education. ENISA (2017). *Strategie reagowania na incydenty i współpracy w zakresie cyberkryzysów*. **Strategie reagowania na incydenty i współpracy w zakresie cyberkryzysów — ENISA (europa.eu)**
Lektura zalecana
Basta, A., Basta, N., Anwar, W., Essar, M. I. (2024). Centrum operacji bezpieczeństwa typu open source (SOC): Kompletny przewodnik po tworzeniu, zarządzaniu i utrzymywaniu nowoczesnego SOC. Cybellium (2023). Zarządzanie centrum operacji bezpieczeństwa (SOC).

5. M5: ZARZĄDZANIE BEZPIECZEŃSTWEM I POLITYKA BEZPIECZEŃSTWA

Tytuł modułu	Kod modułu
ZARZĄDZANIE BEZPIECZEŃSTWEM I POLITYKA BEZPIECZEŃSTWA	

Wykładowca (wykładowcy)	Instytucja lub wydział, na którym realizowany jest moduł

Sposób realizacji	Język
Stacjonarne / Online / Hybrydowe	*Angielski, fiński, turecki, norweski, litewski, rumuński, francuski, polski, hiszpański*

Wymagania wstępne
Brak

Liczba przyznanych punktów ECTS	Obciążenie pracą studenta	Godziny zajęć kontaktowych	Indywidualne godziny pracy
3	75	50	25

Cel i efekty modułu
Przedmiot „Zarządzanie bezpieczeństwem i polityka bezpieczeństwa” ma na celu przygotowanie studentów do stawiania czoła wyzwaniom związanym z cyberbezpieczeństwem w małych i średnich przedsiębiorstwach, integrując zarządzanie bezpieczeństwem ze strategią biznesową i zapewniając zgodność z przepisami prawnymi, takimi jak RODO. Moduł obejmuje takie aspekty, jak identyfikacja zagrożeń i słabych punktów, projektowanie solidnych i elastycznych polityk bezpieczeństwa oraz skuteczne zarządzanie incydentami. Ponadto koncentruje się na opracowywaniu struktur zarządzania, które przypisują jasne role w organizacji, dostosowując cyberbezpieczeństwo do celów strategicznych. Studenci zdobędą kompetencje techniczne w zakresie oceny i ograniczania ryzyka cybernetycznego oraz rozwiną umiejętności analityczne, aby proponować ulepszenia w zakresie dojrzałości bezpieczeństwa. Zdobędą również umiejętności skutecznego komunikowania potrzeb w zakresie cyberbezpieczeństwa kadrze kierowniczej, wspierając podejmowanie świadomych decyzji oraz zapewniając zgodność z przepisami i etyką w zakresie cyberbezpieczeństwa. Moduł „Zarządzanie bezpieczeństwem i polityka bezpieczeństwa” obejmuje również szczegółową analizę zapobiegania phishingowi, cyberataków opartych na sztucznej inteligencji oraz zarządzania oprogramowaniem ransomware, analizując, w jaki sposób te konkretne zagrożenia wymagają zintegrowanego podejścia do zarządzania i zgodności z przepisami. Skuteczność polityk bezpieczeństwa będzie mierzona nie tylko pod kątem ich zdolności do zapobiegania incydentom, ale także pod kątem ich zdolności do dostosowywania się do pojawiających się zagrożeń i zgodności z obowiązującymi przepisami prawnymi.

Efekty kształcenia modułu	Metody nauczania i uczenia się	Metody oceny
Wiedza: Uczestnicy zdobędą zaawansowaną wiedzę na temat wdrażania nowych procedur i procesów związanych z cyberbezpieczeństwem w miejscach pracy w małych i średnich przedsiębiorstwach, uwzględniając aktualne zasady cyberbezpieczeństwa, trendy oraz zgodność z krajowymi i międzynarodowymi przepisami dotyczącymi ich branży. Zdobycie zaawansowanej wiedzy na temat integracji zabezpieczeń przed phishingiem, zarządzania zagrożeniami związanymi ze sztuczną inteligencją oraz reagowania na oprogramowanie ransomware w środowiskach MŚP.	**Wykłady (czytania kierowane):** Wykłady zapewnią solidne podstawy koncepcyjne w zakresie cyberbezpieczeństwa, zarządzania, prywatności i zgodności z przepisami, zachęcając studentów do aktywnego udziału. Obejmują one interaktywne wykłady, które zawierają regularne sesje pytań i odpowiedzi, ankiety oraz ćwiczenia z rozwiązywania problemów na żywo. Wykorzystując narzędzia takie jak Mentimeter i Poll Everywhere, **Udział w dyskusjach i forach:** Udział w dyskusjach i forach pozwoli studentom debatować i krytycznie analizować kwestie związane z cyberbezpieczeństwem, rozwijając ich umiejętności argumentacyjne. Zostanie to zastosowane do kwestii związanych z etyką, polityką i podejmowaniem decyzji w zakresie cyberbezpieczeństwa. **Studia przypadków:** Studia przypadków pozwolą studentom analizować sytuacje związane z cyberbezpieczeństwem w małych i średnich przedsiębiorstwach, wykorzystując wiedzę teoretyczną do rozwiązywania rzeczywistych problemów. Skupią się one na takich tematach, jak zarządzanie naruszeniami danych, oprogramowanie ransomware, phishing, ataki oparte na sztucznej inteligencji, wdrażanie polityki bezpieczeństwa i zarządzanie.	**Testy samooceny:** Testy samooceny pozwalają studentom ocenić swoje zrozumienie każdego podtematu poprzez różnorodne pytania, zapewniając ciągłą informację zwrotną w celu zidentyfikowania obszarów wymagających poprawy. Nie mają one wpływu na ocenę końcową, ale są kluczowe dla samodzielnej nauki. **Egzamin końcowy (opcjonalny):** Egzamin końcowy jest opcjonalny i pozwala studentom uzyskać certyfikat ukończenia kursu poprzez ocenę ich ogólnego zrozumienia kursu za pomocą pytań rozwojowych, analizy przypadków i pytań wielokrotnego wyboru. Zdanie egzaminu jest wymagane do uzyskania certyfikatu ukończenia kursu, natomiast osoby, które nie przystąpią do egzaminu, otrzymają certyfikat uczestnictwa.

Umiejętności: Uczestnicy kursu zdobędą umiejętności w zakresie stosowania zaawansowanych metodologii do przeprowadzania ocen ryzyka, projektowania i wdrażania nowych procedur bezpieczeństwa cybernetycznego oraz przygotowywania strategii reagowania, zapewniając skuteczne zarządzanie i zgodność z przepisami w miejscach pracy małych i średnich przedsiębiorstw. Rozwijanie umiejętności projektowania i wdrażania kompleksowych procedur bezpieczeństwa cybernetycznego, które pozwalają przeciwdziałać zaawansowanym zagrożeniom i zapewniają zgodność z przepisami w organizacji.	**Praktyczne warsztaty:** Praktyczne warsztaty pozwolą studentom zastosować koncepcje cyberbezpieczeństwa poprzez ćwiczenia, takie jak opracowywanie polityk i symulacje incydentów, z informacją zwrotną od instruktora w czasie rzeczywistym. Warsztaty mają na celu wzmocnienie umiejętności praktycznych i przygotowanie studentów do zastosowania zdobytej wiedzy w rzeczywistych sytuacjach. **Praca praktyczna i projekty indywidualne:** Praca praktyczna i projekty indywidualne pozwolą studentom zastosować koncepcje cyberbezpieczeństwa poprzez zadania takie jak tworzenie polityk i analiza ryzyka, rozwijając umiejętności samodzielnej pracy i praktyczne zastosowanie wiedzy teoretycznej. **Projekty zespołowe:** Projekty zespołowe pozwolą studentom pracować w zespołach nad opracowaniem rozwiązań w zakresie cyberbezpieczeństwa dla MŚP, w tym polityk bezpieczeństwa i modeli zarządzania. Będą one zachęcać do pracy zespołowej, zarządzania projektami i praktycznego zastosowania zdobytej wiedzy, przy wsparciu nauczycieli i innych studentów.	**Oceny praktyczne:** Oceny praktyczne w trakcie kursu pozwolą studentom zastosować wiedzę teoretyczną w symulowanych sytuacjach, takich jak opracowywanie polityki cyberbezpieczeństwa i symulacje incydentów, w celu oceny ich zdolności do rozwiązywania rzeczywistych problemów w kontekście MŚP. **Projekty grupowe:** Projekty grupowe pozwolą studentom opracować kompleksowy projekt dotyczący cyberbezpieczeństwa, od identyfikacji ryzyka po propozycję modeli zarządzania i planów reagowania na incydenty, oceniając zarówno jakość treści, jak i umiejętność współpracy. Projekt ten ma kluczowe znaczenie dla końcowej oceny i integruje całą wiedzę zdobytą podczas kursu.
Kompetencje: Uczestnicy kursu będą kompetentni w zakresie opracowywania i wdrażania strategicznych polityk bezpieczeństwa cybernetycznego, kierowania inicjatywami mającymi na celu ustanowienie nowych procedur i przepływów pracy w miejscach pracy MŚP oraz podejmowania etycznych decyzji zgodnych z celami organizacyjnymi i wymogami zgodności. Uczestnicy zdobędą kompetencje w zakresie formułowania i wdrażania polityk cyberbezpieczeństwa, które zapobiegają zaawansowanym cyberzagrożeniom i zapewniają zgodność z międzynarodowymi przepisami dotyczącymi cyber	**Symulacje scenariuszy:** Symulacje scenariuszy pozwolą studentom zarządzać incydentami cyberbezpieczeństwa w środowiskach wirtualnych, które odzwierciedlają rzeczywiste ataki, podejmując strategiczne decyzje pod presją. Metoda ta zwiększa umiejętności w zakresie zarządzania kryzysowego i reagowania na incydenty i ma kluczowe znaczenie dla nauczania oceny polityki bezpieczeństwa i podejmowania decyzji w sytuacjach krytycznych. Studenci będą musieli wykazać, w jaki sposób zastosowaliby polityki zarządzania, aby zapobiegać konkretnym incydentom, takim jak ataki phishingowe, ransomware i ataki oparte na sztucznej inteligencji, lub reagować na nie, oceniając swoje zrozumienie odpowiednich ram regulacyjnych.	**Symulacje i zarządzanie incydentami:** Studenci będą oceniani pod kątem umiejętności zarządzania incydentami związanymi z cyberbezpieczeństwem w symulacjach odzwierciedlających rzeczywiste kryzysy w małych i średnich przedsiębiorstwach. Celem jest zmierzenie ich zdolności do radzenia sobie z presją, podejmowania strategicznych decyzji i realizacji planów reagowania w czasie rzeczywistym, oceniając ich praktyczne zastosowanie w dynamicznych sytuacjach.

Zawartość modułu: podział tematów	Godziny pracy kontaktowej					Indywidualne godziny pracy i zadania	
	Wykłady (HEI)	Konsultacje	Praktyka (HEI)	Testy	**Wszystkie**	**Praca**	**Zadania**
Kontekst organizacyjny -Ewolucja cyberbezpieczeństwa w MŚP -Aktualne główne zagrożenia i słabe punkty -Wpływ cyberbezpieczeństwa na strategię biznesową -Szczególne wyzwania związane z cyberbezpieczeństwem w MŚP w porównaniu z dużymi przedsiębiorstwami - Zrozumienie implikacji regulacyjnych praktyk w zakresie cyberbezpieczeństwa i ich zgodności ze strukturami zarządzania. - Typowe wyzwania związane z cyberbezpieczeństwem charakterystyczne dla MŚP, takie jak ograniczone budżety, brak wyspecjalizowanego personelu ds. bezpieczeństwa oraz praktyczne metody ustalania priorytetów inwestycji w cyberbezpieczeństwo.	5	0,5	3	0,5	**9**	**4**	Czytanie, badania, przygotowanie studiów przypadków
Prywatność -Zasady prywatności w cyberbezpieczeństwie -Ochrona danych osobowych i RODO -Wpływ prywatności na działalność MŚP -Narzędzia i techniki ochrony prywatności	4	0,5	3	0,5	**8**	**4**	Analiza polityki, zadanie indywidualne
Prawo, etyka i zgodność z przepisami -Organizacje, polityki i standardy dotyczące cyberbezpieczeństwa -Odpowiednie przepisy krajowe i międzynarodowe -Zgodność z przepisami w małych i średnich przedsiębiorstwach -Etyka w cyberbezpieczeństwie -Konsekwencje prawne nieprzestrzegania przepisów dotyczących cyberbezpieczeństwa - Analiza sposobów wykorzystania narzędzi opartych na sztucznej inteligencji do wzmocnienia zarządzania cyberbezpieczeństwem i zapewnienia	5	0,5	3	0,5	**9**	**5**	Studium przypadku, analiza przepisów prawnych

zgodności z przepisami poprzez ciągłe monitorowanie i automatyczne reagowanie na zagrożenia.							
Zarządzanie bezpieczeństwem -Struktura zarządzania cyberbezpieczeństwem -Role i obowiązki w zarządzaniu bezpieczeństwem -Modele dojrzałości cyberbezpieczeństwa -Włączenie cyberbezpieczeństwa do zarządzania przedsiębiorstwem - Zwiększenie umiejętności przeprowadzania ocen ryzyka i formułowania strategicznych planów reagowania w symulowanych warunkach kryzysowych (oprogramowanie ransomware, ataki phishingowe itp.)	4	0,5	3	0,5	**8**	**4**	Analiza scenariuszy zarządzania ryzykiem
Komunikacja na szczeblu kierowniczym i zarządu - Strategie komunikacji w zakresie cyberbezpieczeństwa -Raportowanie kwestii bezpieczeństwa kierownictwu wyższego szczebla -Podejmowanie decyzji w oparciu o dane dotyczące bezpieczeństwa -Zarządzanie kryzysowe i komunikacja w zakresie cyberbezpieczeństwa - Opanowanie umiejętności zarządzania kryzysowego i podejmowania decyzji w sytuacjach silnego stresu związanych z atakami opartymi na sztucznej inteligencji i oprogramowaniem ransomware.	4	0,5	3	0,5	**8**	**4**	Przygotowanie prezentacji, komunikacja z interesariuszami
Polityka zarządzania -Opracowanie polityki bezpieczeństwa -Wdrażanie i monitorowanie polityki - Ocena i ciągłe doskonalenie polityk -Dostosowanie polityki bezpieczeństwa do zmian technologicznych i regulacyjnych - Badanie, w jaki sposób skuteczne szkolenia i polityka uświadamiająca mogą stanowić kluczowy element zgodności z przepisami i ograniczania ryzyka.	4	0,5	3	0,5	**8**	**4**	Opracowanie i zmiana dokumentu dotyczącego polityki
Razem	**26**	**3**	**18**	**3**	**50**	**25**	

Strategia oceny	**Porównawczy procent wagowy**	**Kryteria oceny**
Samokontrola I	10%	Ocena podstawowych pojęć dotyczących kontekstu organizacyjnego.

Test samodzielny II	10	Ocena podstawowych pojęć dotyczących prywatności.
Test samodzielny III	10	Ocena przepisów prawnych, zasad etycznych i polityki zgodności.
Test samodzielny IV	10	Ocena zasad dotyczących cyberbezpieczeństwa.
Test samodzielny V	10	Ocena komunikacji na szczeblu kierowniczym.
Test samodzielny VI	10	Ocena polityki zarządzania i tworzenia polityki w zakresie bezpieczeństwa.
Test sprawdzający wiedzę	40	Egzamin końcowy obejmujący pytania integracyjne dotyczące wszystkich tematów kursu.
10 punktów – 96%-100%		

Materiały do nauki *(Nazwisko, inicjał imienia. (Rok, miesiąc, dzień). Tytuł artykułu. Tytuł czasopisma/dziennika/gazety, numer tomu (numer wydania), numery stron całego artykułu, wydawca, adres URL)*

Lektura obowiązkowa

...

„Prawo UE dotyczące cyberbezpieczeństwa: zarządzanie odpornością i spójnością w erze cyfrowej” autorstwa Luisy Marin

- Książka zawiera dogłębną analizę przepisów i polityk UE dotyczących cyberbezpieczeństwa, niezbędną do zrozumienia struktury i wdrażania zarządzania cyberbezpieczeństwem w kontekście UE.

„Cyberbezpieczeństwo w Unii Europejskiej: odporność i zdolność adaptacyjna w polityce zarządzania” autorstwa George'a Christou

- Książka ta analizuje ramy zarządzania i procesy tworzenia polityki w zakresie cyberbezpieczeństwa w UE, pomagając studentom zrozumieć dynamiczną interakcję między różnymi poziomami zarządzania.

„Phishing i środki zaradcze: zrozumienie narastającego problemu kradzieży tożsamości elektronicznej” autorstwa Markusa Jakobssona i Stevena Myersa

- Chociaż książka ta nie dotyczy wyłącznie UE, szczegółowe omówienie technik phishingu i środków zaradczych można odnieść do kontekstu UE, skupiając się na zgodności z RODO i zasadach ochrony danych.

„Europejskie prawo i regulacje dotyczące cyberbezpieczeństwa” pod redakcją Nadya Purtova i Bert-Jaap Koops

- Ten zbiór artykułów obejmuje środki prawne i regulacyjne dotyczące cyberbezpieczeństwa w Unii Europejskiej, w tym wyzwania związane z zapewnieniem zgodności z przepisami oraz ramy prawne, takie jak dyrektywa NIS i RODO.

„Ransomware: zrozumienie cyfrowego wymuszenia i zagrożenia dla Twojej organizacji” autorstwa Allana Liska i Timothy'ego Gallo

- Tekst ten, uzupełniony o studia przypadków i przykłady dotyczące UE, pomoże studentom zrozumieć konsekwencje ataków ransomware w świetle przepisów UE.

Lektury zalecane

„Ogólne rozporządzenie o ochronie danych (RODO) UE: komentarz” autorstwa Lukasa Feilera i Nikolausa Forgó

- Komentarz ten zawiera szczegółowe informacje na temat RODO, niezbędne do zrozumienia otoczenia regulacyjnego w UE i jego wpływu na praktyki w zakresie cyberbezpieczeństwa.

„Ochrona danych i cyberbezpieczeństwo w Europie: ramy prawne i praktyczne aspekty” autorstwa Paula Lamberta

- Książka ta zawiera praktyczne informacje na temat dostosowania strategii ochrony danych i cyberbezpieczeństwa w UE, w tym zgodności z przepisami i najlepszymi praktykami w zakresie środków bezpieczeństwa.

„Bezpieczeństwo sieci i informacji: perspektywy europejskie i międzynarodowe” pod redakcją Jeanne Pia Mifsud Bonnici i Joe Cannataci

- W niniejszym zbiorze przeanalizowano sytuację w zakresie bezpieczeństwa sieci i informacji zarówno z perspektywy europejskiej, jak i międzynarodowej, przedstawiając szerszy kontekst działań UE w zakresie cyberbezpieczeństwa.

„Sztuczna inteligencja w cyberbezpieczeństwie: praktyki, wyzwania i etyka” autorstwa Eleny Fersman i Martina Fredrikssona

- Kompleksowy przegląd integracji technologii sztucznej inteligencji w cyberbezpieczeństwie, poruszający kwestie wyzwań etycznych, operacyjnych i regulacyjnych, szczególnie istotnych w kontekście UE.

„Cybersecurity in the Digital Age: Tools, Techniques, and Applications” autorstwa Gregory'ego B. White'a, Erica A. Fishera i Jamesa L. Antonakosa

- Chociaż książka ta nie skupia się wyłącznie na UE, obejmuje ona również szeroki zakres współczesnych zagadnień związanych z cyberbezpieczeństwem.

Materiały do nauki *(oryginalne materiały HackerU i Cybint)*
Lektura obowiązkowa
• Administracja sieciami TCP/IP: pomoc dla administratorów systemów Unix, wydanie trzecie, autor: Craig Hunt (O'Reilly) • Podstawowe informacje dotyczące administrowania systemami: polecenia i formaty plików (Pocket Administrator) autorstwa Eleen Frisch (O'Reilly) • Sieci komputerowe: przewodnik dla początkujących po sieciach komputerowych, Internecie i modelu OSI autorstwa Ramona Nastase
Lektury zalecane
• Certyfikacja CompTIA A+ All-in-One For Dummies (komputery/technologia), wydanie piąte, autorzy: Glen E. Clarke, Edward Tetz, Timothy L. Warner • Coding All-in-One For Dummies, wydanie pierwsze, autor: Nikhil Abraham • Podstawy technologii informacyjnej, tom 1: Wprowadzenie do systemów informatycznych autorstwa Erica Fricka • IT Architecture For Dummies, wydanie pierwsze, autorzy: Kalani Kirk Hausman, Susan L. Cook • Cybersecurity For Dummies (Komputery/Technologia) wydanie pierwsze autorstwa Steinberga • Linux dla opornych, wydanie 10. autorstwa Richarda Bluma

- Windows 10 dla opornych, wydanie trzecie (komputery/technologia), wydanie trzecie autorstwa Rathbone
- Sieci dla opornych, wydanie 12. autorstwa Douga Lowe'a

6. M6: PLANOWANIE CYBERBEZPIECZEŃSTWA

Tytuł modułu	Kod modułu
PLANOWANIE BEZPIECZEŃSTWA CYBERNETYCZNEGO	

Wykładowca (wykładowcy)	Instytucja lub wydział, na którym realizowany jest moduł

Sposób realizacji	Język
Stacjonarne, online, mieszane, konsultacje	*Angielski, fiński, turecki, norweski, litewski, rumuński, francuski, polski, hiszpański*

Wymagania wstępne
-

Liczba przyznanych punktów ECTS	Obciążenie pracą studenta	Godziny zajęć kontaktowych	Indywidualne godziny pracy
3	75	50	25

Cel i efekty modułu

Po ukończeniu tego kursu studenci będą potrafili zrozumieć i stosować podstawowe zasady planowania i zarządzania cyberbezpieczeństwem. Zdobędą umiejętność wdrażania międzynarodowych standardów i ram, opracowywania długoterminowych strategii bezpieczeństwa, zarządzania operacyjnymi i taktycznymi środkami cyberbezpieczeństwa oraz planowania bezpiecznych architektur sieciowych, takich jak chmura i zero trust. Ponadto studenci będą przygotowani do opracowywania skutecznych planów reagowania na incydenty i wdrażania strategii ciągłości działania, zapewniających odporność organizacji i skuteczne środki cyberbezpieczeństwa w obliczu zmieniających się zagrożeń.

Efekty kształcenia modułu	Metody nauczania i uczenia się	Metody oceny
Wiedza: Uczestnicy zdobędą zaawansowaną wiedzę na temat tego, jak włączyć zaawansowane zasady cyberbezpieczeństwa i aktualne trendy do planowania strategicznego i zarządzania operacyjnego.	Wykłady, studia przypadków, dyskusje grupowe, samokształcenie	Testy samooceny, testy sprawdzające wiedzę
Umiejętności: Uczestnicy zdobędą umiejętności w zakresie planowania strategicznego i zarządzania operacyjnego, które pozwolą im skutecznie opracowywać i wdrażać strategie cyberbezpieczeństwa uwzględniające pojawiające się zagrożenia i zapewniające solidne reakcje taktyczne.	Ćwiczenia praktyczne, warsztaty, studia przypadków	Oceny oparte na projektach, oceny praktyczne

Kompetencje: Uczestnicy zdobędą kompetencje w zakresie opracowywania i wdrażania strategicznych ram cyberbezpieczeństwa oraz kierowania inicjatywami w zakresie cyberbezpieczeństwa i zarządzania nimi.	Warsztaty, seminaria, ćwiczenia z odgrywaniem ról	Ocena ciągła, testy oparte na scenariuszach

Zawartość modułu: podział tematów	**Godziny pracy kontaktowej**					**Indywidualne godziny pracy i zadania**	
	Wykłady (HEI)	Konsultacje	Praktyka (HEI)	Testy	**Wszystkie prace kontaktowe**	**Praca indywidualna**	**Zadania**
1. Wprowadzenie do planowania cyberbezpieczeństwa: bezpieczeństwo danych, ludzi i społeczeństwa - bezpieczeństwo danych - bezpieczeństwo przechowywania informacji, proces dochodzeniowy - bezpieczeństwo danych - techniki ataków na hasła - bezpieczeństwo ludzi - świadomość i zrozumienie - bezpieczeństwo społeczne – czym jest cyberprzestępczość, cyberetyka - bezpieczeństwo społeczne – prawo cyberprzestrzeni – dowody cyfrowe, umowy cyfrowe, konwencje międzynarodowe (porozumienia)	8	0,5	6	0,5	**15**	**8**	Określenie aspektów prawnych dotyczących bezpieczeństwa danych, ludzi i społeczeństwa, przepisów i polityk regulujących kwestie danych w MŚP. Klasyfikacja rodzajów cyberataków istotnych dla MŚP. Zidentyfikować przydatne narzędzia zapobiegania cyberatakom.
2. Planowanie strategiczne -Określenie celów i zadań w zakresie cyberbezpieczeństwa -Analiza SWOT (mocne strony, słabe strony, szanse, zagrożenia) -Opracowanie długoterminowych strategii bezpieczeństwa -Ustalanie kluczowych wskaźników efektywności (KPI) -Przegląd i aktualizacja strategii bezpieczeństwa	8	2	6	2	**18**	**8**	Określ cele w zakresie cyberbezpieczeństwa istotne dla MŚP przy użyciu analizy SWOT, opracuj długoterminowe strategie przeciwdziałania ryzyku, odpowiednio przydziel zasoby i budżet, ustal wskaźniki KPI do pomiaru postępów i regularnie aktualizuj strategię w oparciu o nowe zagrożenia.

3. Zarządzanie operacyjne i taktyczne -Wdrażanie kontroli dostępu -Zarządzanie poprawkami i aktualizacjami oprogramowania -Ciągłe monitorowanie systemu - Szkolenia dla pracowników w zakresie świadomości bezpieczeństwa	8	1	6	2	**17**	**9**	Wdrożenie środków kontroli dostępu w celu ograniczenia nieuprawnionego dostępu, utrzymanie systemów poprzez zarządzanie poprawkami, skonfigurowanie monitorowania nietypowych działań oraz zapewnienie pracownikom szkoleń z zakresu świadomości cyberbezpieczeństwa.
Razem	**24**	**3,5**	**18**	**4,5**	**50**	**25**	

Strategia oceny	**Porównawczy procent wagowy**	**Kryteria oceny**
Test samooceny (1)	10%	10 punktów – 96–100% poprawnych odpowiedzi. 9 punktów – 91–95% poprawnych odpowiedzi. 8 punktów – 86–90% poprawnych odpowiedzi. 7 punktów – 80–85% poprawnych odpowiedzi. 6 punktów – 70–79% poprawnych odpowiedzi. 5 punktów – 60–69% poprawnych odpowiedzi. 4 punkty – 50–59% poprawnych odpowiedzi. 3 punkty – 40–49% poprawnych odpowiedzi. 2 punkty – 30–39% poprawnych odpowiedzi. 1 punkt – 0–29% poprawnych odpowiedzi.
Test samooceny (2)	10	
Test samooceny (3)	10	
Test sprawdzający wiedzę	70%	

Materiały do badań *(nazwisko, inicjał imienia. (rok, miesiąc, dzień). Tytuł artykułu. Tytuł czasopisma/dziennika/gazety, numer tomu (numer wydania), numery stron całego artykułu, wydawca, adres URL)*

Lektura obowiązkowa

1. Nair, A. i Greeshma, M. R. (2023). Mastering Information Security Compliance Management: A Comprehensive Handbook on ISO/IEC 27001:2022 Compliance. Packt Publishing Limited.
2. Falco, G. J. i Rosenbach, E. (2021). Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity. Oxford University Press.
3. Ramy cyberbezpieczeństwa NIST (CSF) 2.0, Narodowy Instytut Standardów i Technologii, 26 lutego 2024 r.

Zalecana lektura

1. Mehta, S. (2023). *Przewodnik egzaminacyjny ISACA Certified in Risk and Information Systems Control (CRISC®)*. Packt Publishing Limited.
2. Gregory, P. H. (2021). *Kompletny przewodnik egzaminacyjny CISM Certified Information Security Manager*. McGraw-Hill.
3. ISACA. (2021). *Podręcznik CRISC, wydanie 7*. ISACA.
4. Parlament Europejski i Rada. (14 grudnia 2022 r.). *Rozporządzenie (UE) 2022/2554 w sprawie cyfrowej odporności operacyjnej sektora finansowego*.

5. Przewodnik po ogólnym rozporządzeniu o ochronie danych (RODO), Biuro Komisarza ds. Informacji

7. M7: ZARZĄDZANIE RYZYKIEM I JEGO OGRANICZANIE

Tytuł modułu	Kod modułu
ZARZĄDZANIE RYZYKIEM I JEGO OGRANICZANIE	

Wykładowca (wykładowcy)	Instytucja lub wydział, na którym realizowany jest moduł

Sposób realizacji	Język
Stacjonarne, online, mieszane, konsultacje	*Angielski, fiński, turecki, norweski, litewski, rumuński, francuski, polski, hiszpański*

Wymagania wstępne			
Brak			
Liczba przyznanych punktów ECTS	**Obciążenie pracą studenta**	**Godziny zajęć kontaktowych**	**Godziny pracy indywidualnej**
3	75	50	25

Cel i efekty modułu		
Po ukończeniu tego kursu studenci będą potrafili w sposób ciągły zarządzać (identyfikować, analizować, oceniać, szacować, łagodzić) ryzykiem związanym z cyberbezpieczeństwem infrastruktur, systemów i usług ICT poprzez planowanie, stosowanie, raportowanie i komunikowanie analizy ryzyka, oceny i postępowania.		
Efekty kształcenia modułu	**Metody nauczania i uczenia się**	**Metody oceny**
Wiedza: Uczestnicy zdobędą zaawansowaną wiedzę na temat procesów zarządzania ryzykiem, w tym identyfikacji, oceny i kontroli ryzyka, co pozwoli im ustanowić i opisać skuteczne procedury bezpieczeństwa cybernetycznego dostosowane do konkretnych potrzeb miejsc pracy w MŚP, zgodnie z krajowymi i międzynarodowymi standardami.	Do wyboru przez wykładowcę z części 1.3. [*Metody nauczania, np. wykłady teoretyczne, analiza literatury, prelegenci zewnętrzni, nauczanie i uczenie się między rówieśnikami, mentoring itp.*	Testy samooceny Test sprawdzający wiedzę

Umiejętności: Uczestnicy zdobędą umiejętności stosowania zaawansowanych metodologii i narzędzi do przeprowadzania kompleksowych ocen ryzyka, projektowania i wdrażania skutecznych strategii zarządzania ryzykiem oraz opracowywania solidnych procedur bezpieczeństwa cybernetycznego dostosowanych specjalnie do miejsc pracy w MŚP.	Do wyboru przez wykładowcę z części 1.3. [*Metody nauczania, np. zadania praktyczne/laboratoria, quizy, gry, analiza filmów technicznych, studia przypadków, zajęcia praktyczne itp.]* z D2.3 „*Struktura ścieżki kształcenia agentów zmian w zakresie cyberbezpieczeństwa w* MŚP”	Testy samooceny Test sprawdzający wiedzę
Kompetencje: Uczestnicy będą potrafili opracowywać i wdrażać strategiczne polityki cyberbezpieczeństwa w miejscach pracy w MŚP.	Do wyboru przez wykładowcę z części 1.3. [*Metody nauczania, np. konkursy, CTF, symulowane środowiska, 5E, CBL, CL, PBL itp.]* z D2.3 „*Struktura ścieżki kształcenia agentów zmian w zakresie cyberbezpieczeństwa w MŚP*”	Testy samooceny Test sprawdzający wiedzę

Zawartość modułu: podział tematów	Godziny pracy kontaktowej					Indywidualne godziny pracy i zadania	
	Wykłady (HEI)	Konsultacje	Praktyka (HEI)	Testy	Wszystkie prace kontaktowe	Praca indywidualna	Zadania
Ocena ryzyka - Ogólny proces zarządzania ryzykiem - Ogólne ramy zarządzania ryzykiem - Zasady zarządzania ryzykiem - Standardy zarządzania ryzykiem - Praktyczne przykłady	2	0	2	0	**4**	5	- Krótko opisz kluczowe etapy procesu zarządzania ryzykiem, w tym identyfikację ryzyka, ocenę ryzyka i kontrolę ryzyka. - Określ wewnętrzne i zewnętrzne konteksty zarządzania ryzykiem dla MŚP. Określ zakres oceny ryzyka i zidentyfikuj kluczowe czynniki ryzyka. - Opracuj kryteria ryzyka specyficzne dla wybranego MŚP.
Identyfikacja ryzyka - przywództwo i zaangażowanie w zarządzaniu ryzykiem - określenie zakresu działań związanych z zarządzaniem ryzykiem - zewnętrzny i wewnętrzny kontekst zarządzania ryzykiem - materialne i niematerialne źródła ryzyka; - przyczyny i zdarzenia; - zagrożenia i możliwości; - słabe punkty i możliwości; - zmiany w kontekście zewnętrznym i wewnętrznym; - wskaźniki pojawiających się ryzyk; - charakter i wartość aktywów i zasobów; - konsekwencje i ich wpływ na cele; - ograniczenia wiedzy i wiarygodności informacji; - uprzedzenia, założenia i przekonania osób zaangażowanych. - Praktyczne przykłady i studia przypadków.	4	0	4	0	**8**	5	- Zidentyfikuj zarówno materialne, jak i niematerialne źródła ryzyka dla MŚP. Sklasyfikuj ryzyka na podstawie przyczyn, zdarzeń, zagrożeń i możliwości. - Przeanalizuj wewnętrzne słabe punkty i możliwości MŚP oraz oceń, w jaki sposób zmiany w kontekście zewnętrznym i wewnętrznym mogą wpłynąć na działalność firmy. - Zidentyfikuj potencjalne pojawiające się zagrożenia dla MŚP i zaproponuj wskaźniki do ich monitorowania. Zastanów się, jak charakter i wartość aktywów oraz zasobów wpływają na tę analizę.
Zagrożenia wewnętrzne - Definicja i rodzaje zagrożeń wewnętrznych	6	0	6	0	**12**	5	- Zdefiniuj i sklasyfikuj różne rodzaje zagrożeń wewnętrznych istotnych dla małych i

- Koszty zagrożeń wewnętrznych - Tworzenie programu ograniczania zagrożeń wewnętrznych - Wykrywanie i identyfikowanie zagrożeń wewnętrznych - Ocena zagrożeń wewnętrznych - Zarządzanie zagrożeniami wewnętrznymi - Praktyczne przykłady i studia przypadków							średnich przedsiębiorstw. Omów potencjalne koszty, jakie zagrożenia te mogą narzucić na działalność gospodarczą. - Opracuj podstawowy program ograniczania zagrożeń wewnętrznych dla MŚP. Podkreśl kluczowe elementy, takie jak strategie wykrywania, identyfikacji i zarządzania. - Zaproponować metodę oceny zagrożeń wewnętrznych i nakreślić kroki niezbędne do skutecznego zarządzania tymi zagrożeniami w kontekście MŚP.
Modele i metodologie pomiaru i oceny ryzyka - Ilościowe i jakościowe modele i metodologie oceny ryzyka - prawdopodobieństwo wystąpienia zdarzeń i konsekwencji; - charakter i skala konsekwencji; - złożoność i powiązania; - czynniki związane z czasem i zmiennością; - ocena skuteczności istniejących środków kontroli; - poziomy wrażliwości i pewności. - Praktyczne przykłady i studia przypadków	6	0	6	0	**12**	5	- Porównaj i skontrastuj jeden ilościowy i jeden jakościowy model oceny ryzyka. - Oceń prawdopodobieństwo wystąpienia zdarzenia ryzyka oraz charakter i skalę jego konsekwencji dla MŚP. Zastanów się, w jaki sposób złożoność, czynniki związane z czasem i zmienność wpływają na tę ocenę. - Oceń skuteczność obecnych środków kontroli w zarządzaniu zidentyfikowanymi ryzykami. Uwzględnij analizę wrażliwości i poziomów pewności w środkach kontroli.
Kontrola ryzyka - formułowanie i wybór opcji postępowania z ryzykiem - planowanie i wdrażanie środków ograniczających ryzyko - ocena skuteczności tych działań - podejmowanie decyzji, czy pozostałe ryzyko jest akceptowalne - monitorowanie i przegląd - rejestrowanie i raportowanie	6	0	6	0	**12**	5	- Zidentyfikuj i wybierz odpowiednie opcje zarządzania ryzykiem dla MŚP. Uzasadnij swój wybór w oparciu o charakter ryzyka. - Opracuj krótki plan postępowania z ryzykiem, opisując, w jaki sposób wybrane opcje postępowania zostaną wdrożone w środowisku MŚP.

- Praktyczne przykłady i studia przypadków							- Zaproponuj metodę oceny skuteczności zarządzania ryzykiem i określenia, czy pozostałe ryzyko jest akceptowalne.
Razem	**24**	**2**	**24**	**0**	**50**	**25**	

Strategia oceny	**Porównawczy procent wagowy**	**Kryteria oceny**
Test samooceny (1)	5	10 punktów – 96–100% poprawnych odpowiedzi. 9 punktów – 91–95% poprawnych odpowiedzi. 8 punktów – 86–90% poprawnych odpowiedzi. 7 punktów – 80–85% poprawnych odpowiedzi. 6 punktów – 70–79% poprawnych odpowiedzi. 5 punktów – 60–69% poprawnych odpowiedzi. 4 punkty – 50–59% poprawnych odpowiedzi. 3 punkty – 40–49% poprawnych odpowiedzi. 2 punkty – 30–39% poprawnych odpowiedzi. 1 punkt – 0–29% poprawnych odpowiedzi.
Test samooceny (2)	5	
Test samooceny (3)	5	
Test samooceny (4)	5	
Test samooceny (5)	5	
Test sprawdzający wiedzę	75%	

Materiały do nauki *(Nazwisko, inicjał imienia. (Rok, miesiąc, dzień). Tytuł artykułu. Tytuł czasopisma/dziennika/gazety, numer tomu (numer wydania), numery stron całego artykułu, wydawca, adres URL)*

Lektura obowiązkowa

1. Adarsh Nair i Greeshma M. R. (2023) Mastering Information Security Compliance Management : A Comprehensive Handbook on ISO/IEC 27001:2022 Compliance. Packt Publishing, Limited **https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30652023&**query=risk%20management
2. Gregory J. Falco, Eric Rosenbach (2021) Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity. Oxford University Press, eBook
3. Kristina Narvaez, Betty Simkins, John Fraser (2014) Wdrażanie zarządzania ryzykiem w przedsiębiorstwie: studia przypadków i najlepsze praktyki. John Wiley & Sons
4. ENISA (2022) Standardy zarządzania ryzykiem
5. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)
6. ISO 31000 Zarządzanie ryzykiem — Wytyczne

Zalecana lektura

1. Shobhit Mehta (2023) ISACA Certified in Risk and Information Systems Control (CRISC®) Exam Guide. Packt Publishing, Limited **https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30806680&query=risk%20management**
2. Peter H. Gregory (2021) Kompletny przewodnik egzaminacyjny CISM Certified Information Security Manager. McGraw-Hill
3. ISACA (2021) Podręcznik CRISC, wydanie 7. ISACA
4. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie cyfrowej odporności operacyjnej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 i (UE) 2016/1011

8. M8: CIĄGŁOŚĆ DZIAŁALNOŚCI, ODZYSKIWANIE DANYCH PO AWARII, ZARZĄDZANIE INCYDENTAMI I BEZPIECZEŃSTWO PERSONELU

Tytuł modułu	Kod modułu
CIĄGŁOŚĆ DZIAŁALNOŚCI, ODZYSKIWANIE DANYCH PO AWARII, ZARZĄDZANIE INCYDENTAMI I BEZPIECZEŃSTWO PERSONELU	

Wykładowca (wykładowcy)	Instytucja lub wydział, w którym realizowany jest moduł

Sposób realizacji	Język
Stacjonarne, online, mieszane, konsultacje	*Angielski, fiński, turecki, norweski, litewski, rumuński, francuski, polski, hiszpański*

Wymagania wstępne
Brak

Liczba przyznanych punktów ECTS	Obciążenie pracą studenta	Godziny zajęć kontaktowych	Indywidualne godziny pracy
3	75	50	25

Cel i efekty modułu
Po ukończeniu tego kursu studenci będą potrafili formułować i wdrażać kompleksowe plany ciągłości działania i odzyskiwania danych po awarii (BC/DR), opracowywać funkcjonalny program zarządzania incydentami oraz ustanawiać solidną i skuteczną politykę bezpieczeństwa personelu. Studenci dowiedzą się, jak chronić aktywa, zapobiegać nadmiernym stratom, unikać przestojów, zapobiegać sytuacjom kryzysowym lub ograniczać je oraz zarządzać środowiskami kryzysowymi. Po ukończeniu tego kursu studenci będą potrafili sporządzić i monitorować trwałe wdrożenie kompleksowego podręcznika cyberbezpieczeństwa dla MŚP, wykorzystując zaawansowane zasady i technologie cyberbezpieczeństwa zintegrowane zgodnie ze wszystkimi krajowymi i międzynarodowymi przepisami. Studenci będą również monitorować egzekwowanie tych zasad.

Efekty kształcenia modułu	Metody nauczania i uczenia się	Metody oceny

Wiedza: Uczestnicy zdobędą zaawansowaną wiedzę na temat tworzenia i wdrażania kompleksowego podręcznika bezpieczeństwa cybernetycznego w miejscu pracy dla MŚP, uwzględniającego zaawansowane zasady bezpieczeństwa cybernetycznego, najnowsze mechanizmy obronne oraz zgodność z krajowymi i międzynarodowymi przepisami i normami w zakresie zarządzania incydentami, ciągłości działania i bezpieczeństwa personelu.	Do wyboru przez wykładowcę z części 1.3. [Metody nauczania] D2.3 „Struktura ścieżki edukacyjnej dla agentów zmian w zakresie cyberbezpieczeństwa w MŚP".	Testy samooceny, test sprawdzający wiedzę
Umiejętności: Uczestnicy zdobędą umiejętności tworzenia i utrzymywania podręcznika dotyczącego cyberbezpieczeństwa w miejscu pracy w MŚP, wykorzystując zaawansowane metody oceny ryzyka, projektowania skutecznych strategii zarządzania ryzykiem i reagowania na incydenty oraz opracowywania kompleksowych planów ciągłości działania dostosowanych do potrzeb ich organizacji.	Do wyboru przez wykładowcę, z części 1.3. [Metody nauczania] dokumentu D2.3 „Struktura ścieżki kształcenia agentów zmian w zakresie cyberbezpieczeństwa w MŚP".	Testy samooceny, test sprawdzający wiedzę
Kompetencje: Uczestnicy kursu będą potrafili opracować i wdrożyć podręcznik dotyczący cyberbezpieczeństwa dla MŚP, skutecznie kierować projektami i zespołami ds. bezpieczeństwa, zapewniając zgodność z celami organizacyjnymi i obowiązkami w zakresie zgodności.	Do wyboru przez wykładowcę, z części 1.3. [Metody nauczania] D2.3 „Struktura ścieżki kształcenia agentów zmian w zakresie cyberbezpieczeństwa w MŚP".	Testy samooceny, test sprawdzający wiedzę

Zawartość modułu: podział tematów	**Godziny pracy kontaktowej**					**Indywidualne godziny pracy i zadania**	
	Wykłady (HEI)	Konsultacje	Ćwiczenia (HEI)	Testy	**Wszystkie**	**Praca**	**Zadania**

Reagowanie na incydenty - Definicja i znaczenie reagowania na incydenty w cyber-bezpieczeństwie - Kluczowe elementy skutecznego reagowania na incydenty - Przegląd typowych zagrożeń dla cyberbezpieczeństwa (phishing, zagrożenia wewnętrzne) - Opracowanie planu reagowania na incydenty (IRP) - Role i obowiązki w zespole reagowania na incydenty - Symulacja incydentu: przeprowadzenie próbnego planu.	5	0,5	3	0,5	**9**	**5**	Opracuj szczegółowy plan reagowania na incydenty dla swojego MŚP, obejmujący role, obowiązki i kroki, które należy podjąć w przypadku incydentu związanego z cyberbezpieczeństwem. Przeprowadź symulację incydentu i ćwiczenia, aby sprawdzić skuteczność swojego planu.
Odzyskiwanie danych po awarii - Zrozumienie odzyskiwania danych po awarii - Opracowanie planu odzyskiwania danych po awarii - Role i obowiązki w ramach odzyskiwania danych po awarii - Kroki przywracania sprawności po awarii	5	0,5	3	0,5	**9**	**5**	Opracuj plan przywracania sprawności po awarii, który określa procedury przywracania infrastruktury IT i danych po katastrofie. Uwzględnij harmonogram przywracania sprawności i przydziel obowiązki członkom zespołu na każdym etapie procesu.
Ciągłość działania - Zrozumienie ciągłości działania - Opracowanie planu ciągłości działania (BCP) - Role i obowiązki w zakresie ciągłości działania - Analiza wpływu na działalność - Testowanie i ulepszanie BCP	5	0,5	3	0,5	**9**	**5**	Opracuj plan ciągłości działania, który zapewni funkcjonowanie kluczowych funkcji biznesowych podczas i po wystąpieniu zakłóceń. Zidentyfikuj niezbędne usługi i zasoby oraz nakreśl strategie awaryjne, aby utrzymać je w różnych scenariuszach.

Świadomość bezpieczeństwa, szkolenia i edukacja - Zrozumienie świadomości bezpieczeństwa - Opracowanie programu szkoleń z zakresu bezpieczeństwa - Obowiązki pracowników w zakresie cyberbezpieczeństwa - Pomiar skuteczności świadomości bezpieczeństwa -	1	0,5	2	0,5	**4**	**1**	Opracuj program szkoleń z zakresu świadomości bezpieczeństwa dla swojego MŚP, koncentrując się na kluczowych zasadach i najlepszych praktykach dotyczących cyberbezpieczeństwa. Przeprowadź sesję szkoleniową dla pracowników i oceń ich zrozumienie poprzez quizy lub interaktywne ćwiczenia.
Praktyki zatrudniania w zakresie bezpieczeństwa - Określanie wymagań dotyczących ról związanych z bezpieczeństwem - Przeprowadzanie kompleksowej weryfikacji kandydatów - Przeprowadzanie rozmów kwalifikacyjnych dotyczących elementów bezpieczeństwa - Bieżąca ocena i rozwój	1	0,5	2	0,5	**4**	**1**	Wprowadź praktyki zatrudniania ukierunkowane na bezpieczeństwo, w tym weryfikację przeszłości i pytania podczas rozmowy kwalifikacyjnej mające na celu ocenę świadomości kandydatów w zakresie cyberbezpieczeństwa. Stwórz listę kontrolną niezbędnych kwalifikacji i cech potencjalnych pracowników w zakresie bezpieczeństwa.
Praktyki dotyczące zwolnień związanych z bezpieczeństwem - Natychmiastowe cofnięcie dostępu - Odzyskiwanie danych i urządzeń - Rozmowa końcowa w celu uzyskania informacji dotyczących bezpieczeństwa - Powiadomienie odpowiednich zespołów - Kwestie prawne i zgodność z przepisami	1	0,5	2	0,5	**4**	**2**	Opracuj procedurę bezpiecznego zwolnienia, która obejmuje kroki dotyczące cofnięcia dostępu, odzyskania aktywów firmy i przeprowadzenia rozmów końcowych. Zaimplementuj scenariusz symulacji zwolnienia, aby ocenić skuteczność procedury.

Bezpieczeństwo stron trzecich - Ocena ryzyka związanego z podmiotami zewnętrznymi - Należyta staranność przy wyborze dostawców - Wdrożenie kontrastów i wymagań bezpieczeństwa - Bieżące monitorowanie i audyt - Reagowanie na incydenty i komunikacja	2	0,5	2	0,5	**5**	**2**	Zidentyfikuj potencjalne ryzyko związane z zewnętrznymi dostawcami i stwórz listę kontrolną oceny bezpieczeństwa, aby sprawdzić, czy spełniają oni standardy cyberbezpieczeństwa Twojej firmy. Przygotuj szablon umowy, który zawiera wymagania dotyczące bezpieczeństwa i kary za nieprzestrzeganie zasad.
Bezpieczeństwo w procesach przeglądu - Włączenie bezpieczeństwa do przeglądów - Przeprowadzanie regularnych audytów bezpieczeństwa - Ocena podatności i testy penetracyjne - Przeglądy po incydentach	1	0,5	1,5	0,5	**3, 5**	**2**	Opracuj proces regularnego przeglądu i aktualizacji polityk i procedur dotyczących cyberbezpieczeństwa w Twojej małej lub średniej firmie. Zaplanuj i przeprowadź próbny audyt, aby upewnić się, że wszystkie środki bezpieczeństwa są aktualne i zgodne z odpowiednimi standardami.
Kwestia szczególna dotycząca prywatności danych osobowych pracowników - Ograniczenia dotyczące gromadzenia danych - Przechowywanie i kontrola dostępu - Zgodność z przepisami dotyczącymi prywatności - Udostępnianie danych i strony trzecie - Zgoda i prawa pracowników	2	0,5	2	0,5	**5**	**2**	Opracowanie polityki prywatności dotyczącej postępowania z danymi osobowymi pracowników, zapewniającej zgodność z przepisami o ochronie danych i najlepszymi praktykami. Przeprowadzenie oceny ryzyka w celu zidentyfikowania potencjalnych słabych punktów w sposobie przechowywania i przetwarzania danych pracowników.

Razem	**23**	**2**	**20,5**	**4,5**	**50**	**25**	

Strategia oceny	**Porównawczy procent wagowy**	**Kryteria oceny**
Test samooceny (1)	5	**10 punktów** – 96–100% poprawnych odpowiedzi. **9 punktów** – 91–95% poprawnych odpowiedzi. **8 punktów** – 86–90% poprawnych odpowiedzi. **7 punktów** – 80–85% poprawnych odpowiedzi. **6 punktów** – 70–79% poprawnych odpowiedzi. **5 punktów** – 60–69% poprawnych odpowiedzi. **4 punkty** – 50–59% poprawnych odpowiedzi. **3 punkty** – 40–49% poprawnych odpowiedzi. **2 punkty** – 30–39% poprawnych odpowiedzi. **1 punkt** – 0–29% poprawnych odpowiedzi.
Test samooceny (2)	5	
Test samooceny (3)	5	
Test samooceny (4)	5	
Test samooceny (5)	5	
Test sprawdzający wiedzę	75%	

Materiały do nauki *(Nazwisko, inicjał imienia. (Rok, miesiąc, dzień). Tytuł artykułu. Tytuł czasopisma/dziennika/gazety, numer tomu (numer wydania), numery stron całego artykułu, wydawca, adres URL)*

Lektura obowiązkowa

- Gregory J. Falco, Eric Rosenbach (2021). *Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity*. Oxford University Press, eBook.
- Michael Wallace, Lawrence Webber (2017). *Podręcznik odzyskiwania danych po awarii: plan krok po kroku zapewniający ciągłość działania i ochronę kluczowych operacji, obiektów i aktywów.* AMACOM.
- Narodowy Instytut Standardów i Technologii (NIST). *Przewodnik planowania awaryjnego dla systemów informatycznych*. NIST SP 800-34 Rev. 1.
- Cochran, K.A. (2024). Reagowanie na incydenty, ciągłość działania i odzyskiwanie danych po awarii. W: Cybersecurity Essentials. Apress, Berkeley, Kalifornia. **https://doi.org/10.1007/979-8-8688-0432-8_14**

Lektury zalecane

- ISACA (2023). *Podręcznik CISM, wydanie 15*. ISACA.
- Peter H. Gregory (2021). *Kompleksowy przewodnik egzaminacyjny CISM Certified Information Security Manager*. McGraw-Hill.
- IT Governance (2022). *ISO 22301:2019 – Systemy zarządzania ciągłością działania. Wymagania.*
- M. Souppaya, L. Feldman, G. Witte [2024], Przewodnik po odzyskiwaniu danych po incydentach związanych z cyberbezpieczeństwem, Dział Bezpieczeństwa Komputerowego Laboratorium Technologii Informacyjnych Narodowy Instytut Standardów i Technologii Departament Handlu Stanów Zjednoczonych
- Ihab Hanna Sawalha [2021]. Poglądy na temat ciągłości działania i odzyskiwania danych po awarii. Międzynarodowe czasopismo służb ratowniczych

ZAŁĄCZNIKI

SZABLON SYLABUSU

OPIS MODUŁU

Tytuł modułu	Kod modułu
...	

Wykładowca (wykładowcy)	Instytucja lub wydział, na którym realizowany jest moduł
...	...

Sposób realizacji	Język
Bezpośredni, online, mieszany, konsultacje	*Angielski, ...*

Wymagania wstępne
...

Liczba przyznanych punktów ECTS	Obciążenie pracą studenta	Godziny zajęć kontaktowych	Indywidualne godziny pracy
3	...	...	...

Cel i efekty modułu		
...		
Efekty kształcenia modułu	**Metody nauczania i uczenia się**	**Metody oceny**

Ułatwianie dostępu do zasobów (sprzęt, oprogramowanie, technologia)
...

Zawartość modułu: podział tematów	Godziny pracy kontaktowej					Indywidualne godziny pracy i zadania	
	Wykłady (HEI)	Konsultacje	Ćwiczenia (HEI)	Testy	**Wszystkie zajęcia**	**Praca indywidualna**	**Zadania**
1							
...							
n							
Razem							

Strategia oceny	Porównawczy procent wagowy	Kryteria oceny
Samokontrola I		...
...		...
Autotest n		...
Test sprawdzający wiedzę		...

Materiały do nauki *(Nazwisko, inicjał imienia. (Rok, miesiąc, dzień). Tytuł artykułu. Tytuł czasopisma/dziennika/gazety, numer tomu (numer wydania), numery stron całego artykułu, wydawca, adres URL)*
Lektura obowiązkowa
...
Lektury zalecane
...

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau