



ASKE Mariusz

Kwapis

★★★★★ 4,8 / 5

60 ocen

Cyberbezpieczeństwo i identyfikacja w erze AI. Kwalifikacja cyfrowa i egzamin ICDL/ECDL S3 - IT Security. Szkolenie na platformie Microsoft 365 - edycja weekendowa.

Numer usługi 2026/05/02/161176/3530387

📄 Usługa szkoleniowa

📖 zdalna w czasie rzeczywistym

🕒 12:00 h

📅 21.08.2026 do 22.08.2026

1 920,00 PLN brutto

1 920,00 PLN netto

160,00 PLN brutto/h

160,00 PLN netto/h

261,33 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, Nowy start w Małopolsce z EURESEM, Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe
Grupa docelowa usługi	<p>Szkolenie przeznaczone jest dla pracowników biurowych, administracji, działów HR, kadr, finansów, sekretariatów oraz młodszych specjalistów IT, którzy potrzebują praktycznego wprowadzenia do cyberbezpieczeństwa. Grupa docelowa to osoby z wykształceniem średnim lub wyższym, znające podstawy Windows, lecz bez doświadczenia w AI i Zero Trust.</p> <p>Udział w szkoleniu pozwala spełnić wymagania NIS 2 i RODO, zdobyć certyfikat ICDL S3 oraz praktyczną wiedzę o ochronie przed cyberatakami. Kurs dedykowany osobom „non-tech”, które mogą stać się celem cyberprzestępców i potrzebują prostych narzędzi do codziennej ochrony siebie i firmy.</p> <p>Nauczysz się rozpoznawać ataki phishingowe i deepfake, szyfrować dane, konfigurować MFA oraz zabezpieczać się przed konsekwencjami naruszenia NIS 2</p> <p>Usługa dodatkowo adresowana do wszystkich Uczestników Projektów z dofinansowaniem również dla Uczestników Projektu MP i/lub dla Uczestników Projektu NSE, Projektu Kierunek-Rozwój, Projektu Zachodniopomorskie Bony Szkoleniowe</p>
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	15-08-2026

Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	12
Podstawa uzyskania wpisu do BUR	Akredytacja Centrów Egzaminacyjnych ECDL

Cel

Cel edukacyjny

Usługa przygotowuje uczestnika do bezpiecznej pracy w środowisku cyfrowym poprzez rozpoznawanie zagrożeń takich jak phishing i deepfake, stosowanie zabezpieczeń, w tym szyfrowania danych i MFA, wdrażanie zasad Zero Trust oraz przygotowuje do spełniania wymagań NIS 2 i RODO oraz uzyskania certyfikatu ICDL S3 IT Security.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Stosuje kwestie bezpieczeństwa.	Definiuje dane/informacje; znaczenie dla sektora publicznego (przedsiębiorstwa, urzędy); regulacje NIS2, DORA, UODO; wpływ AI na zagrożenia.	Test teoretyczny
	Wyjaśnia cyberprzestępczość; AI-enhanced: LLM-phishing, deepfakes audio/video, AI-vulnerability discovery, generacyjny malware; case studies BEC/ransomware. Socjotechnika 2.0: phishing/spear/smishing/vishing, pretexting AI, QR-phishing, deepfake voice, shoulder surfing; praktyka: analiza maili/SMS/filmów; psychologia manipulacji. Szyfrowanie at rest; praktyka: szyfr plików Windows, bezpieczna poczta; ryzyka klucza; chmura.	Test teoretyczny Test teoretyczny
Rozpoznaje złośliwe oprogramowanie.	Charakteryzuje Malware/ransomware/trojany; AI-generowany kod; real-world w instytucjach publicznych. Hasła, MFA (MS Authenticator/Google/Authy, YubiKey, Windows Hello, biometria); ryzyka SMS/email; Entra ID: Conditional Access, passwordless, least privilege; strategia MFA.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Zarządza kontrolą dostępu.	Zarządza hasłami. Stosuje dobre praktyki haseł dla biurowego użytkownika M365.	Test teoretyczny
	Stosuje bezpieczeństwo sieci LAN/WLAN/VPN; Zero Trust (mikrosegmentacja, identity-first, continuous verification); firewall; ryzyka hotspoty (MITM/sniffing).	Test teoretyczny
	Stosuje ochronę endpointów Bezpieczeństwo urządzeń (laptopy/telefony/pendrive); MDM/Intune, device compliance (Defender), USB/AppLocker.	Test teoretyczny
	Stosuje bezpieczną komunikację. Phishing analiza (SPF/DKIM/DMARC, VirusTotal/URLhaus); DLP; Teams zagrożenia; social media compliance.	Test teoretyczny
	Wyjaśnia znaczenie posiadania procedury kopii zapasowej (backupu) w przypadku utraty danych z zawartości komputerów i urządzeń.	Test teoretyczny
	Zarządza bezpiecznie danymi.	Charakteryzuje własności procedury tworzenia kopii zapasowej: regularność/częstotliwość tworzenia kopii zapasowej, planowanie, miejsce zapisu danych, kompresja danych.
Tworzy kopię zapasową i przywraca dane z kopii zapasowej z lokalizacji: dysk lokalny, dysk zewnętrzny/sieciowy, usługa w chmurze cyfrowej.		Test teoretyczny
Automatyzuje reagowanie na incydenty.	Stosuje reagowanie na incydenty. Objawy infekcji (powolny system, procesy); M365 telemetria; zgłaszanie, forensics, phishing email (nagłówki/linki), deepfake voice, ransomware, MFA atak, kradzież tożsamości.	Test teoretyczny
	Wykonuje automatyzację SOAR (Microsoft): playbooks auto-izolacja; Power Automate.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Stosuje bezpieczeństwo Web.	Wybiera/czyści ustawienia: autouzupełnianie, cookies, historia, hasła; kasuje dane prywatne z przeglądarki.	Test teoretyczny
	Wybiera/czyści ustawienia: autouzupełnianie, cookies, historia, hasła; kasuje dane prywatne z przeglądarki.	Test teoretyczny
Stosuje ochronę środowiska.	Rozpoznaje koszty zasilania TIK; stosuje oszczędzanie: wyłączenie urządzeń, zarządzanie energią w M365/Defender.	Test teoretyczny
	Minimalizuje wpływ: energooszczędne urządzenia, utylizacja sprzętu TIK; monitoruje środowisko.	Test teoretyczny

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

Pytanie 3. Czy dokument jest certyfikatem wydawanym przez międzynarodowe instytucje?

TAK

Strona internetowa Instytucji Certyfikującej: <https://icdl.pl/>

Informacje

Nazwa Podmiotu prowadzącego walidację	ASKE numer CE:PL-CE0198; Centrum Egzaminacyjne akredytowane przez Polskie Towarzystwo Informatyczne. Lista nazw akredytowanych podmiotów dostępna jest pod adresem: https://icdl.pl/centra-egzaminacyjne/
--	---

Nazwa Podmiotu certyfikującego	Polskie Towarzystwo Informatyczne
---------------------------------------	-----------------------------------

Program

Program szkoleniowy skierowany jest do osób, które chcą profesjonalnie rozwijać swoje umiejętności w zakresie cyberbezpieczeństwa.

Zakres szkolenia obejmuje następujące obszary wiedzy i umiejętności:

MODUŁ 1: FUNDAMENTY + AI-DRIVEN ZAGROŻENIA

Wprowadzenie do cyberbezpieczeństwa

- Definicja i znaczenie dla sektora publicznego (przedsiębiorstwa, urzędy, instytucje)
- Wpływ AI na krajobraz zagrożeń
- Regulacje: NOWE NIS 2, DORA, UODO

Zagrożenia tradycyjne i AI-enhanced

- Malware, ransomware, trojany – mechanizmy
- Ataki oparte na AI
- Autonomiczne phishing campaigns (LLM-generated emails)
- AI-powered vulnerability discovery
- Deepfake w socjotechnice (audio/video deepfake)
- Generacyjny malware (AI-generated code)
- Real-world case studies: BEC, ransomware na instytucjach publicznych

Socjotechnika 2.0 – Ataki na człowieka

- Phishing, spear phishing, smishing, vishing
- Zaawansowane techniki:
- Pretexting z profilem AI (research ofiary)
- QR code phishing / URL shortener tricks
- Voice phishing (deepfake voice)
- Shoulder surfing + mobile photography
- Interaktywna analiza fałszywych maili, SMS'ów, filmów
- Psychologia manipulacji: emocje, autorytety, naglące terminy

Bezpieczeństwo osobiste i tożsamość cyfrowa

- Kradzież tożsamości – przypadki w sektorze publicznym
- Prywatność w social mediach – ryzyka dla pracownika sektora publicznego
- Weryfikacja stron (certyfikat SSL, URL, WHOIS, VirusTotal)
- OSINT – jakie dane publiczne o Tobie są dostępne?

MODUŁ 2: OCHRONA DANYCH, IDENTITY-FIRST SECURITY, ZERO TRUST

Identity & Access Management – Nowy Standard

- Zarządzanie hasłami: polityka, menedżery haseł
- MFA/2FA
- Autentykatory (authenticator apps: MS Authenticator, Google, Authy)
- Klucze bezpieczeństwa (YubiKey, Apple Security Key)
- Windows Hello, biometria
- SMS/Email – ryzyka
- Azure AD / Microsoft Entra ID
- Conditional Access – automatyczne reguły dostępu
- Passwordless sign-in – przyszłość
- Least Privilege Principle – dostęp minimalny

Szyfrowanie i bezpieczne przetwarzanie danych

- Szyfrowanie „at rest” (BitLocker, EFS, Azure Encryption)
- Szyfrowanie „in transit” (TLS, HTTPS, S/MIME, PGP)
- Szyfr plików w Windows, wysyłka bezpiecznej poczty
- Ryzyka utraty klucza szyfrującego
- Kiedy (i kiedy NIE) szyfrować dane w organizacji publicznej
- Szyfrowanie w chmurze

Bezpieczeństwo urządzeń i Endpoint Protection

- Bezpieczeństwo laptopów, telefonów, pendrive'ów
- Mobile Device Management (MDM) – co to jest?
- Zero Trust na urządzeniu:
- Device compliance checks (Windows Defender, Intune)
- Application Control
- USB restrictions

- Zdalne wymazanie, blokowanie – scenariusz utraconego telefonu
- Ograniczenia uprawnień dla aplikacji (AppLocker, Group Policy)

Bezpieczeństwo sieci, firewall, Zero Trust Architecture

- Typy sieci: LAN, WLAN, VPN
- Zero Trust Model
- Nigdy nie ufaj – zawsze weryfikuj
- Mikrosegmentacja
- Identity-first (tożsamość = nowy obwód)
- Continuous verification
- Firewall – rola i konfiguracja
- Hotspoty publiczne – ryzyka (MITM, packet sniffing)
- VPN – kiedy i jak używać

MODUŁ 3: INCIDENT RESPONSE, AUTOMATION, PRAKTYKA

Rozpoznawanie incydentów i procedury reagowania

- Objawy infekcji: powolny system, podejrzane procesy, błędy logowania
- Telemetria w Microsoft 365
- Procedury zgłaszania: do kogo, jak, co mówić
- Forensics basics: zachowanie dowodów, niezmiennianie sceny

Symulacje ataków

- Analiza phishing emailu – czy to atak?
- Nagłówki emaila (SPF/DKIM/DMARC)
- Linki – analiza URL (URLhaus, VirusTotal)
- Deepfake voice analysis – czy to naprawdę szef?
- Ransomware – kroki reagowania
- Izolacja urządzenia
- Identyfikacja malware'u (hashcode → VirusTotal)
- Opcje odzyskania (backup vs. decryption tools)
- SOAR playbook – automatyzacja
- Atak na konto z MFA
- Zmiana hasła
- Anulowanie sesji
- Recovery – jak powiadomić zespół IT
- Kradzież tożsamości pracownika
- Kontakt z UODO / inspektorem ochrony danych
- Komunikacja z kadrą i mediami

Automatyzacja reagowania – Wprowadzenie do SOAR

- Co to jest SOAR? (Security Orchestration, Automation, Response)
- Microsoft Security Orchestration Automation and Response (SOAR):
- Playbooks – automacja procedur
- Automatyczne izolowanie zainfekowanego urządzenia

Bezpieczna komunikacja i compliance

- Email security: szyfrowanie, podpis elektroniczny, SPF/DKIM/DMARC
- Data Loss Prevention (DLP) – co można wysłać na zewnątrz?
- Komunikacja w Teams – zagrożenia i bezpieczeństwo
- Social media – co można/nie można publikować

Program szkolenia obejmuje 12 godzin dydaktycznych (co odpowiada 9 godzinom zegarowym). Zajęcia prowadzone są w godzinach dydaktycznych (każda trwa 45 minut). Przerwy nie są wliczane do czasu trwania szkolenia.

Szkolenie zostało zaprojektowane z praktycznym podejściem do zagrożeń cyfrowych, zapewniając uczestnikom umiejętność natychmiastowego zastosowania wiedzy w codziennej pracy biurowej z Microsoft 365. Struktura łączy teorię z intensywną praktyką:

Wykłady teoretyczne: 7 godzin dydaktycznych kluczowych zagadnień z cyberbezpieczeństwa.

Ćwiczenia praktyczne: 4 godziny dydaktyczne warsztatów na platformie M365: symulator phishingu (Defender), analiza VirusTotal, konfiguracja MFA/Entra ID, szyfrowanie BitLocker, symulacje incydentów.

Walidacja: 1 godzina dydaktyczna – samodzielne zadania końcowe z oceną efektów uczenia się w formie testu.

Egzamin:

Organizator w ramach usługi szkolenia **pokrywa koszt przystąpienia do pierwszego egzaminu z modułu S3 - IT Security poziom podstawowy**. Egzamin odbywa się w formie zdalnej w czasie rzeczywistym.

Ocena umiejętności Kandydata dokonywana jest na podstawie wyniku testu, który polega na rozwiązywaniu zadań. Test ma formę elektroniczną i trwa 45 minut. Test składa się z kilku zadań, które należy wykonać w określonej kolejności i zgodnie z instrukcjami. Zadania mogą dotyczyć dowolnych tematów z zakresu sylabusu modułu. Każde zadanie jest oceniane punktowo, przy czym część punktów może być przyznana za poprawność wykonania poszczególnych kroków. Aby zaliczyć test, Kandydat musi uzyskać co najmniej 75% punktów.

Walidacja:

Metoda weryfikacji: egzamin zewnętrzny ICDL, realizowany na komputerze, składający się z zadań (poleceń).

Certyfikat ICDL S3 - IT Security poziom podstawowy poświadczają zdobycie kompetencji cyfrowych z obszarów numer: 2.6, 4.1, 4.2, 4.3, 4.4. zgodnie z wytycznymi Komisji Europejskiej zawartymi w raporcie "**DigComp 2.2 Ramy Kompetencji Cyfrowych dla Obywateli**".

Informacja o kwalifikacji ICDL (ECDL): Certyfikat ICDL (ECDL) jest kwalifikacją potwierdzaną **międzynarodowym certyfikatem** i może być uznawany jako kwalifikacja w projektach współfinansowanych z **EFS+ oraz FST** zgodnie z „Wytycznymi dotyczącymi monitorowania postępu rzeczowego realizacji programów na lata 2021–2027” oraz **Załącznikiem nr 2, pkt 2 lit. c)**, gdzie ICDL (ECDL) wskazano jako przykład kwalifikacji nadawanej przez podmiot międzynarodowy.

Więcej informacji: <https://icdl.pl/projekty-unijne/>

Harmonogram

Liczba pozycji harmonogramu: 5

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 5 Wprowadzenie do cyberbezpieczeństwa. Zagrożenia tradycyjne i AI-enhanced. Socjotechnika 2.0. Bezpieczeństwo osobiste i tożsamość cyfrowa - prezentacja, ćwiczenia.	Eliasz Rafalski	21-08-2026	16:30	19:30	03:00

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 5 Identity & Access Management. Szyfrowanie i bezpieczne przetwarzanie danych. Bezpieczeństwo urządzeń, sieci, firewall, Zero Trust Architecture - prezentacja, ćwiczenia.	Eliasz Rafalski	22-08-2026	09:00	12:00	03:00
3 z 5 Przerwa	Eliasz Rafalski	22-08-2026	12:00	12:15	00:15
4 z 5 Rozpoznawanie incydentów i procedury reagowania. Symulacje ataków. Automatyzacja reagowania. Bezpieczna komunikacja i compliance - prezentacja, ćwiczenia.	Eliasz Rafalski	22-08-2026	12:15	14:30	02:15
5 z 5 Walidacja - test teoretyczny. Egzamin ICDL/ECDL.	-	22-08-2026	14:30	15:15	00:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 920,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	1 920,00 PLN
Koszt osobogodziny brutto	160,00 PLN

Koszt osobogodziny netto	160,00 PLN
W tym koszt walidacji brutto	300,00 PLN
W tym koszt walidacji netto	300,00 PLN
W tym koszt certyfikowania brutto	100,00 PLN
W tym koszt certyfikowania netto	100,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Eliasz Rafalski

Absolwent Wyższej Szkoły Pedagogicznej oraz Wyższej Szkoły Informatyki i Ekonomii TWP w Olsztynie. Obecnie doktorant w Instytucie Podstaw Informatyki Polskiej Akademii Nauk w Warszawie, gdzie prowadzi badania nad historią informatyki w medycynie. Posiada bogate doświadczenie jako wykładowca akademicki oraz trener szkoleń z zakresu aplikacji Microsoft Office, baz danych, programowania w Pythonie, C++, JavaScript, a także obsługi programów graficznych takich jak Adobe i CorelDRAW. Specjalizuje się również w zagadnieniach związanych ze sztuczną inteligencją. W ciągu ostatnich 5 lat przeprowadził ponad 200 godzin szkoleń z umiejętności cyfrowych. Od 2005 roku corocznie odnawia uprawnienia egzaminatora ICDL, co potwierdza jego zaangażowanie w rozwój kompetencji cyfrowych uczestników szkoleń.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy z Uczestników otrzymuje dostęp do OneDrive, gdzie znajdują się materiały szkoleniowe w wersji elektronicznej, tj. skrypt i zestawy do ćwiczeń.

Dodatkowo, Uczestnicy otrzymują rozwiązane podczas szkolenia zestawy ćwiczeń oraz inne materiały, które są tworzone w trakcie zajęć.

Warunki uczestnictwa

1. W przypadku egzaminu ICDL w formie zdalnej Uczestnik wyraża zgodę na zainstalowanie przed szkoleniem na swoim komputerze/laptopie (wyposażonym w głośnik, mikrofon oraz kamerę), z którego będzie zdawał egzamin aplikacji egzaminacyjnej PTI (wg. instrukcji Egzaminatora/Centrum Egzaminacyjnego).
2. Zawarcie przez Uczestnika umowy z Organizatorem na realizację usługi szkoleniowej.
3. Uczestnik powinien być obecny na minimum 80% godzin usługi szkoleniowej. Frekwencja potwierdzana jest na podstawie raportu z logowań.

Informacje dodatkowe

Uczestnik po zdaniu egzaminu otrzymuje zaświadczenie oraz **Europejski Certyfikat Umiejętności Komputerowych ICDL S3 - IT Security** w wersji elektronicznej. Certyfikat jest bezterminowy.

Zawarto umowę z WUP w Krakowie w ramach **Projektu „Małopolski pociąg do kariery – sezon 1”** oraz **Projektu „Nowy start w Małopolsce z EURESem”**

Zawarto umowę z WUP w Toruniu w ramach **Projektu "Kierunek – Rozwój"**

Zawarto umowę z WUP w Szczecinie na świadczenie usług rozwojowych z wykorzystaniem elektronicznych bonów szkoleniowych w ramach projektu **Zachodniopomorskie Bony Szkoleniowe**

Nasze szkolenie dostępne jest również w trybie indywidualnym, gwarantującym wygodne godziny spotkań dostosowane do Twoich potrzeb.

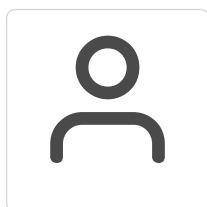
Podana cena dotyczy szkolenia dofinansowania w co najmniej 70% ze środków publicznych (zwolnienie z VAT na podst. § 3 ust. 1 pkt 14 rozp. Ministra Finansów z 20.12.2013 r. (Dz.U. 2018 poz. 701).

Warunki techniczne

Zanim weźmiesz udział w szkoleniu, zapoznaj się z następującymi informacjami:

1. Szkolenie odbywa się na **aplikacji Microsoft 365 (w tym Teams) udostępnianej przez Organizatora**. Nie jest wymagane posiadanie własnego oprogramowania.
2. Potrzebujesz komputera lub laptopa z głośnikiem, mikrofonem i kamerą (Procesor: 1 GHz lub szybszy, co najmniej z 2 rdzeniami, zgodny procesor 64-bitowy lub rozwiązanie SoC (System on a Chip). RAM: 4 GB. Miejsce na dysku: 64 GB lub więcej. Karta graficzna: zgodna z biblioteką DirectX 12 lub nowszą ze sterownikiem WDDM 2.0).
3. Musisz mieć dostęp do Internetu - przewodowego lub bezprzewodowego (3G lub 4G/LTE). Minimalna przepustowość to 600 kb/s, a rekomendowana 1,5 Mb/s.
4. System operacyjny: macOS 10.7 lub nowszy/Windows 10, 8, 7; na urządzeniu mobilnym: iOS lub Android.
5. Możesz korzystać z dowolnej przeglądarki internetowej: Edge, Chrome, Firefox, Safari, Internet Explorer itp.
6. Link umożliwiający uczestnictwo w spotkaniu on-line jest ważny podczas trwania całej usługi rozwojowej. Link zostanie przekazany Uczestnikom oraz Operatorom.
7. Jeśli chcesz przystąpić do egzaminu w formie zdalnej, musisz mieć możliwość zainstalowania aplikacji egzaminacyjnej PTI.

Kontakt



Administrator

E-mail info@aske.com.pl

Telefon (+48) 698 301 596