„TECHNIK CYBERBEZPIECZEŃSTWA 351304

KWALIFIKACJE WYODRĘBNIONE W ZAWODZIE

INF.11. Zarządzanie bezpieczeństwem systemów i sieci komputerowych

INF.12. Programowanie bezpiecznych aplikacji webowych

CELE KSZTAŁCENIA

Absolwent szkoły prowadzącej kształcenie w zawodzie technik cyberbezpieczeństwa powinien być przygotowany do wykonywania zadań zawodowych:

1) w zakresie kwalifikacji INF.11. Zarządzanie bezpieczeństwem systemów i sieci komputerowych:
   a) programowania w języku Python,
   b) projektowania i administracji relacyjnymi bazami danych,
   c) użytkowania, konfiguracji i utwardzania systemu Windows i Linux,
   d) testowania bezpieczeństwa systemów operacyjnych,
   e) konfiguracji i administrowania sieciami TCP/IP,
   f) testowania bezpieczeństwa sieci TCP/IP;
2) w zakresie kwalifikacji INF.12. Programowanie bezpiecznych aplikacji webowych:
   a) programowania w języku Java lub C#,

b) implementacji aplikacji webowych,
c) weryfikowania bezpieczeństwa implementacji aplikacji webowych,
d) przeprowadzania testów penetracyjnych aplikacji webowych.

EFEKTY KSZTAŁCENIA I KRYTERIA WERYFIKACJI TYCH EFEKTÓW

Do wykonywania zadań zawodowych w zakresie kwalifikacji INF.11. Zarządzanie bezpieczeństwem systemów i sieci komputerowych jest niezbędne osiągnięcie niżej wymienionych efektów kształcenia:

INF.11. Zarządzanie bezpieczeństwem systemów i sieci komputerowych	
INF.11.1. Bezpieczeństwo i higiena pracy	
Efekty kształcenia	Kryteria weryfikacji
Uczeń:	Uczeń:
1) charakteryzuje warunki i organizację pracy zapewniające wymagany poziom ochrony zdrowia i życia przed zagrożeniami występującymi w środowisku pracy	1) wymienia przepisy prawa dotyczące bezpieczeństwa i higieny pracy, ochrony przeciwpożarowej, ochrony środowiska i ergonomii 2) identyfikuje regulacje wewnątrzzakładowe dotyczące bezpieczeństwa i higieny pracy 3) opisuje zasady ochrony przeciwpożarowej w środowisku pracy 4) określa wymagania ergonomiczne na stanowisku pracy
2) opisuje prawa i obowiązki pracownika oraz pracodawcy w zakresie bezpieczeństwa i higieny pracy	1) wymienia obowiązki pracodawcy i pracowników w zakresie bezpieczeństwa i higieny pracy 2) wymienia rodzaje profilaktycznych badań lekarskich 3) wymienia rodzaje obowiązkowych szkoleń z zakresu bezpieczeństwa i higieny pracy 4) identyfikuje system kar dla pracownika z tytułu nieprzestrzegania przepisów bezpieczeństwa i higieny pracy w trakcie wykonywania pracy

	5) wskazuje obowiązki pracownika i pracodawcy w zakresie zapobiegania wypadkom przy pracy i chorobom zawodowym 6) wymienia rodzaje świadczeń z tytułu wypadku przy pracy i chorób zawodowych 7) wymienia instytucje oraz służby działające w zakresie ochrony pracy i ochrony środowiska 8) wskazuje zadania i uprawnienia instytucji oraz służb działających w zakresie ochrony pracy i ochrony środowiska
3) określa skutki oddziaływania czynników szkodliwych na organizm człowieka	1) określa zagrożenia występujące w środowisku pracy 2) określa skutki oddziaływania czynników psychofizycznych na organizm człowieka 3) opisuje skutki oddziaływania czynników niebezpiecznych i uciążliwych na organizm człowieka 4) wyjaśnia pojęcia choroba zawodowa i wypadek przy pracy
4) przestrzega zasad bezpieczeństwa i higieny pracy oraz przepisów prawa dotyczących ochrony przeciwpożarowej i ochrony środowiska występujących w zawodzie	1) stosuje zasady zachowania się w przypadku pożaru 2) rozróżnia środki gaśnicze ze względu na zakres ich stosowania 3) obsługuje komputery i urządzenia na stanowiskach pracy zgodnie z zasadami i przepisami bezpieczeństwa i higieny pracy, ochrony przeciwpożarowej i ochrony środowiska 4) stosuje zasady postępowania z odpadami niebezpiecznymi

5) organizuje stanowisko pracy zgodnie z wymaganiami ergonomii oraz przepisami dotyczącymi bezpieczeństwa i higieny pracy, ochrony przeciwpożarowej i ochrony środowiska	1) identyfikuje czynniki, które należy brać pod uwagę przy organizacji stanowiska pracy zgodnie z zasadami ergonomii 2) stosuje wymagania ergonomiczne dla stanowiska pracy 3) wskazuje obowiązki pracodawcy w zakresie organizacji czasu pracy pracownika 4) identyfikuje działania prewencyjne zapobiegające powstawaniu zagrożeń na stanowisku pracy 5) rozpoznaje sytuacje grożące pożarem na stanowisku pracy 6) stosuje sprzęt i materiały ekologiczne na stanowisku pracy
6) stosuje środki ochrony indywidualnej i zbiorowej podczas wykonywania zadań zawodowych	1) identyfikuje środki ochrony zbiorowej 2) wskazuje środki ochrony zabezpieczające przed hałasem w pracy biurowej 3) identyfikuje wymagania w zakresie oświetlenia, temperatury i mikroklimatu pomieszczeń biurowych 4) stosuje środki ochrony zapobiegające porażeniem prądem w pracy biurowej 5) stosuje środki ochrony zapobiegające pogorszeniu wzroku i zniekształceniu kręgosłupa 6) dobiera środki ochrony zbiorowej do rodzaju zagrożeń w pracy biurowej
7) udziela pierwszej pomocy w sytuacji nagłego zagrożenia zdrowotnego	1) opisuje podstawowe symptomy wskazujące na stany nagłego zagrożenia zdrowotnego 2) ocenia sytuację poszkodowanego na podstawie analizy objawów obserwowanych u poszkodowanego

	3) zabezpiecza siebie, poszkodowanego i miejsce wypadku 4) układa poszkodowanego w pozycji bezpiecznej 5) powiadamia odpowiednie służby 6) prezentuje udzielanie pierwszej pomocy w urazowych stanach nagłego zagrożenia zdrowotnego (np. krwotok, zmiażdżenie, amputacja, złamanie, oparzenie) 7) prezentuje udzielanie pierwszej pomocy w nieurazowych stanach nagłego zagrożenia zdrowotnego (np. omdlenie, zawał, udar) 8) wykonuje resuscytację krążeniowo-oddechową na fantomie zgodnie z wytycznymi Polskiej Rady Resuscytacji i Europejskiej Rady Resuscytacji
INF.11.2. Podstawy cyberbezpieczeństwa systemów IT	
Efekty kształcenia	Kryteria weryfikacji
Uczeń:	Uczeń:
1) stosuje podstawową terminologię związaną z cyberbezpieczeństwem	1) wyjaśnia pojęcie cyberbezpieczeństwa 2) wyjaśnia pojęcie cyberataku 3) wyjaśnia pojęcie triady CIA (Confidentiality – Poufność, Integrity – Integralność, Availability – Dostępność) 4) opisuje znaczenie triady CIA dla bezpieczeństwa informacji 5) określa znaczenie posiadanych uprawnień i zgody właściciela systemu dla legalności działań w sieciach komputerowych (etyczny hacking vs. przestępstwo)

2) charakteryzuje zagrożenia cyberbezpieczeństwa	1) rozróżnia zagrożenia wewnętrzne i zewnętrzne w systemach IT 2) wskazuje zależności między zagrożeniami a podatnościami 3) opisuje rodzaje ataków: a) włamania sieciowe b) ataki za pomocą malware c) ataki typu DoS/DDoS d) ataki fizyczne e) ataki socjotechniczne 3) opisuje działanie różnych typów złośliwego oprogramowania (np. wirus, spyware, ransomware, trojan, backdoor) 4) wskazuje cele i potencjalne skutki ataków: a) nieuprawnione pozyskanie informacji b) nieuprawniona modyfikacja danych c) kradzież tożsamości d) zakłócenie działania systemu e) wymuszenie okupu 5) opisuje proste scenariusze ataków: a) ataki phishingowe z wykorzystaniem poczty elektronicznej b) podrzucenie zainfekowanego nośnika USB c) próby automatycznego łamania haseł d) podsłuch
3) charakteryzuje i analizuje ataki socjotechniczne	1) wyjaśnia mechanizm działania ataków socjotechnicznych 2) rozróżnia ataki socjotechniczne typu phishing i spear phishing 3) podaje przykłady realizacji ataku socjotechnicznego z wykorzystaniem: a) poczty elektronicznej

	b) nośnika USB c) rozmowy telefonicznej d) wiadomości tekstowej e) fałszywego pracownika 4) omawia mechanizmy obrony przed atakami socjotechnicznymi, również przeprowadzonymi z wykorzystaniem narzędzi sztucznej inteligencji: a) weryfikacja nadawcy b) weryfikacja linku w wiadomości c) weryfikacja rozmówcy d) weryfikacja tożsamości 5) stosowanie niezależnych kanałów komunikacji wspomaganie oceny wiarygodności przekazu z wykorzystaniem narzędzi sztucznej inteligencji
4) charakteryzuje mechanizmy kontroli tożsamości	1) wyjaśnia pojęcie identyfikacji użytkownika 2) wyjaśnia pojęcie uwierzytelniania użytkownika i podaje przykłady metod uwierzytelniania (np. hasło, biometria, kod autoryzacyjny) 3) wyjaśnia pojęcie wzajemnego (dwustronnego) uwierzytelniania 4) wyjaśnia znaczenie procesu uwierzytelniania dla ochrony zasobów systemów
5) stosuje uwierzytelnianie wieloskładnikowe MFA (Multi-Factor Authentication)	1) wyjaśnia pojęcie uwierzytelniania wieloskładnikowego 2) wymienia składniki MFA („coś, co wie”, „coś, co ma”, „coś, czym jest”) 3) podaje przykłady metod MFA (np. OTP (One-Time Password), Google Authenticator TOTP (Time-Based OTP), token, biometria, techniki behawioralne)

	4) wyjaśnia, dlaczego MFA zwiększa poziom bezpieczeństwa w porównaniu do uwierzytelniania jednoskładnikowego 5) podaje praktyczne przykłady zastosowania MFA
6) stosuje zasady kontroli dostępu	1) rozróżnia procesy uwierzytelniania, autoryzacji i kontroli dostępu 2) opisuje zasadę najmniejszych uprawnień 3) wyjaśnia ideę przydzielania użytkownikowi tylko niezbędnych uprawnień 4) wskazuje zagrożenia wynikające z nadmiernych uprawnień 5) podaje przykłady zastosowania zasady najmniejszych uprawnień w systemach operacyjnych i aplikacjach 6) uzasadnia znaczenie zasady najmniejszych uprawnień w ograniczaniu skutków incydentów bezpieczeństwa 7) stosuje modele i mechanizmy kontroli dostępu (np. kontrola oparta na rolach (RBAC), kontrola oparta na atrybutach (ABAC), kontrola obowiązkowa (MAC), listy kontroli dostępu (ACL))
7) wyjaśnia podstawy kryptografii i jej zastosowanie w bezpieczeństwie IT	1) rozróżnia dane wymagające ochrony i dane jawne 2) wyjaśnia znaczenie kryptografii w bezpieczeństwie systemów i aplikacji 3) wyjaśnia sposób działania funkcji skrótu (hash) oraz jej przeznaczenie (weryfikacja integralności danych, podpisy cyfrowe) 4) wskazuje funkcje skrótu uznane za aktualny standard bezpieczeństwa

	5) wyjaśnia przeznaczenie i sposób działania szyfrów symetrycznych 6) wskazuje szyfry symetryczne uznane za aktualny standard bezpieczeństwa 7) wyjaśnia sposób działania szyfrów asymetrycznych oraz pojęcia dotyczące klucza publicznego i prywatnego 8) wyjaśnia mechanizm oraz przeznaczenie podpisu cyfrowego 9) omawia rolę kryptografii asymetrycznej w wymianie kluczy, uwierzytelnianiu i podpisach cyfrowych 10) wskazuje szyfry asymetryczne uznane za aktualny standard bezpieczeństwa 11) wyjaśnia potencjalny wpływ komputerów kwantowych na klasyczną kryptografię 12) wyjaśnia hybrydowe mechanizmy post-kwantowe (PQC)
8) wykonuje podstawowe operacje kryptograficzne w środowisku testowym	1) wyjaśnia pojęcia certyfikatu cyfrowego, urzędu certyfikacji, infrastruktury klucza publicznego (PKI), łańcucha certyfikacji 2) interpretuje informacje w certyfikacie (np. okres ważności, wystawcę, podmiot, algorytm, numer seryjny) 3) wyjaśnia rolę certyfikatów w zapewnieniu autentyczności i integralności 4) tworzy parę kluczy asymetrycznych (RSA lub ECC) 5) przechowuje klucze w bezpieczny sposób 6) generuje własne certyfikaty użytkownika lub serwera 7) generuje certyfikat własnego CA (Certificate Authority)

	8) weryfikuje ważność certyfikatów 9) stosuje certyfikaty do generowania i weryfikacji podpisów cyfrowych 10) stosuje certyfikaty do zabezpieczenia sesji zdalnego dostępu w systemach Windows i Linux 11) szyfruje i deszyfruje dane przy użyciu dostępnych narzędzi 12) oblicza skróty dla przykładowych danych i wskazuje efekty zmiany danych na wartość skrótu
9) charakteryzuje organizację i funkcjonowanie KSC (Krajowego Systemu Cyberbezpieczeństwa)	1) wyjaśnia cel funkcjonowania KSC oraz jego znaczenie dla bezpieczeństwa państwa i systemów informatycznych w Polsce 2) opisuje strukturę KSC, wskazując role poszczególnych podmiotów, w tym w szczególności Computer Security Incident Response Teamów (CSIRT-ów) oraz organów właściwych, a także operatorów usług kluczowych, dostawców usług cyfrowych oraz podmiotów publicznych 3) wyjaśnia pojęcie infrastruktury krytycznej i omawia znaczenie systemów teleinformatycznych dla jej funkcjonowania oraz wskazuje zależność między cyberbezpieczeństwem a zarządzaniem kryzysowym 4) wymienia podstawowe obowiązki operatorów usług kluczowych, 5) wyjaśnia pojęcie incydentu bezpieczeństwa, w tym incydentu krytycznego, oraz wyjaśnia rolę współpracy w procesie reagowania na zagrożenia

	6) omawia odpowiedzialność prawną (karną i administracyjną) związaną z nieuprawnionym dostępem do informacji oraz niewypełnieniem obowiązków nałożonych przez ustawę o KSC
10) rozpoznaje właściwe normy i procedury oceny zgodności podczas realizacji zadań przewozowych	1) wymienia cele normalizacji krajowej 2) podaje definicje i cechy normy 3) rozróżnia oznaczenie normy krajowej i normy międzynarodowej, w tym norm europejskich 4) korzysta ze źródeł informacji dotyczących norm i procedur oceny zgodności
INF.11.3. Programowanie w języku Python	
Efekty kształcenia	Kryteria weryfikacji
Uczeń:	Uczeń:
1) stosuje podstawy programowania w języku Python	1) tworzy środowisko do programowania w języku Python 2) instaluje i importuje pakiety 3) przetwarza i konwertuje liczby niedziesiątkowe: dwójkowe, ósemkowe, szesnastkowe 4) stosuje podstawy logiki boolowskiej i prawa De Morgana 5) wykorzystuje podstawowe typy danych języka Python 6) stosuje podstawowe operacje na ciągach znaków (stringach) 7) stosuje podstawowe operacje na plikach 8) stosuje instrukcje sterowania wykonaniem programu: instrukcje warunkowe, instrukcje wyboru, pętle 9) stosuje iterację i rekurencję

2) implementuje proste programy w języku Python	1) wykorzystuje struktury danych: lista (kolejka FIFO), stos (kolejka LIFO), słownik 2) implementuje proste algorytmy sortowania, wyszukiwania 3) korzysta z funkcji, wyrażeń lambda, domknięć (closures) oraz generatorów 4) korzysta z narzędzi programistycznych wspierających pracę własną i zespołową (IDE, GIT)
3) implementuje zaawansowane programy w języku Python	1) dokumentuje programy w kodzie źródłowym (docstring) 2) wykorzystuje klasy i hierarchie klas 3) stosuje mechanizmy enkapsulacji danych dostępne w języku Python 4) implementuje programy asynchroniczne (asyncio) (np. do pobierania danych z wielu usług webowych) 5) wykorzystuje wyjątki
4) tworzy poprawne i bezpieczne programy w języku Python	1) stosuje podejście defensywne: a) zabezpiecza się przed błędami podczas wykonywania programu b) obsługuje błędy c) przechwytuje i obsługuje wyjątki (try/except/finally) d) stosuje konwersje typów 2) zarządza zasobami systemu operacyjnego (pliki, gniazda, wątki) w sposób deterministyczny: a) zwalnia zasoby, gdy przestają być potrzebne b) stosuje instrukcję with 3) zabezpiecza program przed wyciekami pamięci

	4) stosuje zasady bezpiecznego programowania: a) unikanie niebezpiecznych konstrukcji związanych z dynamicznym wykonywaniem kodu: eval, exec, pickle b) używanie właściwych typów danych do przechowywania sekretów c) walidacja danych wejściowych d) walidacja ścieżek do systemu plików 5) wykonuje automatyczne testy oprogramowania 6) wykorzystuje narzędzia do weryfikacji programów Python pod kątem obecności błędów bezpieczeństwa 7) wykorzystuje narzędzia sztucznej inteligencji do: a) generacji kodu b) generacji testów na podstawie opisu lub dokumentacji docstring c) weryfikacji programów pod kątem poprawności i bezpieczeństwa
5) wykorzystuje język Python do przetwarzania danych oraz automatyzacji działań operacyjnych w cyberbezpieczeństwie	1) wykorzystuje biblioteki do analizy danych, (np. Pandas, NumPy) do wczytywania, oczyszczania i transformacji dużych zbiorów danych (np. logów, baz danych, zrzutów ruchu sieciowego) 2) wykrywa proste anomalie i incydenty (np. skanowanie portów, eksfiltrację danych) poprzez korelację danych z różnych źródeł 3) tworzy wizualizacje danych (np. wykresy rozkładu, mapy ciepła logowań) w celu identyfikacji trendów i wektorów ataków

	4) automatyzuje proces zbierania informacji oraz weryfikacji podatności przy użyciu bibliotek sieciowych (np. Requests, Socket, Scapy) 5) buduje skrypty integrujące różne narzędzia bezpieczeństwa poprzez ich interfejsy API (np. VirusTotal, Shodan, systemy Security Information and Event Management (SIEM)) 6) automatyzuje powtarzalne czynności administracyjne związane z utwardzaniem systemu (np. masowa zmiana konfiguracji, sprawdzanie uprawnień plików) 7) wykorzystuje proste mechanizmy parsowania i generowania raportów technicznych w formatach takich jak JSON, XML, CSV, Markdown czy HTML
INF.11.4. Projektowanie i administracja relacyjnymi bazami danych	
Efekty kształcenia	Kryteria weryfikacji
Uczeń:	Uczeń:
1) projektuje struktury relacyjnych baz danych przy użyciu języka SQL z uwzględnieniem mechanizmów bezpieczeństwa	1) wyjaśnia pojęcia związane z budową systemów baz danych: a) tabela b) wiersz/rekord c) kolumna d) klucz główny e) typy danych f) relacje g) indeksowanie h) partycjonowanie i) mechanizmy transakcyjne j) więzy spójności k) audytowalność operacji

	2) dobiera typy danych ograniczające ryzyko błędów przepełnienia oraz określa rygorystyczne więzy integralności (np. klucze główne, klucze obce, ograniczenia CHECK oraz wymóg unikalności i niepustości danych) 3) projektuje schematy baz danych z fizyczną i logiczną separacją danych wrażliwych 4) stosuje zasady normalizacji bazy danych w celu eliminacji redundancji 5) tworzy diagramy związków encji dla systemów informatycznych 6) planuje mechanizmy transakcyjne zapewniające spójność danych
2) tworzy i modyfikuje struktury bazy danych przy użyciu języka SQL	1) stosuje polecenia języka definicji danych do tworzenia izolowanych schematów i przestrzeni tabel 2) modyfikuje struktury bazy danych w sposób zapewniający ciągłość działania i bezpieczeństwo danych 3) tworzy i zarządza indeksami w celu optymalizacji szybkości dostępu do danych 4) implementuje widoki ułatwiające dostęp do wybranych informacji 5) stosuje klucze obce oraz mechanizmy kaskadowe w celu utrzymania spójności referencyjnej 6) dokumentuje proces tworzenia i zmian w schemacie bazy danych 7) wykorzystuje narzędzia do wersjonowania schematów baz danych i śledzenia zmian w strukturach

3) zarządza danymi w relacyjnych bazach danych z zachowaniem najwyższych standardów poufności i rozliczalności	1) stosuje polecenia języka manipulacji danymi do wprowadzania rekordów w sposób umożliwiający pełny audyt operacji 2) wykonuje masowe aktualizacje danych z wykorzystaniem transakcji i punktów przywracania 3) przeprowadza bezpieczne usuwanie danych z bazy, zgodnie z procedurami 4) tworzy zapytania wybierające dane, z uwzględnieniem mechanizmów maskowania danych wrażliwych 5) weryfikuje poprawność wprowadzonych danych pod kątem zdefiniowanych typów 6) stosuje mechanizmy transakcyjne w celu wycofania lub zatwierdzenia zmian
4) tworzy złożone zapytania SQL	1) tworzy zapytania korelujące dane z wielu tabel logów (wyrażenia JOIN) i zdarzeń systemowych 2) stosuje funkcje agregujące do identyfikacji statystycznych anomalii i prób ataków brute-force na poziomie bazy 3) buduje złożone podzapytania w celu identyfikacji nieautoryzowanych powiązań między użytkownikami a danymi 4) wykorzystuje narzędzia generatywnej sztucznej inteligencji do generowania złożonych zapytań SQL na podstawie opisu naturalnego 5) przeprowadza refaktoryzację zapytań SQL pod kątem czytelności i wydajności przy użyciu narzędzi generatywnej sztucznej inteligencji

	6) weryfikuje ręcznie kod SQL wygenerowany przez narzędzia sztucznej inteligencji
5) administruje systemami zarządzania bazą danych (SZBD)	1) instaluje i konfiguruje środowisko serwera bazy danych 2) konfiguruje dostęp zdalny i lokalny do serwera bazy danych 3) zarządza przestrzenią dyskową i wydajnością procesów bazodanowych 4) wykonuje pełne i przyrostowe kopie zapasowe baz danych 5) przeprowadza procedury odtwarzania bazy danych po awarii 6) planuje harmonogram zadań administracyjnych (backupy, czyszczenie logów) 7) monitoruje logi systemowe w celu wykrywania błędów i prób nadużyć
6) wdraża mechanizmy autoryzacji w systemach zarządzania bazami danych i nadzoruje dostępność zasobów bazodanowych	1) konfiguruje uwierzytelnianie wieloskładnikowe (np. wykorzystanie kodów TOTP w aplikacji mobilnej lub kluczy sprzętowych Universal 2nd Factor (U2F) dla personelu z uprawnieniami administracyjnymi) 2) przydziela oraz cofa dostęp do konkretnych elementów schematu (np. ograniczanie widoczności kolumn z numerami PESEL lub procedur zmieniających stany magazynowe zgodnie z dokumentacją) 3) buduje hierarchię ról i grup, implementując w praktyce regułę najniższych przywilejów 4) wprowadza restrykcyjne wymogi dotyczące parametrów haseł (np. minimalna długość znaków, znaki specjalne, zakaz używania

	haseł historycznych) oraz ich wymuszoną rotację dla kont serwisowych 5) wykorzystuje zewnętrzne magazyny sekretów do bezpiecznego dostarczania danych logowania do aplikacji bez zapisywania ich w plikach konfiguracyjnych 6) monitoruje procesy autoryzacji pod kątem wykrywania prób eskalacji uprawnień (np. sytuacji, w której zwykły użytkownik próbuje wywołać komendy zarezerwowane dla superużytkownika) 7) integruje system bazy danych z zewnętrznymi dostawcami tożsamości (np. poprzez protokoły Lightweight Directory Access Protocol (LDAP) w usłudze Active Directory, aby scentralizować weryfikację pracowników w przedsiębiorstwie) 8) definiuje okna czasowe oraz limity sesji dla kont o charakterze technicznym, ograniczając możliwość ich wykorzystania poza godzinami planowanych prac serwisowych
7) implementuje mechanizmy ochrony i monitorowania bezpieczeństwa danych w systemach zarządzania bazami danych	1) wdraża szyfrowanie danych w spoczynku, co chroni pliki bazy danych przed odczytem w przypadku ich fizycznej kradzieży z serwera 2) interpretuje dzienniki zdarzeń pod kątem wykrywania nietypowych wzorców zapytań, (np. gwałtowny wzrost liczby operacji SELECT na danych wrażliwych, które mogą świadczyć o próbie eksfiltracji danych) 3) przystosowuje schematy bazodanowe do wymogów audytowych poprzez implementację wyzwalaczy (triggers)

	rejestrujących każdą zmianę w kluczowych rekordach wraz z informacją o autorze modyfikacji 4) opracowuje automatyczne reguły alarmowe, (np. wysyłanie powiadomień na kanał komunikatora technicznego lub e-mail)natychmiast po wykryciu krytycznych błędów bazy 5) blokuje nieużywane funkcje sieciowe i porty na poziomie silnika bazy danych, aby zminimalizować powierzchnię potencjalnego ataku: a) dezaktywuje funkcje pozwalające na bezpośrednią interakcję bazy z powłoką systemu operacyjnego (np. COPY FROM PROGRAM w PostgreSQL) co zapobiega wykonaniu złośliwego kodu na poziomie serwera b) blokuje zbędne protokoły sieciowe oraz ogranicza nasłuchiwanie usługi wyłącznie do wymaganych interfejsów, (np. bindowanie do adresu localhost lub konkretnego VLAN-u) zamiast wszystkich dostępnych interfejsów c) wyłącza wbudowane komponenty rozszerzające, takie jak moduły do bezpośredniej wysyłki e-mail z bazy czy obsługa skryptów zewnętrznych (np. w językach Python/R) jeśli nie są one niezbędne dla aplikacji d) zamyka porty komunikacyjne na systemowej zaporze ogniowej (firewall), dopuszczając ruch wyłącznie z

	autoryzowanych adresów IP serwerów aplikacji e) wyłącza funkcję automatycznego odnajdywania serwerów bazy w sieci w systemie zarządzania bazą danych, aby utrudnić potencjalnemu intruzowi lokalizację instancji 6) wykonuje systematyczne przeglądy konfiguracji systemu zarządzania bazą danych pod kątem znanych luk: a) weryfikuje status kont domyślnych i technicznych, wymuszając zmianę fabrycznych haseł lub całkowitą blokadę profili predefiniowanych przez producenta (np. konta sa, root, admin, postgres) aby zapobiec atakom typu credential stuffing b) analizuje listę aktywnych sesji oraz uprawnień gościa, identyfikując i zamykając połączenia porzucone, niezamknięte lub nieposiadające uzasadnienia w bieżącej architekturze aplikacji (np. usuwanie schematów GUEST lub PUBLIC) c) konfrontuje bieżące parametry serwera z uznanymi wzorcami bezpieczeństwa (np. wytyczne Center for Internet Security (CIS) Benchmarks lub Security Technical Implementation Guides (STIG)) eliminując odstępstwa od zalecanej konfiguracji bezpiecznej d) identyfikuje brakujące aktualizacje i poprawki krytyczne, weryfikując wersję

	silnika bazy pod kątem publicznie ogłoszonych luk (baza Common Vulnerabilities and Exposures (CVE)) oraz biuletynów bezpieczeństwa dostawcy e) kontroluje uprawnienia na poziomie systemu operacyjnego, sprawdzając, czy dostęp do plików danych, logów transakcyjnych i plików konfiguracyjnych bazy jest ograniczony wyłącznie do konta usługi silnika SQL f) wykrywa i usuwa pozostałości po procesach wdrożeniowych, takie jak bazy przykładowe, skrypty demonstracyjne czy nieużywane procedury składowane, które mogą stanowić wektor ataku g) ewaluuje protokoły i szyfry komunikacyjne, wymuszając stosowanie bezpiecznych wersji TLS oraz wyłączając podatne na ataki, przestarzałe standardy (np. SSL 3.0, TLS 1.0/1.1) 7) rozmieszcza kopie zapasowe w różnych lokalizacjach (stosując zasadę 3-2-1, czyli 3 kopie na 2 różnych nośnikach, z czego jedna w innej lokalizacji fizycznej), zapewniając przetrwanie danych w razie pożaru serwerowni
8) identyfikuje i przeciwdziała podatnościom typu SQL Injection	1) wyjaśnia mechanizm działania i skutki ataku typu SQL Injection 2) identyfikuje miejsca w aplikacjach podatne na wstrzykiwanie kodu SQL

	3) stosuje parametryzację zapytań w celu ochrony bazy 4) wdraża walidację i sanityzację danych wejściowych od użytkownika 5) konfiguruje bazę danych tak, aby zminimalizować skutki udanego wstrzyknięcia kodu 6) przeprowadza testy bezpieczeństwa pod kątem obecności luk typu injection
9) obsługuje nierelacyjne systemy baz danych (NoSQL)	1) rozróżnia nierelacyjne i relacyjne bazy danych 2) instaluje i konfiguruje system zarządzania bazą danych typu dokumentowego 3) wykonuje podstawowe operacje na dokumentach i kolekcjach NoSQL (tworzenie, odczyt, aktualizacja, usuwanie) 4) projektuje proste struktury danych w formacie JSON/BSON na potrzeby baz NoSQL 5) identyfikuje zagrożenia bezpieczeństwa specyficzne dla baz nierelacyjnych 6) stosuje narzędzia sztucznej inteligencji do migracji lub integracji danych między SQL a NoSQL 7) dobiera rodzaj bazy danych (SQL/NoSQL) do specyficznych wymagań projektu
INF.11.5. Administrowanie sieciami TCP/IP	
Efekty kształcenia	Kryteria weryfikacji
Uczeń:	Uczeń:
1) wyjaśnia podstawowe pojęcia i zasady funkcjonowania sieci komputerowych	1) wyjaśnia pojęcie sieci komputerowej oraz cele wymiany danych pomiędzy urządzeniami

	2) opisuje rodzaje sieci komputerowych (np. LAN, MAN, WAN) oraz podaje przykłady ich zastosowania 3) wyjaśnia pojęcie transmisji danych oraz znaczenie standardów i protokołów w komunikacji sieciowej 4) rozróżnia sieci przewodowe i bezprzewodowe oraz wskazuje różnice w sposobie transmisji danych 5) rozróżnia podstawowe elementy sieci komputerowej (urządzenia końcowe, medium transmisyjne, urządzenia pośredniczące) 6) opisuje topologie sieci komputerowych (np. gwiazdy, magistrali, pierścienia) oraz wskazuje ich zalety i ograniczenia
2) charakteryzuje działanie sieci komputerowych w oparciu o modele OSI/TCP-IP oraz protokoły transmisji danych	1) opisuje warstwy modeli ISO/OSI i TCP/IP oraz przypisuje im protokoły 2) wyjaśnia rolę protokołów Ethernet, ARP, IP, TCP i UDP w komunikacji sieciowej 3) opisuje budowę adresu IPv4 (adres IP, maska, adres sieci, adres rozgłoszeniowy) 4) rozróżnia adresowanie unicast, broadcast i multicast oraz podaje przykłady ich zastosowania 5) porównuje działanie protokołów TCP i UDP 6) opisuje mechanizm zestawiania i zamykania połączenia TCP (three-way handshake) 7) wskazuje zależność pomiędzy protokołami warstwy sieciowej i transportowej, a protokołami warstwy aplikacji (na przykładzie HTTP)

	8) wyjaśnia rolę protokołu DNS w procesie translacji nazw adresów 9) wyjaśnia pojęcie routingu oraz opisuje rolę routera w komunikacji pomiędzy sieciami IP 10) opisuje pojęcie sniffingu sieciowego oraz przeznaczenie narzędzia Wireshark jako analizatora ruchu sieciowego, z uwzględnieniem zastosowań diagnostycznych i bezpieczeństwa
3) stosuje adresację IPv4 i IPv6	1) rozpoznaje adresy IPv4 i IPv6 oraz określa ich budowę, w tym zapis adresów z wykorzystaniem notacji Classless Inter-Domain Routing (CIDR) 2) rozróżnia adresy publiczne i prywatne oraz określa ich zastosowanie 3) identyfikuje adres sieci, adres rozgłoszeniowy i adres hosta na podstawie adresu IP i notacji CIDR 4) opisuje różnice pomiędzy statyczną i dynamiczną adresacją IP oraz opisuje rolę protokołu DHCP w automatycznym przydzielaniu adresów 5) wyjaśnia znaczenie adresacji IP dla bezpieczeństwa i identyfikacji źródeł ruchu
4) konfiguruje podstawowe parametry sieciowe urządzeń końcowych	1) konfiguruje podstawowe parametry sieciowe hosta, w tym nazwę hosta, adresację statyczną i dynamiczną (DHCP), maskę podsieci, bramę domyślną oraz serwer DNS 2) weryfikuje ustawienia sieciowe przy użyciu narzędzi arp, ipconfig lub ifconfig, route 3) diagnozuje problemy z łącznością sieciową na stacji roboczej (brak połączenia z siecią

	Wi-Fi, awaria karty sieciowej, adres IP z niewłaściwej sieci, konflikt IP, błędny adres)
	serwera DNS, stan interfejsu sieciowego) 4) sprawdza poprawność rozwiązywania nazw domenowych 5) sprawdza podstawowe informacje o domenie w publicznych rejestrach (np. WHOIS, RDAP, ccTLD) i wyjaśnia ich znaczenie dla bezpieczeństwa użytkownika 6) wyjaśnia wpływ błędnej konfiguracji hosta na bezpieczeństwo sieci
5) posługuje się podstawowymi narzędziami diagnostycznymi sieci TCP/IP	1) wykorzystuje polecenie ping do sprawdzania osiągalności hostów 2) stosuje traceroute do analizy trasy pakietów w sieci 3) interpretuje informacje uzyskiwane za pomocą polecenia netstat, w tym wskazuje porty otwarte przez konkretne procesy 4) wykorzystuje narzędzia do testowania połączeń sieciowych (np. netcat)
6) przeprowadza podstawową konfigurację podsieci	1) wyjaśnia różnice między przełączaniem a routowaniem 2) wyjaśnia pojęcie mostkowania (bridgingu) oraz opisuje jego zastosowanie w łączeniu segmentów sieci na poziomie warstwy drugiej 3) konfiguruje podstawowe parametry przełączników i routerów, w tym: a) sprawdza aktualną konfigurację urządzenia sieciowego

	b) ustawia nazwę urządzenia oraz podstawowe zabezpieczenie dostępu administracyjnego c) włącza i wyłącza interfejs sieciowy oraz sprawdza jego stan d) przypisuje adres IP do interfejsu routera e) konfiguruje podstawową trasę domyślną f) testuje łączność sieciową z poziomu urządzenia sieciowego g) sprawdza zawartość tablicy routingu oraz interpretuje podstawowe wpisy (sieć lokalna, trasa domyślna) 3) konfiguruje bezpieczny dostęp do sieci bezprzewodowych, w tym: a) SSID b) standard zabezpieczenia (WPA2/WPA3) c) hasło dostępu d) wyłączenie funkcji WPS e) sieć dla gości
7) stosuje mechanizmy segmentacji i kontroli ruchu w sieciach TCP/IP	1) wyjaśnia znaczenie segmentacji sieci dla bezpieczeństwa, 2) wyjaśnia znaczenie pojęć: a) topologia gwiazdy b) strefa zdemilitaryzowana (DMZ) c) router brzegowy, rdzeniowy, agregacyjny d) strefa wewnętrzna (użytkownika) 3) tworzy i konfiguruje sieci VLAN 4) konfiguruje połączenia typu trunk 5) stosuje listy kontroli dostępu (ACL) do ograniczania ruchu sieciowego 6) konfiguruje podstawowe reguły sprzętowej zapory sieciowej

	7) konfiguruje podstawowe połączenia VPN, (np. OpenVPN, WireGuard, IPsec)
8) konfiguruje mechanizmy routingu i translacji	1) tworzy i modyfikuje trasy statyczne 2) rozpoznaje protokoły routingu dynamicznego i opisuje ich zastosowanie 3) konfiguruje translację adresów sieciowych (NAT) oraz translację numerów portów (port forwarding) 4) wyjaśnia wpływ NAT na bezpieczeństwo i analizę ruchu sieciowego

INF.11.6. Użytkowanie, konfiguracja i utwardzanie systemu Windows i Linux	
Efekty kształcenia	Kryteria weryfikacji
Uczeń:	Uczeń:
1) charakteryzuje architekturę i podstawowe mechanizmy bezpieczeństwa systemów operacyjnych	1) opisuje proces rozruchu systemu operacyjnego (BIOS/UEFI, bootloader) 2) rozróżnia rodzaje systemów plików i ich podstawowe cechy 3) opisuje mechanizmy ochrony i izolacji pamięci w systemach Windows i Linux 4) identyfikuje modele uprawnień użytkowników i grup (np. SID w Windows, UID/GID w Linux) 5) wyjaśnia różnicę między trybem użytkownika a trybem jądra 6) opisuje rolę jądra systemu w zarządzaniu bezpieczeństwem operacji 7) wymienia podstawowe rodzaje zagrożeń dla architektury systemu operacyjnego 8) wyjaśnia pojęcie powierzchni ataku w kontekście systemów komputerowych
2) analizuje architekturę systemów operacyjnych pod kątem	1) wyjaśnia bezpieczeństwo przejść między trybem użytkownika a trybem jądra oraz

mechanizmów ochronnych i wektorów ataków	ryzyka z nimi związane (np. eskalacja uprawnień) 2) analizuje mechanizmy ochrony pamięci (np. ASLR, DEP) pod kątem mitygacji exploitów 3) ocenia wpływ specyfiki systemów plików na bezpieczeństwo i poufność danych 4) omawia bezpieczeństwo łańcucha rozruchu (Secure Boot, Trusted Boot) w kontekście ochrony przed rootkitami 5) analizuje wpływ modeli uprawnień na bezpieczeństwo obiektów systemowych w środowiskach wielodostępowych 6) weryfikuje integralność jądra systemu oraz autentyczność sterowników 7) identyfikuje wektory ataków wykorzystujące specyficzne podatności architektury systemów operacyjnych
3) wdraża systemy operacyjne w standardzie utwardzonej instalacji	1) tworzy nośniki instalacyjne dla systemów Windows i Linux 2) przeprowadza partycjonowanie dysków z uwzględnieniem izolacji katalogów systemowych i stosowania flag montowania ograniczających wykonywanie kodu 3) weryfikuje integralność i autentyczność obrazów instalacyjnych oraz sterowników za pomocą sum kontrolnych i podpisów cyfrowych 4) konfiguruje ustawienia regionalne, językowe oraz czas systemowy 5) konfiguruje parametry sieciowe 6) wyłącza zbędne usługi bezpośrednio po instalacji

	7) aktualizuje system bezpośrednio po instalacji w celu wyeliminowania luk bezpieczeństwa
4) wdraża polityki tożsamości i kontroli dostępu zgodnie z modelem zerowego zaufania w systemach Linux i Windows	1) konfiguruje konta techniczne i serwisowe, minimalizując ich uprawnienia logowania interaktywnego 2) projektuje strukturę grup bezpieczeństwa w celu implementacji modelu RBAC (Role-Based Access Control) na poziomie lokalnym a) identyfikuje role użytkowników w systemie oraz przypisane do nich niezbędne zasoby b) tworzy i konfiguruje grupy zabezpieczeń odpowiadające zidentyfikowanym rolom funkcjonalnym c) konfiguruje konta i grupy lokalne użytkowników w systemach Windows i Linux w ramach struktury ról d) konfiguruje prawa i przywileje użytkowników poprzez ich przynależność do określonych grup e) analizuje hierarchię grup pod kątem optymalizacji dziedziczenia uprawnień w systemie f) definiuje standardy nazewnictwa grup ułatwiające identyfikację ról i audyt bezpieczeństwa g) weryfikuje poprawność implementacji modelu RBAC poprzez testowanie dostępów dla poszczególnych grup h) opracowuje dokumentację projektową opisującą mapowanie ról na konkretne grupy systemowe

	3) stosuje mechanizmy eskalacji uprawnień (np. sudo w Linux, elewacja w Windows) 4) wdraża polityki haseł do systemu operacyjnego wymuszające ich złożoność i okresową zmianę a) konfiguruje i zarządza zasadami haseł na poziomie lokalnym b) stosuje zasady zabezpieczeń lokalnych do ochrony poświadczeń użytkowników c) określa ramy czasowe ważności haseł dla poszczególnych grup użytkowników d) sprawdza poprawność działania mechanizmów wymuszających zmianę hasła przy pierwszym logowaniu 5) konfiguruje mechanizmy kontroli konta użytkownika w systemach Linux i Windows 6) konfiguruje bezpieczeństwo profili użytkowników, w tym mechanizmami ochrony poświadczeń w pamięci (np. Windows Defender Credential Guard, Linux PAM i systemy izolacji) a) konfiguruje różne profile użytkowników w lokalnych systemach operacyjnych Windows i Linux b) stosuje zasady zabezpieczeń lokalnych oraz konfiguruje prawa i przywileje użytkowników w celu ochrony danych profilu c) konfiguruje konta i grupy lokalne użytkowników w systemach Windows i Linux pod kątem bezpiecznego dostępu do poświadczeń

	d) konfiguruje i zarządza zasadami haseł oraz mechanizmami uwierzytelniania wieloskładnikowego w systemie Linux (moduły PAM) e) aktywuje i weryfikuje działanie funkcji Windows Defender Credential Guard, wykorzystującej wirtualizację do izolacji poświadczeń Local Security Authority (LSA) f) wdraża systemy obowiązkowej kontroli dostępu (MAC), takie jak AppArmor lub SELinux, w celu izolacji procesów użytkownika g) programuje przechowywanie danych i preferencji użytkownika w sposób bezpieczny, wykorzystując systemowe magazyny kluczy h) konfiguruje dzienniki i rejestry zdarzeń w celu monitorowania i audytu prób dostępu do danych uwierzytelniających 7) stosuje zasadę minimalnych uprawnień podczas nadawania dostępu do zasobów
5) zarządza systemami plików i zabezpiecza dostęp do danych	1) nadaje i modyfikuje uprawnienia do plików i folderów 2) wykorzystuje listy kontroli dostępu do precyzyjnego zarządzania uprawnieniami 3) konfiguruje udziały sieciowe i określa zasady dostępu dla użytkowników 4) stosuje szyfrowanie plików i całych wolumenów 5) monitoruje wykorzystanie przestrzeni dyskowej przez użytkowników

	6) konfiguruje punkty montowania w systemie Linux 7) weryfikuje integralność systemu plików po awariach
6) wykorzystuje narzędzia sztucznej inteligencji do zarządzania systemem	1) generuje skrypty PowerShell i Bash przy użyciu narzędzi sztucznej inteligencji 2) wykorzystuje narzędzia sztucznej inteligencji do analizy i optymalizacji istniejącego kodu skryptów 3) interpretuje za pomocą sztucznej inteligencji skomplikowane komunikaty błędów systemowych 4) weryfikuje poprawność i bezpieczeństwo kodu skryptu wygenerowanego przez sztuczną inteligencję 5) automatyzuje tworzenie dokumentacji skryptów przy użyciu modeli językowych 6) wyszukuje za pomocą narzędzi sztucznej inteligencji optymalne parametry konfiguracji usług 7) identyfikuje potencjalne podatności w skryptach przy wsparciu sztucznej inteligencji
7) administruje usługami i harmonogramem zadań	1) zarządza stanem usług (uruchamianie, zatrzymywanie, restartowanie) a) lokalizuje i uruchamia przystawkę „Usługi” (services.msc) jako podstawowe narzędzie administracyjne do zarządzania systemem operacyjnym Windows b) odnajduje funkcje sterowania usługami (np. w systemie operacyjnym Linux za

	pomocą narzędzi tekstowych) oraz graficznych (np. ustawienia systemu) c) identyfikuje polecenia systemów operacyjnych z poziomu konsoli służące do sprawdzania statusu demonów w Linux (systemctl) d) monitoruje pracę usług, odnajdując w systemie informacje o tym, czy dany proces jest uruchomiony, zatrzymany czy w stanie błędu e) korzysta z pomocy w konsoli systemów operacyjnych (np. man, help) aby odnaleźć przełączniki poleceń odpowiedzialne za wymuszony restart usług f) diagnozuje błędy startu usług, lokalizując w systemie narzędzia do podglądu logów, które wskazują przyczynę niepowodzenia operacji 2) konfiguruje tryb uruchamiania usług systemowych (automatyczny, ręczny, wyłączony) 3) planuje cykliczne zadania przy użyciu Harmonogramu Zadań (Windows) i cron (Linux) 4) analizuje zależności między usługami systemowymi oraz identyfikuje powiązania i błędy kaskadowe a) lokalizuje zakładkę „Zależności” we właściwościach usługi, wykorzystując narzędzia administracyjne do zarządzania systemem operacyjnym Windows

	b) identyfikuje polecenia systemów operacyjnych z poziomu konsoli (np. systemctl list-dependencies) w celu wygenerowania drzewa powiązań w systemie Linux c) rozróżnia usługi nadrzędne (od których dana usługa zależy) oraz usługi podrzędne (które zależą od niej) w strukturze systemu operacyjnego d) analizuje logi generowane przez poszczególne usługi, wskazując, która usługa w łańcuchu powiązań spowodowała zatrzymanie pozostałych elementów e) korzysta z pomocy w konsoli systemów operacyjnych, aby odnaleźć parametry poleceń wyświetlające tylko krytyczne (twarde) zależności procesów f) weryfikuje wpływ wyłączenia zbędnych usług na stabilność pozostałych komponentów systemu, minimalizując ryzyko wystąpienia błędów kaskadowych g) tworzy dokumentację w formie schematu lub listy, opisującą kluczowe zależności dla krytycznych usług serwerowych (np. DNS czy DHCP) 5) monitoruje logi generowane przez poszczególne usługi
8) utwardza konfigurację systemu Windows	1) konfiguruje zasady grup lokalnych (GPO) w celu wzmocnienia bezpieczeństwa 2) konfiguruje ustawienia usługi AppLocker i zasadami ograniczeń oprogramowania

	3) optymalizuje autostart systemu 4) konfiguruje zabezpieczenia sprzętowe 5) wdraża mechanizmy ochrony przed exploitami i atakami na pamięć 6) weryfikuje źródła pochodzenia instalowanego oprogramowania 7) wykonuje przegląd konfiguracji bezpieczeństwa narzędziami typu secpol 8) konfiguruje ustawienia systemu operacyjnego w zakresie prywatności: a) telemetrii w Windows i Linux, usług lokalizacji i śledzenia położenia urządzenia w Windows b) uprawnień aplikacji do korzystania z kamery oraz mikrofonu w Windows c) dostępu do kontaktów i kalendarza w Windows d) historii połączeń i czytania wiadomości e-mail w Windows, identyfikatora reklamowego w Windows e) rozpoznawania mowy online w Windows f) personalizacji pisma odręcznego w Windows g) zbierania danych diagnostycznych i próbek oprogramowania w Windows, h) historii aktywności użytkownika na osi czasu w Windows i) uprawnień aplikacji w tle w Windows j) synchronizacji ustawień z chmurą w Windows k) telemetrii przeglądarki i filtrów SmartScreen w Windows

	l) funkcji „Znajdź moje urządzenie” w Windows m) zbierania logów systemowych przez usługę journald w Linux n) przechowywania historii poleceń w pliku .bash_history w Linux o) zbierania metadanych przez menedżery pakietów w Linux p) przesyłania statystyk użytkowania w dystrybucjach Linux q) czyszczenia plików tymczasowych i śladów aktywności w systemach Windows i Linux
9) utwardza konfigurację systemu Linux	1) ogranicza dostęp do konta root 2) konfiguruje narzędzie sudo 3) zabezpiecza bootloader hasłem i blokuje nieautoryzowany dostęp fizyczny 4) konfiguruje mechanizmy kontroli dostępu 5) usuwa zbędne pakiety oprogramowania i usługi sieciowe 6) wdraża bezpieczną konfigurację stosu TCP/IP 7) weryfikuje uprawnienia plików systemowych pod kątem bitów SUID i SGID
10) zarządza zaporą sieciową i bezpieczeństwem sieciowym hosta	1) konfiguruje reguły przychodzące i wychodzące w Zaporze Windows 2) konfiguruje reguły przychodzące i wychodzące za pomocą iptables lub nftables w systemach Linux 3) blokuje nieużywane porty komunikacyjne na poziomie systemu operacyjnego 4) weryfikuje skuteczność reguł zapory poprzez testy łączności

	5) monitoruje aktywne połączenia sieciowe narzędziami netstat i ss 6) konfiguruje strefy sieciowe w celu odizolowania ruchu 7) wdraża ochronę przed atakami typu Denial of Service na poziomie hosta 8) dokumentuje wprowadzone zmiany w konfiguracji sieciowej
11) obsługuje systemy logowania i audytu zdarzeń	1) wykorzystuje narzędzie „Podgląd Zdarzeń” do analizy błędów i ostrzeżeń systemowych 2) analizuje pliki logów w systemie Linux 3) konfiguruje „Audyt zdarzeń logowania” w przystawce „Zasady zabezpieczeń lokalnych” (secpol.msc) w Windows oraz system audytu auditd w Linux w celu rejestrowania prób logowania i dostępu do plików 4) wdraża rotację logów w celu optymalizacji przestrzeni dyskowej 5) identyfikuje w logach wzorce wskazujące na próby nieautoryzowanego dostępu 6) konfiguruje zdalne przesyłanie logów do serwera logowania 7) tworzy raporty na podstawie zebranych danych z audytu
12) zapewnia ochronę systemu operacyjnego przed szkodliwym oprogramowaniem	1) konfiguruje i monitoruje pracę systemu antywirusowego 2) przeprowadza regularne skanowanie systemu pod kątem obecności złośliwego oprogramowania 3) interpretuje wyniki skanowania i podejmuje działania naprawcze

	4) analizuje przykłady działania złośliwego oprogramowania 5) symuluje przeprowadzenie ataku typu „reverse shell” i wykrywa atak w środowisku testowym 6) wdraża białe listy aplikacji (allowlist) przy użyciu narzędzia AppLocker lub zasad ograniczeń oprogramowania w Windows oraz modułów AppArmor lub SELinux w Linux w celu blokowania nieznanego kodu 7) monitoruje integralność krytycznych plików systemowych 8) edukuje użytkowników w zakresie higieny cyfrowej i zagrożeń
13) sprawdza i zabezpiecza niskopoziomową konfigurację systemu	1) modyfikuje ustawienia systemowe w celu wyłączenia podatnych protokołów 2) wykonuje kopie zapasowe i przywraca fragmenty rejestru 3) zabezpiecza pliki konfiguracyjne w systemie Linux, stosując atrybuty niezmienności (chattr) oraz restrykcyjne maski uprawnień 4) identyfikuje i usuwa niebezpieczne wpisy w sekcjach autostartu 5) monitoruje zmiany w rejestrze pod kątem działań złośliwego oprogramowania 6) stosuje skrypty do masowej modyfikacji ustawień systemowych 7) weryfikuje wpływ zmian w konfiguracji na stabilność systemu
14) wykorzystuje wirtualizację i konteneryzację w pracy z systemami	1) tworzy i konfiguruje maszyny wirtualne dla różnych systemów operacyjnych

	2) zarządza (tworzy, przywraca, usuwa, konsoliduje oraz monitoruje) migawki i punkty przywracania maszyn wirtualnych 3) instaluje system operacyjny w środowisku zwirtualizowanym 4) konfiguruje wirtualne interfejsy sieciowe i izolowane sieci (np. NAT, Host-only) 5) instaluje i obsługuje środowisko Docker do uruchamiania kontenerów 6) zarządza (buduje, wdraża, wersjonuje, monitoruje oraz usuwa) obrazy i steruje pełnym cyklem życia kontenerów 7) optymalizuje wykorzystanie zasobów sprzętowych przez systemy wirtualne 8) wdraża zasady bezpieczeństwa dla środowisk kontenerowych 9) migruje systemy między różnymi platformami wirtualizacyjnymi: a) analizuje i planuje strategię przenoszenia zasobów b) przeprowadza konwersję formatów dysków i sterowników c) rekonfiguruje parametry sieciowe i sprzętowe d) testuje i weryfikuje poprawność działania usług
15) wdraża w sposób bezpieczny środowiska wirtualne oparte na systemie operacyjnym Linux oraz kontenerowe w środowisku chmurowym	1) wyjaśnia pojęcie chmury obliczeniowej 2) rozróżnia modele serwisowe (IaaS, PaaS, SaaS) oraz modele wdrożeniowe (publiczna, prywatna, hybrydowa) 3) wyjaśnia model współdzielonej odpowiedzialności w chmurze

	4) uruchamia i konfiguruje instancje wirtualne Linux w chmurze, korzystając z utwardzonych obrazów systemowych 5) wdraża bezpieczny dostęp do instancji Linux przy użyciu par kluczy SSH, wyłączając uwierzytelnianie hasłem oraz blokując dostęp dla konta root 6) konfiguruje chmurowe zapory sieciowe (np. Security Groups, Network ACLs) zgodnie z zasadą „Default Deny” dla usług działających na systemie Linux 7) przypisuje instancjom wirtualnym oraz usługom kontenerowym role tożsamości, unikając stosowania statycznych poświadczeń wewnątrz systemów 8) wdraża środowiska kontenerowe w chmurze (np. usługi typu Container Instances lub zarządzane klastry Kubernetes), dbając o izolację sieciową zasobów 9) korzysta z prywatnych rejestrów obrazów kontenerowych w chmurze i konfiguruje automatyczne skanowanie obrazów pod kątem podatności 10) konfiguruje chmurowe mechanizmy zarządzania sekretami 11) konfiguruje przestrzeń do przechowywania danych w chmurze z wymuszeniem szyfrowania danych w spoczynku (at-rest)
INF.11.7. Testowanie bezpieczeństwa sieci TCP/IP	

Efekty kształcenia	Kryteria weryfikacji
Uczeń:	Uczeń:
1) rozpoznaje zagrożenia bezpieczeństwa występujące w sieciach TCP/IP	1) wymienia podstawowe zagrożenia sieciowe, w tym: a) podsłuch ruchu sieciowego b) spoofing adresów IP/MAC c) ataki DoS d) skanowanie portów e) nieautoryzowany dostęp do usług sieciowych 2) identyfikuje zagrożenia związane z sieciami bezprzewodowymi 3) wyjaśnia wpływ zagrożeń sieciowych na poufność, integralność i dostępność danych na przykładzie: a) podsłuchu ruchu sieciowego b) modyfikacji ruchu sieciowego c) ataków typu DoS
2) weryfikuje konfigurację sieci pod kątem bezpieczeństwa	1) wykorzystuje narzędzia do identyfikacji ekspozycji i podatności sieciowej (nmap, skaner podatności): a) skanuje sieci w celu wykrycia aktywnych hostów i otwartych portów z wykorzystaniem narzędzi typu nmap b) identyfikuje dostępne usługi sieciowe i ich ekspozycję c) wykonuje automatyczne skanowanie podatności z wykorzystaniem skanera podatności 2) sprawdza konfigurację VLAN, ACL i NAT pod kątem bezpieczeństwa: a) właściwej segmentacji

	b) konfiguracji portów c) blokowania sfałszowanych adresów przez ACL 3) identyfikuje niebezpieczne konfiguracje sieciowe na podstawie (np. zaleceń producentów, obowiązujących standardów oraz wewnętrznych polityk bezpieczeństwa) 4) ocenia skuteczność zastosowanych zabezpieczeń sieciowych: a) weryfikuje czy zapora sieciowa blokuje ruch zgodnie z politykami b) sprawdza, czy dostęp do usług jest możliwy tylko z dozwolonych adresów IP lub sieci c) porównuje stan faktyczny z obowiązującymi w organizacji politykami bezpieczeństwa 4) wskazuje elementy konfiguracji wymagające poprawy
3) monitoruje i dokumentuje operacyjne działanie infrastruktury sieciowej	1) monitoruje operacyjny ruch sieciowy i stan urządzeń sieciowych 2) konfiguruje rejestrowanie zdarzeń sieciowych 3) przesyła logi urządzeń sieciowych do serwera syslog 4) dokumentuje zmiany i zdarzenia zachodzące w sieci
4) rozpoznaje i analizuje próby naruszenia bezpieczeństwa sieci TCP/IP	1) wyjaśnia znaczenie logów systemowych i sieciowych w procesie wykrywania i analizy prób naruszenia bezpieczeństwa 2) analizuje zdarzenia bezpieczeństwa z wykorzystaniem narzędzi monitorowania i detekcji (IDS/IPS, Security Information and

	Event Management (SIEM)), w tym interpretuje alerty oraz skorelowane logi pod kątem: a) masowych prób połączeń do wielu portów lub hostów, b) automatycznych prób nawiązywania sesji, c) nieuprawnionego skanowania zasobów sieciowych, d) prób wykorzystania błędnej konfiguracji, e) komunikatów o błędnym logowaniu 3) rozpoznaje próby nieautoryzowanego dostępu na podstawie podstawowych informacji o zdarzeniach sieciowych: a) czas zdarzenia b) źródło i cel komunikacji c) adresy IP i numery portów d) próby logowania e) status zdarzenia (dozwolone/zablokowane) 4) rozpoznaje nietypowe wzorce ruchu i zdarzeń sieciowych mogące świadczyć o naruszeniu bezpieczeństwa, w tym: a) nagłego wzrostu liczby połączeń lub pakietów, b) ruchu generowanego poza standardowymi godzinami pracy, c) komunikacji z nieznanymi lub podejrzanymi adresami IP i domenami
5) analizuje incydenty sieciowe oraz opracowuje dokumentację analityczną cyberbezpieczeństwa	1) dokumentuje wykryte incydenty bezpieczeństwa 2) przygotowuje informacje do eskalacji incydentu zgodnie z procedurami

	3) ocenia poziom ryzyka wykrytych podatności w uproszczonej skali (niskie, średnie, wysokie, krytyczne) 4) klasyfikuje podatności na potrzeby obsługi incydentu: a) ze względu na rodzaj podatności (błędy konfiguracji, podatności oprogramowania, podatności sieciowe) b) ze względu na skutki dla atrybutów informacji (naruszenie poufności, integralności, dostępności) c) ze względu na priorytet obsługi (natychmiastowa reakcja, zaplanowana poprawka, do obserwacji) 5) opracowuje podstawowe raporty z testów bezpieczeństwa zawierające opisy zagrożeń i rekomendacje

INF.11.8. Język angielski zawodowy	
Efekty kształcenia	Kryteria weryfikacji
Uczeń:	Uczeń:
1) posługuje się podstawowym zasobem środków językowych w języku angielskim (ze szczególnym uwzględnieniem środków leksykalnych), umożliwiającym realizację czynności zawodowych w zakresie tematów związanych: a) ze stanowiskiem pracy i jego wyposażeniem b) z głównymi technologiami stosowanymi w danym zawodzie	1) rozpoznaje oraz stosuje środki językowe umożliwiające realizację czynności zawodowych w zakresie: a) czynności wykonywanych na stanowisku pracy, w tym związanych z zapewnieniem bezpieczeństwa i higieny pracy b) narzędzi, maszyn, urządzeń i materiałów koniecznych do realizacji czynności zawodowych c) procesów i procedur związanych z realizacją zadań zawodowych

c) z dokumentacją związaną z danym zawodem d) z usługami świadczonymi w danym zawodzie	d) formularzy, specyfikacji oraz innych dokumentów związanych z wykonywaniem zadań zawodowych e) świadczonych usług, w tym obsługi klienta
2) rozumie proste wypowiedzi ustne artykułowane wyraźnie, w standardowej odmianie języka angielskiego, a także proste wypowiedzi pisemne w języku angielskim, w zakresie umożliwiającym realizację zadań zawodowych: a) rozumie proste wypowiedzi ustne dotyczące czynności zawodowych (np. rozmowy, wiadomości, komunikaty, instrukcje lub filmy instruktażowe, prezentacje), artykułowane wyraźnie, w standardowej odmianie języka b) rozumie proste wypowiedzi pisemne dotyczące czynności zawodowych (np. napisy, broszury, instrukcje obsługi, przewodniki, dokumentację zawodową)	1) określa główną myśl wypowiedzi lub tekstu, ewentualnie fragmentu wypowiedzi lub tekstu 2) znajduje w wypowiedzi lub tekście określone informacje 3) rozpoznaje związki między poszczególnymi częściami tekstu 4) układa informacje w określonym porządku
3) samodzielnie tworzy krótkie, proste, spójne i logiczne wypowiedzi ustne i pisemne w języku angielskim, w zakresie umożliwiającym realizację zadań zawodowych:	1) opisuje przedmioty, działania i zjawiska związane z czynnościami zawodowymi 2) przedstawia sposób postępowania w różnych sytuacjach zawodowych (np. udziela instrukcji, wskazówek, określa zasady) 3) wyraża i uzasadnia swoje stanowisko

a) tworzy krótkie, proste, spójne i logiczne wypowiedzi ustne dotyczące czynności zawodowych (np. polecenie, komunikat, instrukcję) b) tworzy krótkie, proste, spójne i logiczne wypowiedzi pisemne dotyczące czynności zawodowych (np. komunikat, e-mail, instrukcję, wiadomość, CV, list motywacyjny, dokument związany z wykonywanym zawodem – według wzoru)	4) stosuje zasady konstruowania tekstów o różnym charakterze 5) stosuje formalny lub nieformalny styl wypowiedzi adekwatnie do sytuacji
4) uczestniczy w rozmowie w typowych sytuacjach związanych z realizacją zadań zawodowych – reaguje w języku angielskim w sposób zrozumiały, adekwatnie do sytuacji komunikacyjnej, ustnie lub w formie prostego tekstu: a) reaguje ustnie (np. podczas rozmowy z innym pracownikiem, klientem, kontrahentem, w tym rozmowy telefonicznej) w typowych sytuacjach związanych z wykonywaniem czynności zawodowych b) reaguje w formie prostego tekstu pisanego (np. wiadomość, formularz, e-mail, dokument związany z wykonywanym	1) rozpoczyna, prowadzi i kończy rozmowę 2) uzyskuje i przekazuje informacje i wyjaśnienia 3) wyraża swoje opinie i uzasadnia je, pyta o opinie, zgadza się lub nie zgadza z opiniami innych osób 4) prowadzi proste negocjacje związane z czynnościami zawodowymi 5) stosuje zwroty i formy grzecznościowe 6) dostosowuje styl wypowiedzi do sytuacji

zawodem) w typowych sytuacjach związanych z wykonywaniem czynności zawodowych	
5) zmienia formę przekazu ustnego lub pisemnego w języku angielskim w typowych sytuacjach związanych z wykonywaniem czynności zawodowych	1) przekazuje w języku angielskim informacje zawarte w materiałach wizualnych (np. wykresach, symbolach, piktogramach, schematach) oraz audiowizualnych (np. filmach instruktażowych) 2) przekazuje w języku polskim informacje sformułowane w języku angielskim 3) przekazuje w języku angielskim informacje sformułowane w języku polskim lub tym języku 4) przedstawia publicznie w języku angielskim wcześniej opracowany materiał (np. prezentację)
6) wykorzystuje strategie służące doskonaleniu własnych umiejętności językowych oraz podnoszące świadomość językową: a) wykorzystuje techniki samodzielnej pracy nad nauką języka b) współdziała w grupie c) korzysta ze źródeł informacji w języku angielskim d) stosuje strategie komunikacyjne i kompensacyjne	1) korzysta ze słownika dwujęzycznego i jednojęzycznego 2) współdziała z innymi osobami, realizując zadania językowe 3) korzysta z tekstów w języku angielskim, również za pomocą technologii informacyjno-komunikacyjnych 4) identyfikuje słowa klucze, internacjonalizmy 5) wykorzystuje kontekst (tam, gdzie to możliwe), aby w przybliżeniu określić znaczenie słowa 6) upraszcza (jeżeli to konieczne) wypowiedź, zastępuje nieznane słowa innymi, wykorzystuje opis, środki niewerbalne
INF.11.9. Kompetencje personalne i społeczne	

Efekty kształcenia	Kryteria weryfikacji
Uczeń:	Uczeń:
1) przestrzega zasad kultury i etyki zawodowej	1) wykazuje się etyczną postawą i przestrzega zasad prawa w obszarze bezpieczeństwa informacji 2) zachowuje pełną poufność informacji uzyskanych w toku wykonywania zadań zawodowych 3) wykazuje się rzetelnością i odpowiedzialnością za powierzone dane oraz systemy IT 4) identyfikuje dylematy etyczne związane z dostępem do systemów i danych użytkowników 5) stosuje zasady netykiety i profesjonalnej komunikacji w środowisku cyfrowym 6) promuje zasady higieny cyfrowej wewnątrz organizacji 7) respektuje własność intelektualną oraz licencje oprogramowania używanego w pracy 8) korzysta z platform edukacyjnych typu Capture The Flag (CTF) i projektów demonstracyjnych (np. WebGoat)
2) współpracuje w zespole oraz z innymi pracownikami organizacji	1) pracuje w zespole nad złożonymi zadaniami z zakresu IT 2) komunikuje się w sposób jasny i rzeczowy z administratorami oraz programistami 3) współpracuje z użytkownikami końcowymi w celu rozwiązywania problemów technicznych

	4) wykazuje otwartość na opinie innych i konstruktywnie przyjmuje informacje zwrotne 5) rozwiązuje konflikty w zespole IT w sposób profesjonalny i merytoryczny 6) dzieli się wiedzą techniczną i doświadczeniem z innymi członkami zespołu 7) uczestniczy w planowaniu wspólnych działań prewencyjnych i procedur bezpieczeństwa 8) przyjmuje i rzetelnie realizuje zadania delegowane w ramach małych zespołów
3) planuje i organizuje pracę własną, szczególnie w sytuacjach stresowych	1) planuje i organizuje pracę własną na stanowisku technicznym 2) określa priorytety zadań zgodnie z ich krytycznością dla bezpieczeństwa systemów 3) wykazuje się dokładnością i skrupulatnością w wykonywaniu powierzonych czynności 4) zachowuje odporność na stres i opanowanie w sytuacjach awaryjnych 5) potrafi efektywnie pracować pod presją czasu podczas obsługi incydentów 6) dokumentuje podejmowane działania i incydenty w sposób systematyczny i przejrzysty 7) dba o ład i porządek na stanowisku pracy oraz o powierzony sprzęt i narzędzia
4) wykazuje gotowość do ciągłego uczenia się i rozwoju zawodowego	1) wykazuje aktywną postawę w śledzeniu nowych trendów w informatyce i cyberbezpieczeństwie 2) samodzielnie wyszukuje informacje o nowych zagrożeniach i metodach ataków

	3) wykazuje gotowość do ciągłego uczenia się i aktualizowania wiedzy specjalistycznej 4) wykazuje się dociekliwością i spostrzegawczością w identyfikowaniu anomalii systemowych 5) samodzielnie rozwiązuje nowe problemy techniczne z wykorzystaniem dostępnej dokumentacji 6) analizuje własne błędy i wyciąga wnioski w celu doskonalenia procedur bezpieczeństwa 7) planuje ścieżkę dalszego kształcenia i zdobywania certyfikacji branżowych
INF.11.10. Organizacja pracy małych zespołów	
Efekty kształcenia	Kryteria weryfikacji
Uczeń:	Uczeń:
1) planuje realizację zadań zespołu technicznego	1) określa cele i zakres zadań zawodowych dla małego zespołu 2) rozdziela zadania między członków zespołu, uwzględniając ich kompetencje i predyspozycje 3) opracowuje harmonogram prac z uwzględnieniem priorytetów, terminów realizacji i planów awaryjnych 4) identyfikuje zasoby techniczne i narzędzia niezbędne do wykonania zadania 5) uwzględnia procedury i zasady bezpieczeństwa podczas planowania działań 6) ocenia ryzyko związane z realizacją zadań i proponuje działania minimalizujące zagrożenia

	7) planuje pracę pod presją czasu, szczególnie w sytuacjach awaryjnych lub przy obsłudze incydentów
2) koordynuje komunikację i współpracę wewnątrz zespołu oraz z otoczeniem	1) komunikuje się z członkami zespołu w sposób jasny, rzeczowy i profesjonalny 2) wykorzystuje narzędzia do pracy grupowej i systemy kontroli wersji 3) koordynuje współpracę między administratorami, programistami i użytkownikami 4) prowadzi spotkania techniczne dotyczące postępów prac i rozwiązywania problemów 5) stosuje zasady netykiety oraz profesjonalnej komunikacji w środowisku cyfrowym 6) rozstrzyga konflikty techniczne i organizacyjne wewnątrz zespołu 7) przekazuje informacje o zagrożeniach i incydentach właściwym organom lub zespołom nadrzędnym 8) dba o przepływ wiedzy i promowanie zasad higieny cyfrowej w zespole
3) monitoruje postępy prac i dokumentuje działania zespołu	1) kontroluje terminowość i jakość zadań wykonywanych przez członków zespołu 2) weryfikuje poprawność dokumentacji technicznej tworzonej w toku prac 3) analizuje logi i raporty z postępów prac w celu wykrywania nieprawidłowości 4) sporządza zbiorcze raporty z działań zespołu oraz dokumentuje zaistniałe incydenty 5) wykorzystuje narzędzia sztucznej inteligencji do wspomagania procesu raportowania i analizy wyników pracy zespołu (np. notatka

	z podsumowaniem i listą zadań do wykonania) 6) ocenia skuteczność wdrożonych zabezpieczeń i procedur na podstawie wyników zespołu 7) dba o systematyczność i dokładność w gromadzeniu dowodów działań naprawczych
4) zarządza odpowiedzialnością i etyką pracy w zespole IT	1) egzekwuje od członków zespołu zachowanie poufności informacji i danych 2) promuje postawy etyczne i przestrzeganie zasad prawa w obszarze cyberbezpieczeństwa 3) wykazuje się odpowiedzialnością za powierzone zespołowi dane i systemy informatyczne 4) motywuje członków zespołu do ciągłego aktualizowania wiedzy i rozwoju zawodowego 5) monitoruje przestrzeganie zasad bezpieczeństwa i higieny pracy na stanowiskach komputerowych 6) nadzoruje prawidłowość stosowania mechanizmów kontroli dostępu przez członków zespołu 7) ocenia wkład poszczególnych osób w realizację celów bezpieczeństwa organizacji

Do wykonywania zadań zawodowych w zakresie kwalifikacji INF.12. Programowanie bezpiecznych aplikacji webowych jest niezbędne osiągnięcie niżej wymienionych efektów kształcenia

INF.12. Programowanie bezpiecznych aplikacji webowych
INF.12.1. Bezpieczeństwo i higiena pracy

Efekty kształcenia	Kryteria weryfikacji
Uczeń:	Uczeń:
1) określa skutki oddziaływania czynników szkodliwych na organizm człowieka	1) określa zagrożenia występujące w środowisku pracy 2) określa skutki oddziaływania czynników psychofizycznych na organizm człowieka 3) opisuje skutki oddziaływania czynników niebezpiecznych i uciążliwych na organizm człowieka 4) wyjaśnia pojęcia choroba zawodowa i wypadek przy pracy
2) przestrzega zasad bezpieczeństwa i higieny pracy oraz przepisów prawa dotyczących ochrony przeciwpożarowej i ochrony środowiska występujących w zawodzie	1) stosuje zasady zachowania się w przypadku pożaru 2) rozróżnia środki gaśnicze ze względu na zakres ich stosowania 3) obsługuje komputery i urządzenia na stanowiskach pracy zgodnie z zasadami i przepisami bezpieczeństwa i higieny pracy, ochrony przeciwpożarowej i ochrony środowiska 4) stosuje zasady postępowania z odpadami niebezpiecznymi
3) organizuje stanowisko pracy zgodnie z wymaganiami ergonomii oraz przepisami dotyczącymi bezpieczeństwa i higieny pracy, ochrony przeciwpożarowej i ochrony środowiska	1) identyfikuje czynniki, które należy brać pod uwagę przy organizacji stanowiska pracy zgodnie z zasadami ergonomii 2) stosuje wymagania ergonomiczne dla stanowiska pracy 3) wskazuje obowiązki pracodawcy w zakresie organizacji czasu pracy pracownika 4) identyfikuje działania prewencyjne zapobiegające powstawaniu zagrożeń na stanowisku pracy

	5) rozpoznaje sytuacje grożące pożarem na stanowisku pracy 6) stosuje sprzęt i materiały ekologiczne na stanowisku pracy
4) stosuje środki ochrony indywidualnej i zbiorowej podczas wykonywania zadań zawodowych	1) identyfikuje środki ochrony zbiorowej 2) wskazuje środki ochrony zabezpieczające przed hałasem w pracy biurowej 3) identyfikuje wymagania w zakresie oświetlenia, temperatury i mikroklimatu pomieszczeń biurowych 4) stosuje środki ochrony zapobiegające porażeniem prądem w pracy biurowej 5) stosuje środki ochrony zapobiegające pogorszeniu wzroku i zniekształceniu kręgosłupa 6) dobiera środki ochrony zbiorowej do rodzaju zagrożeń w pracy biurowej
5) udziela pierwszej pomocy w sytuacji nagłego zagrożenia zdrowotnego	1) opisuje podstawowe symptomy wskazujące na stany nagłego zagrożenia zdrowotnego 2) ocenia sytuację poszkodowanego na podstawie analizy objawów obserwowanych u poszkodowanego 3) zabezpiecza siebie, poszkodowanego i miejsce wypadku 4) układa poszkodowanego w pozycji bezpiecznej 5) powiadamia odpowiednie służby 6) prezentuje udzielanie pierwszej pomocy w urazowych stanach nagłego zagrożenia zdrowotnego (np. krwotok, zmiażdżenie, amputacja, złamanie, oparzenie)

	7) prezentuje udzielanie pierwszej pomocy w nieurazowych stanach nagłego zagrożenia zdrowotnego (np. omdlenie, zawał, udar) 8) wykonuje resuscytację krążeniowo-oddechową na fantomie zgodnie z wytycznymi Polskiej Rady Resuscytacji i Europejskiej Rady Resuscytacji
INF.12.2. Podstawy cyberbezpieczeństwa systemów IT	
Efekty kształcenia	Kryteria weryfikacji
Uczeń:	Uczeń:
1) stosuje podstawową terminologię związaną z cyberbezpieczeństwem	1) wyjaśnia pojęcie cyberbezpieczeństwa 2) wyjaśnia pojęcie cyberataku 3) wyjaśnia pojęcie triady CIA (Confidentiality –Poufność, Integrity – Integralność, Availability – Dostępność) 4) opisuje znaczenie triady CIA dla bezpieczeństwa informacji 5) określa znaczenie posiadanych uprawnień i zgody właściciela systemu dla legalności działań w sieciach komputerowych (etyczny hacking vs. przestępstwo)
2) charakteryzuje zagrożenia cyberbezpieczeństwa	1) rozróżnia zagrożenia wewnętrzne i zewnętrzne w systemach IT 2) wskazuje zależności między zagrożeniami a podatnościami 3) opisuje rodzaje ataków: a) włamania sieciowe b) ataki za pomocą malware c) ataki typu DoS/DDoS d) ataki fizyczne e) ataki socjotechniczne

	3) opisuje działanie różnych typów złośliwego oprogramowania (np. wirus, spyware, ransomware, trojan, backdoor) 4) wskazuje cele i potencjalne skutki ataków: a) nieuprawnione pozyskanie informacji b) nieuprawniona modyfikacja danych c) kradzież tożsamości d) zakłócenie działania systemu e) wymuszenie okupu 5) opisuje proste scenariusze ataków: a) ataki phishingowe z wykorzystaniem poczty elektronicznej b) podrzucenie zainfekowanego nośnika USB c) próby automatycznego łamania haseł d) podsłuch
3) charakteryzuje i analizuje ataki socjotechniczne	1) wyjaśnia mechanizm działania ataków socjotechnicznych 2) rozróżnia ataki socjotechniczne typu phishing i spear phishing 3) podaje przykłady realizacji ataku socjotechnicznego z wykorzystaniem: a) poczty elektronicznej b) nośnika USB c) rozmowy telefonicznej d) wiadomości tekstowej e) fałszywego pracownika 4) omawia mechanizmy obrony przed atakami socjotechnicznymi, również przeprowadzonymi z wykorzystaniem narzędzi sztucznej inteligencji: a) weryfikacja nadawcy b) weryfikacja linku w wiadomości

	c) weryfikacja rozmówcy d) weryfikacja tożsamości 5) stosowanie niezależnych kanałów komunikacji wspomaganie oceny wiarygodności przekazu z wykorzystaniem narzędzi sztucznej inteligencji
4) charakteryzuje mechanizmy kontroli tożsamości	1) wyjaśnia pojęcie identyfikacji użytkownika 2) wyjaśnia pojęcie uwierzytelniania użytkownika i podaje przykłady metod uwierzytelniania (np. hasło, biometria, kod autoryzacyjny) 3) wyjaśnia pojęcie wzajemnego (dwustronnego) uwierzytelniania 4) wyjaśnia znaczenie procesu uwierzytelniania dla ochrony zasobów systemów
5) stosuje uwierzytelnianie wieloskładnikowe MFA (Multi-Factor Authentication)	1) wyjaśnia pojęcie uwierzytelniania wieloskładnikowego 2) wymienia składniki MFA („coś, co wie”, „coś, co ma”, „coś, czym jest”) 3) podaje przykłady metod MFA (np. OTP (One-Time Password), Google Authenticator TOTP (Time-Based OTP), token, biometria, techniki behawioralne) 4) wyjaśnia, dlaczego MFA zwiększa poziom bezpieczeństwa w porównaniu do uwierzytelniania jednoskładnikowego 5) podaje praktyczne przykłady zastosowania MFA
6) stosuje zasady kontroli dostępu	1) rozróżnia procesy uwierzytelniania, autoryzacji i kontroli dostępu 2) opisuje zasadę najmniejszych uprawnień 3) wyjaśnia ideę przydzielania użytkownikowi tylko niezbędnych uprawnień

	4) wskazuje zagrożenia wynikające z nadmiernych uprawnień 5) podaje przykłady zastosowania zasady najmniejszych uprawnień w systemach operacyjnych i aplikacjach 6) uzasadnia znaczenie zasady najmniejszych uprawnień w ograniczaniu skutków incydentów bezpieczeństwa 7) stosuje modele i mechanizmy kontroli dostępu (np. kontrola oparta na rolach (RBAC), kontrola oparta na atrybutach (ABAC), kontrola obowiązkowa (MAC), listy kontroli dostępu (ACL))
7) wyjaśnia podstawy kryptografii i jej zastosowanie w bezpieczeństwie IT	1) rozróżnia dane wymagające ochrony i dane jawne 2) wyjaśnia znaczenie kryptografii w bezpieczeństwie systemów i aplikacji 3) wyjaśnia sposób działania funkcji skrótu (hash) oraz jej przeznaczenie (weryfikacja integralności danych, podpisy cyfrowe) 4) wskazuje funkcje skrótu uznane za aktualny standard bezpieczeństwa 5) wyjaśnia przeznaczenie i sposób działania szyfrów symetrycznych 6) wskazuje szyfry symetryczne uznane za aktualny standard bezpieczeństwa 7) wyjaśnia sposób działania szyfrów asymetrycznych oraz pojęcia dotyczące klucza publicznego i prywatnego 8) wyjaśnia mechanizm oraz przeznaczenie podpisu cyfrowego

	9) omawia rolę kryptografii asymetrycznej w wymianie kluczy, uwierzytelnianiu i podpisach cyfrowych 10) wskazuje szyfry asymetryczne uznane za aktualny standard bezpieczeństwa 11) wyjaśnia potencjalny wpływ komputerów kwantowych na klasyczną kryptografię 12) wyjaśnia hybrydowe mechanizmy post-kwantowe (PQC)
8) wykonuje podstawowe operacje kryptograficzne w środowisku testowym	1) wyjaśnia pojęcia certyfikatu cyfrowego, urzędu certyfikacji, infrastruktury klucza publicznego (PKI), łańcucha certyfikacji 2) interpretuje informacje w certyfikacie (np. okres ważności, wystawcę, podmiot, algorytm, numer seryjny) 3) wyjaśnia rolę certyfikatów w zapewnieniu autentyczności i integralności 4) tworzy parę kluczy asymetrycznych (RSA lub ECC) 5) przechowuje klucze w bezpieczny sposób 6) generuje własne certyfikaty użytkownika lub serwera 7) generuje certyfikat własnego CA (Certificate Authority) 8) weryfikuje ważność certyfikatów 9) stosuje certyfikaty do generowania i weryfikacji podpisów cyfrowych 10) stosuje certyfikaty do zabezpieczenia sesji zdalnego dostępu w systemach Windows i Linux 11) szyfruje i deszyfruje dane przy użyciu dostępnych narzędzi

	12) oblicza skróty dla przykładowych danych i wskazuje efekty zmiany danych na wartość skrótu
9) charakteryzuje organizację i funkcjonowanie KSC (Krajowego Systemu Cyberbezpieczeństwa)	1) wyjaśnia cel funkcjonowania KSC oraz jego znaczenie dla bezpieczeństwa państwa i systemów informatycznych w Polsce 2) opisuje strukturę KSC, wskazując role poszczególnych podmiotów, w tym w szczególności Computer Security Incident Response Teamów (CSIRT-ów) oraz organów właściwych, a także operatorów usług kluczowych, dostawców usług cyfrowych oraz podmiotów publicznych 3) wyjaśnia pojęcie infrastruktury krytycznej i omawia znaczenie systemów teleinformatycznych dla jej funkcjonowania oraz wskazuje zależność między cyberbezpieczeństwem a zarządzaniem kryzysowym 4) wymienia podstawowe obowiązki operatorów usług kluczowych, 5) wyjaśnia pojęcie incydentu bezpieczeństwa, w tym incydentu krytycznego, oraz wyjaśnia rolę współpracy w procesie reagowania na zagrożenia 6) omawia odpowiedzialność prawną (karną i administracyjną) związaną z nieuprawnionym dostępem do informacji oraz niewypełnieniem obowiązków nałożonych przez ustawę o KSC

10) rozpoznaje właściwe normy i procedury oceny zgodności podczas realizacji zadań przewozowych	1) wymienia cele normalizacji krajowej 2) podaje definicje i cechy normy 3) rozróżnia oznaczenie normy krajowej i normy międzynarodowej, w tym norm europejskich 4) korzysta ze źródeł informacji dotyczących norm i procedur oceny zgodności
INF.12.3. Implementacja aplikacji webowych	
Efekty kształcenia	Kryteria weryfikacji
Uczeń:	Uczeń:
1) programuje obiektowo w języku Java (lub C#)	1) stosuje narzędzia programisty do pracy własnej i grupowej: IDE, GIT 2) wyjaśnia zasadę działania maszyny wirtualnej i automatycznego odzyskiwania pamięci (GC) oraz przyczyny błędów wycieku pamięci (trzymanie referencji do niepotrzebnych obiektów) 3) programuje obiektowo, stosując interfejsy i klasy, wykorzystując techniki dziedziczenia i kompozycji oraz mechanizmy enkapsulacji danych 4) stosuje podstawowe wzorce projektowe: fabryka, singleton, adapter, fasada, pełnomocnik (proxy) 5) stosuje szablony oraz wyrażenia lambda 6) wykorzystuje podstawowe techniki programowania współbieżnego: wątki oraz mechanizmy synchronizacji (dla C# również mechanizm async/await): a) uruchamiając i zatrzymując wątki w sposób kontrolowany b) wykorzystując pule wątków

	c) synchronizując wątki z wykorzystaniem semaforów lub barier d) komunikując się z wątkami za pomocą kolejek e) synchronizując dostęp do danych 7) wyjaśnia skutki błędów synchronizacji, w tym błąd wyścigu (race condition) 8) dokumentuje programy za pomocą komentarzy dołączonych do kodu źródłowego (javadoc/XML docs)
2) tworzy poprawne i bezpieczne programy w języku Java (C#)	1) stosuje podejście defensywne: a) zabezpiecza się przed błędami podczas wykonywania programu b) obsługuje błędy c) przechwytuje i obsługuje wyjątki (try/catch/finally) 2) zarządza zasobami systemu operacyjnego (pliki, gniazda, wątki) w sposób deterministyczny: a) zwalnia zasoby, gdy przestają być potrzebne b) wspomaga się instrukcją try-with-resources (using w C#) 3) zabezpiecza program przed wyciekami pamięci 4) stosuje zasady bezpiecznego programowania: a) używanie właściwych typów danych do przechowywania sekretów b) walidacja danych wejściowych c) walidacja ścieżek do systemu plików

	d) preferowanie stosowania klas niemodyfikowalnych (zwłaszcza w programach wielowątkowych) 5) wykonuje automatyczne testy oprogramowania 6) wykorzystuje narzędzia do weryfikacji programów pod kątem obecności błędów bezpieczeństwa 7) wykorzystuje narzędzia sztucznej inteligencji do: a) generacji kodu b) generacji testów na podstawie opisu lub dokumentacji javadoc/XML docs c) weryfikacji programów pod kątem poprawności i bezpieczeństwa
3) programuje aplikacje webowe	1) wyjaśnia i stosuje technologie klienta: HTML, CSS, JavaScript 2) programuje formularze z walidacją danych po stronie klienta 3) programuje skrypty JavaScript wykorzystujące DOM (jQuery), obsługę zdarzeń, interakcję z serwerem (Fetch API) 4) przetwarza (waliduje, serializuje i deserializuje) dane w formacie JSON i XML 5) wyjaśnia zasady działania protokołów HTTP i HTTPS: zapytania, nagłówki, kody odpowiedzi 6) implementuje usługi typu CRUD/REST z prostym interfejsem webowym, wykorzystujące ruting, kontrolery, walidację danych wejściowych, sesje, ciasteczka 7) dokumentuje i testuje interfejsy webowe (np. za pomocą narzędzia Swagger)

	8) implementuje warstwę dostępu do relacyjnej bazy danych, stosując parametryzację zapytań SQL 9) stosuje podstawowe zasady bezpieczeństwa usług webowych: a) walidacja po stronie serwera b) weryfikacja danych wejściowych c) bezpieczne przechowywanie sekretów d) stosowanie audytu (logów) z informacjami o działaniu aplikacji 10) wykorzystuje narzędzia sztucznej inteligencji do generacji i weryfikacji kodu aplikacji webowej
4) konfiguruje oraz uruchamia aplikacje webowe	1) bezpiecznie konfiguruje aplikację webową i web serwer (lub proxy serwer): a) wymusza stosowanie protokołu HTTPS oraz kluczowych nagłówków b) wyłącza zbędne mechanizmy (przeglądanie katalogów) c) przygotowuje dedykowane konta dla uruchamiania aplikacji (web serwera, serwera proxy) 2) bezpiecznie konfiguruje serwer bazy danych oraz dostęp do serwera z poziomu aplikacji (konta z odpowiednimi uprawnieniami) 3) przygotowuje obraz aplikacji webowej wraz z całym środowiskiem uruchomieniowym (web serwer, serwer bazy danych) w kontenerze Docker 4) stosuje podstawowe mechanizmy bezpieczeństwa kontenera Docker: a) wykorzystanie dedykowanego użytkownika

	b) stosowanie minimalnych obrazów bazowych c) konfiguracja minimalnego dostępu do systemu plików d) otwieranie jedynie wymaganych portów
5) wdraża aplikacje webowe w środowisku chmurowym	1) wyjaśnia procesy ciągłej integracji i ciągłego wdrażania (CI/CD) 2) publikuje aplikację webową w środowisku chmurowym, wykorzystując dedykowane usługi platformowe (PaaS) lub konteneryzację 3) konfiguruje proces CI/CD w środowisku chmurowym 4) konfiguruje bezpieczne połączenie HTTPS poprzez instalację i zarządzanie certyfikatami SSL/TLS w infrastrukturze chmurowej 5) integruje aplikację webową z chmurowym magazynem sekretów w celu bezpiecznego przechowywania haseł do baz danych i kluczy API 6) definiuje reguły chmurowej zapory sieciowej, ograniczając ruch przychodzący wyłącznie do niezbędnych portów aplikacji (np. 80, 443) 7) konfiguruje izolowaną sieć wirtualną (np. VPC/VNet) dla bazy danych, tak aby nie była ona dostępna bezpośrednio z sieci internet 8) implementuje mechanizmy logowania zdarzeń w aplikacji i integruje je z chmurowymi systemami monitorowania bezpieczeństwa 9) weryfikuje poprawność wdrożenia poprzez testy łączności oraz skanowanie publicznego

	adresu IP aplikacji pod kątem niepotrzebnie wystawionych usług
INF.12. 4. Weryfikowanie bezpieczeństwa implementacji aplikacji webowych	
Efekty kształcenia	Kryteria weryfikacji
Uczeń:	Uczeń:
1) identyfikuje błędy w kodzie źródłowym związane z poprawnością działania i bezpieczeństwem	1) rozpoznaje typowe błędy programistyczne: a) brak lub niewłaściwa obsługa błędów podczas wykonywania programu, w tym niewłaściwa obsługa wyjątków b) brak właściwego zarządzania zasobami systemu operacyjnego (pliki, gniazda, wątki) c) możliwość zaistnienia wyścigu (race condition) przy wykonywaniu złożonych modyfikacji danych (np. w bazie danych, bez właściwej synchronizacji) 2) rozpoznaje typowe błędy bezpieczeństwa aplikacji: a) przechowywanie sekretów bezpośrednio w kodzie, zwłaszcza w postaci jawnej b) stosowanie niewłaściwych typów do przechowywania sekretów c) brak walidacji danych wejściowych (zwłaszcza po stronie serwera), w tym wgrywanych plików d) brak weryfikacji uprawnień użytkownika do wykonania danej operacji e) ujawnianie wewnętrznych informacji o aplikacji (wersji aplikacji i bibliotek, stosu wywołań) przy raportowaniu błędów

	3) wskazuje podstawowe błędy konfiguracji aplikacji: a) stosowanie słabych lub domyślnych haseł b) przechowywanie sekretów w postaci jawnej w plikach c) włączone informacje o stosie wywołań przy raportowaniu błędów
2) identyfikuje typowe podatności aplikacji webowych na podstawie analizy kodu źródłowego	1) korzysta z dokumentu OWASP Top 10 2) rozpoznaje błędy programistyczne pozwalające na wykonanie ataków typowych dla aplikacji webowych: a) wstrzykiwanie SQL (SQL injection) b) wstrzykiwanie kodu (code injection) c) XSS (Cross-Site Scripting) d) CSRF (Cross-Site Request Forgery) e) przeglądanie katalogów (directory traversal) 3) opisuje znaczenie dla bezpieczeństwa aplikacji nagłówków protokołu HTTP: a) Strict-Transport-Security b) Content-Security-Policy c) X-Frame-Options d) X-Content-Type-Options e) Access-Control-Allow-Origin
3) wykorzystuje narzędzia do analizy i poprawy bezpieczeństwa aplikacji webowych	1) wykorzystuje narzędzia do automatycznej analizy kodu aplikacji pod kątem bezpieczeństwa 2) stosuje narzędzia sztucznej inteligencji w trybie interaktywnym do weryfikacji i korekty fragmentów kodu aplikacji 3) koryguje zidentyfikowane błędy bezpieczeństwa

	4) demonstruje praktycznie poprawność wprowadzonych korekt
4) zabezpiecza aplikacje webowe przed atakiem	1) konfiguruje i uruchamia web serwer w trybie reverse proxy z modułem WAF (Web Application Firewall), chroniący dostęp do aplikacji webowej 2) weryfikuje i koryguje konfigurację web serwera, na którym uruchomiona jest aplikacja webowa 3) weryfikuje i koryguje konfigurację aplikacji webowej, poprawiając jej bezpieczeństwo 4) weryfikuje i koryguje konfigurację serwera bazy danych, ograniczając dostęp do serwera tylko dla aplikacji webowej i wyłączając zbędne konta 5) włącza zaawansowane mechanizmy logowania w celu monitorowania bezpieczeństwa

INF.12.5. Przeprowadzanie testów penetracyjnych aplikacji webowych w środowisku testowym	
Efekty kształcenia	Kryteria weryfikacji
Uczeń:	Uczeń:
1) planuje i przygotowuje testy penetracyjne aplikacji webowych	1) opisuje cel i zakres testów penetracyjnych typu „czarna skrzynka” (black box) aplikacji webowych 2) wyjaśnia pojęcia skanowania podatności oraz testów penetracyjnych i wskazuje różnice pomiędzy nimi 3) określa zakres testu, jego cele, ograniczenia oraz możliwe negatywne skutki

	4) planuje podstawowe etapy testu (rekonesans, identyfikacja podatności i jej wykorzystanie, raportowanie) 5) omawia aspekty prawne, etyczne i organizacyjne testów penetracyjnych i wskazuje wynikające z nich ograniczenia
2) przeprowadza rekonesans i analizę powierzchni ataku aplikacji webowej	1) identyfikuje punkty wejścia do aplikacji: formularze, parametry URL, nagłówki (w tym ciasteczka) oraz inne dane zapytań (payload) 2) analizuje interfejs i logikę działania aplikacji na podstawie: a) obserwacji zachowania interfejsu użytkownika (np. dostępnych widoków, nawigacji, formularzy, akcji użytkownika) b) analizy żądań i odpowiedzi HTTP (np. adresów URL, parametrów, kodów statusu, nagłówków) 3) wskazuje elementy aplikacji należące do jej powierzchni ataku 4) dokumentuje wyniki rekonesansu
3) identyfikuje podstawowe podatności aplikacji webowych metodą „czarnej skrzynki” (black box)	1) wskazuje podatności typu: SQL Injection, XSS (reflected, stored), injection w JavaScript, CSRF 2) rozpoznaje symptomy podatności poprzez analizę: a) błędów przy wprowadzaniu, sanityzacji i walidacji danych b) komunikatów o błędach aplikacji zawierających nadmiarowe informacje c) nagłówków HTTP

	d) zmian w zachowaniu aplikacji przy niestandardowych scenariuszach testowych e) wrażliwości na manipulację parametrami zapytań f) zachowań aplikacji przy manipulacji parametrami sesji (np. podmiana ciasteczek, wygasanie sesji) 3) wskazuje potencjalne skutki wykrytych podatności dla poufności, integralności, dostępności danych i dostępności usługi
4) wykorzystuje narzędzia do automatyzacji testowania bezpieczeństwa aplikacji webowych	1) przeprowadza analizę ruchu HTTP/HTTPS z wykorzystaniem narzędzi typu proxy 2) wykonuje automatyczne skanowanie wykorzystując skanery aplikacji i interpretuje wyniki 3) odróżnia wyniki fałszywie pozytywne od rzeczywistych podatności, poprzez analizę raportów narzędzi bezpieczeństwa 4) interpretuje poziomy krytyczności wykrytych podatności wskazywane przez narzędzie oraz ocenia ich potencjalny wpływ na bezpieczeństwo systemu 5) łączy wyniki skanowania automatycznego z testami manualnymi poprzez samodzielne podatności wytypowanych przez narzędzia automatyczne
5) przeprowadza ataki na mechanizmy uwierzytelniania i sesji aplikacji webowych	1) analizuje mechanizmy logowania i zarządzania sesją: a) identyfikuje metody przesyłania poświadczeń (np. formularze HTML, Basic Auth oraz typy tokenów sesyjnych (np. ciasteczka SessionID, tokeny JWT)

	b) weryfikuje atrybuty bezpieczeństwa ciasteczek (np. HttpOnly, Secure, SameSite) przy użyciu narzędzi deweloperskich 2) demonstruje ataki typu brute force oraz ataki słownikowe na poświadczenia użytkowników w formularzach WWW i usługach systemowych (np. SSH) wykorzystując narzędzia automatyzujące oraz autorskie skrypty w języku Python do łamania słabych haseł 3) identyfikuje błędy w implementacji cyklu życia sesji i ich odporność na manipulację: a) wykrywa podatność na przewidywalność identyfikatorów (np. ID sesji oparte na słabych skrótach/kodowaniu oraz brak wygasania sesji po stronie serwera) b) diagnozuje błędy typu Session Fixation oraz brak unieważnienia tokenów po operacji wylogowania 4) demonstruje techniki przechwytywania i manipulacji aktywną sesją (Session Hijacking): a) przeprowadza praktyczny dowód słuszności poprzez ręczne wstrzyknięcie skradzionego identyfikatora sesji do przeglądarki b) wykonuje akcje wewnątrz aplikacji w imieniu ofiary bez znajomości jej danych uwierzytelniających, dokumentując skuteczność przejęcia konta 5) ocenia skutki przejęcia sesji użytkownika w kontekście bezpieczeństwa całego systemu

	6) analizuje ryzyko kradzieży tokenów poprzez ataki XSS lub podsłuch ruchu sieciowego 7) szacuje potencjalne szkody wynikające z nieautoryzowanego dostępu do danych osobowych lub funkcji administracyjnych
6) demonstruje atak typu Man-in-the-Middle (MiTM)	1) wyjaśnia istotę ataku MiTM 2) przechwytuje i analizuje ruch sieciowy aplikacji webowej z wykorzystaniem narzędzi analizy ruchu w środowisku testowym (np. Wireshark, mitmproxy) do ekstrakcji wrażliwych danych z sesji (np. loginów, haseł, tokenów) 3) przeprowadza atak typu MiTM w celu przechwycenia komunikacji między klientem a serwerem, wykorzystując techniki przekierowania ruchu (np. ARP Spoofing) w sieci lokalnej lub konfigurację złośliwej bramy oraz maszynę pośredniczącą (proxy) 4) wskazuje konsekwencje braku lub niewłaściwego użycia protokołu HTTPS – wyjaśnia rolę certyfikatów SSL/TLS i omawia zagrożenia wynikające z ignorowania błędów certyfikacji przez użytkownika lub błędnej konfiguracji serwera 5) interpretuje przechwycone dane pod kątem ryzyka bezpieczeństwa – analizuje pakiety sieciowe w celu odnalezienia informacji o infrastrukturze serwera, strukturze bazy danych lub prywatnej aktywności użytkownika 6) przeprowadza atak na niewystarczające zabezpieczenia po stronie serwera z

	pominięciem zabezpieczeń klienta (np. modyfikując „w locie” parametry formularza)
7) analizuje wyniki testów penetracyjnych i sporządza podstawową dokumentację testową	1) opisuje wykryte podatności (np. zgodnie z klasyfikacjami CWE (Common Weakness Enumeration, CVE (Common Vulnerabilities and Exposures), CAPEC (Common Attack Pattern Enumeration and Classification)) 2) określa poziom ryzyka wykrytych podatności 3) wskazuje możliwe kierunki ograniczania ryzyka 4) sporządza prosty raport z testu penetracyjnego 5) stosuje zasady rozróżniania testów legalnych od działań nieuprawnionych oraz stosuje zasady odpowiedzialnego ujawniania podatności
INF.12.6. Język angielski zawodowy	
Efekty kształcenia	Kryteria weryfikacji
Uczeń:	Uczeń:
1) posługuje się podstawowym zasobem środków językowych w języku angielskim (ze szczególnym uwzględnieniem środków leksykalnych), umożliwiającym realizację czynności zawodowych w zakresie tematów związanych: a) ze stanowiskiem pracy i jego wyposażeniem b) z głównymi technologiami stosowanymi w danym zawodzie	1) rozpoznaje oraz stosuje środki językowe umożliwiające realizację czynności zawodowych w zakresie: a) czynności wykonywanych na stanowisku pracy, w tym związanych z zapewnieniem bezpieczeństwa i higieny pracy b) narzędzi, maszyn, urządzeń i materiałów koniecznych do realizacji czynności zawodowych c) procesów i procedur związanych z realizacją zadań zawodowych

c) z dokumentacją związaną z danym zawodem d) z usługami świadczonymi w danym zawodzie	d) formularzy, specyfikacji oraz innych dokumentów związanych z wykonywaniem zadań zawodowych e) świadczonych usług, w tym obsługi klienta
2) rozumie proste wypowiedzi ustne artykułowane wyraźnie, w standardowej odmianie języka angielskiego, a także proste wypowiedzi pisemne w języku angielskim, w zakresie umożliwiającym realizację zadań zawodowych: a) rozumie proste wypowiedzi ustne dotyczące czynności zawodowych (np. rozmowy, wiadomości, komunikaty, instrukcje lub filmy instruktażowe, prezentacje), artykułowane wyraźnie, w standardowej odmianie języka b) rozumie proste wypowiedzi pisemne dotyczące czynności zawodowych (np. napisy, broszury, instrukcje obsługi, przewodniki, dokumentację zawodową)	1) określa główną myśl wypowiedzi lub tekstu, ewentualnie fragmentu wypowiedzi lub tekstu 2) znajduje w wypowiedzi lub tekście określone informacje 3) rozpoznaje związki między poszczególnymi częściami tekstu 4) układa informacje w określonym porządku
3) samodzielnie tworzy krótkie, proste, spójne i logiczne wypowiedzi ustne i pisemne w języku angielskim, w zakresie umożliwiającym realizację zadań zawodowych:	1) opisuje przedmioty, działania i zjawiska związane z czynnościami zawodowymi 2) przedstawia sposób postępowania w różnych sytuacjach zawodowych (np. udziela instrukcji, wskazówek, określa zasady) 3) wyraża i uzasadnia swoje stanowisko

a) tworzy krótkie, proste, spójne i logiczne wypowiedzi ustne dotyczące czynności zawodowych (np. polecenie, komunikat, instrukcję) b) tworzy krótkie, proste, spójne i logiczne wypowiedzi pisemne dotyczące czynności zawodowych (np. komunikat, e-mail, instrukcję, wiadomość, CV, list motywacyjny, dokument związany z wykonywanym zawodem – według wzoru)	4) stosuje zasady konstruowania tekstów o różnym charakterze 5) stosuje formalny lub nieformalny styl wypowiedzi adekwatnie do sytuacji
4) uczestniczy w rozmowie w typowych sytuacjach związanych z realizacją zadań zawodowych – reaguje w języku angielskim w sposób zrozumiały, adekwatnie do sytuacji komunikacyjnej, ustnie lub w formie prostego tekstu: a) reaguje ustnie (np. podczas rozmowy z innym pracownikiem, klientem, kontrahentem, w tym rozmowy telefonicznej) w typowych sytuacjach związanych z wykonywaniem czynności zawodowych b) reaguje w formie prostego tekstu pisanego (np. wiadomość, formularz, e-mail, dokument związany z wykonywanym	1) rozpoczyna, prowadzi i kończy rozmowę 2) uzyskuje i przekazuje informacje i wyjaśnienia 3) wyraża swoje opinie i uzasadnia je, pyta o opinie, zgadza się lub nie zgadza z opiniami innych osób 4) prowadzi proste negocjacje związane z czynnościami zawodowymi 5) stosuje zwroty i formy grzecznościowe 6) dostosowuje styl wypowiedzi do sytuacji

zawodem) w typowych sytuacjach związanych z wykonywaniem czynności zawodowych	
5) zmienia formę przekazu ustnego lub pisemnego w języku angielskim w typowych sytuacjach związanych z wykonywaniem czynności zawodowych	1) przekazuje w języku angielskim informacje zawarte w materiałach wizualnych (np. wykresach, symbolach, piktogramach, schematach) oraz audiowizualnych (np. filmach instruktażowych) 2) przekazuje w języku polskim informacje sformułowane w języku angielskim 3) przekazuje w języku angielskim informacje sformułowane w języku polskim lub tym języku 4) przedstawia publicznie w języku angielskim wcześniej opracowany materiał (np. prezentację)
6) wykorzystuje strategie służące doskonaleniu własnych umiejętności językowych oraz podnoszące świadomość językową: a) wykorzystuje techniki samodzielnej pracy nad nauką języka b) współdziała w grupie c) korzysta ze źródeł informacji w języku angielskim d) stosuje strategie komunikacyjne i kompensacyjne	1) korzysta ze słownika dwujęzycznego i jednojęzycznego 2) współdziała z innymi osobami, realizując zadania językowe 3) korzysta z tekstów w języku angielskim, również za pomocą technologii informacyjno-komunikacyjnych 4) identyfikuje słowa klucze, internacjonalizmy 5) wykorzystuje kontekst (tam, gdzie to możliwe), aby w przybliżeniu określić znaczenie słowa 6) upraszcza (jeżeli to konieczne) wypowiedź, zastępuje nieznane słowa innymi, wykorzystuje opis, środki niewerbalne
INF.12.7. Kompetencje personalne i społeczne	

Efekty kształcenia	Kryteria weryfikacji
Uczeń:	Uczeń:
1) przestrzega zasad kultury i etyki zawodowej	1) wykazuje się etyczną postawą i przestrzega zasad prawa w obszarze bezpieczeństwa informacji 2) zachowuje pełną poufność informacji uzyskanych w toku wykonywania zadań zawodowych 3) wykazuje się rzetelnością i odpowiedzialnością za powierzone dane oraz systemy IT 4) identyfikuje dylematy etyczne związane z dostępem do systemów i danych użytkowników 5) stosuje zasady netykiety i profesjonalnej komunikacji w środowisku cyfrowym 6) promuje zasady higieny cyfrowej wewnątrz organizacji 7) respektuje własność intelektualną oraz licencje oprogramowania używanego w pracy 8) korzysta z platform edukacyjnych typu Capture The Flag (CTF) i projektów demonstracyjnych (np. WebGoat)
2) współpracuje w zespole oraz z innymi pracownikami organizacji	1) pracuje w zespole nad złożonymi zadaniami z zakresu IT 2) komunikuje się w sposób jasny i rzeczowy z administratorami oraz programistami 3) współpracuje z użytkownikami końcowymi w celu rozwiązywania problemów technicznych

	4) wykazuje otwartość na opinie innych i konstruktywnie przyjmuje informacje zwrotne 5) rozwiązuje konflikty w zespole IT w sposób profesjonalny i merytoryczny 6) dzieli się wiedzą techniczną i doświadczeniem z innymi członkami zespołu 7) uczestniczy w planowaniu wspólnych działań prewencyjnych i procedur bezpieczeństwa 8) przyjmuje i rzetelnie realizuje zadania delegowane w ramach małych zespołów
3) planuje i organizuje pracę własną, szczególnie w sytuacjach stresowych	1) planuje i organizuje pracę własną na stanowisku technicznym 2) określa priorytety zadań zgodnie z ich krytycznością dla bezpieczeństwa systemów 3) wykazuje się dokładnością i skrupulatnością w wykonywaniu powierzonych czynności 4) zachowuje odporność na stres i opanowanie w sytuacjach awaryjnych 5) potrafi efektywnie pracować pod presją czasu podczas obsługi incydentów 6) dokumentuje podejmowane działania i incydenty w sposób systematyczny i przejrzysty 7) dba o ład i porządek na stanowisku pracy oraz o powierzony sprzęt i narzędzia
4) wykazuje gotowość do ciągłego uczenia się i rozwoju zawodowego	1) wykazuje aktywną postawę w śledzeniu nowych trendów w informatyce i cyberbezpieczeństwie 2) samodzielnie wyszukuje informacje o nowych zagrożeniach i metodach ataków

	3) wykazuje gotowość do ciągłego uczenia się i aktualizowania wiedzy specjalistycznej 4) wykazuje się dociekliwością i spostrzegawczością w identyfikowaniu anomalii systemowych 5) samodzielnie rozwiązuje nowe problemy techniczne z wykorzystaniem dostępnej dokumentacji 6) analizuje własne błędy i wyciąga wnioski w celu doskonalenia procedur bezpieczeństwa 7) planuje ścieżkę dalszego kształcenia i zdobywania certyfikacji branżowych
INF.12.8. Organizacja pracy małych zespołów	
Efekty kształcenia	Kryteria weryfikacji
Uczeń:	Uczeń:
1) planuje realizację zadań zespołu technicznego	1) określa cele i zakres zadań zawodowych dla małego zespołu 2) rozdziela zadania między członków zespołu, uwzględniając ich kompetencje i predyspozycje 3) opracowuje harmonogram prac z uwzględnieniem priorytetów, terminów realizacji i planów awaryjnych 4) identyfikuje zasoby techniczne i narzędzia niezbędne do wykonania zadania 5) uwzględnia procedury i zasady bezpieczeństwa podczas planowania działań 6) ocenia ryzyko związane z realizacją zadań i proponuje działania minimalizujące zagrożenia

	7) planuje pracę pod presją czasu, szczególnie w sytuacjach awaryjnych lub przy obsłudze incydentów
2) koordynuje komunikację i współpracę wewnątrz zespołu oraz z otoczeniem	1) komunikuje się z członkami zespołu w sposób jasny, rzeczowy i profesjonalny 2) wykorzystuje narzędzia do pracy grupowej i systemy kontroli wersji 3) koordynuje współpracę między administratorami, programistami i użytkownikami 4) prowadzi spotkania techniczne dotyczące postępów prac i rozwiązywania problemów 5) stosuje zasady netykiety oraz profesjonalnej komunikacji w środowisku cyfrowym 6) rozstrzyga konflikty techniczne i organizacyjne wewnątrz zespołu 7) przekazuje informacje o zagrożeniach i incydentach właściwym organom lub zespołom nadrzędnym 8) dba o przepływ wiedzy i promowanie zasad higieny cyfrowej w zespole
3) monitoruje postępy prac i dokumentuje działania zespołu	1) kontroluje terminowość i jakość zadań wykonywanych przez członków zespołu 2) weryfikuje poprawność dokumentacji technicznej tworzonej w toku prac 3) analizuje logi i raporty z postępów prac w celu wykrywania nieprawidłowości 4) sporządza zbiorcze raporty z działań zespołu oraz dokumentuje zaistniałe incydenty 5) wykorzystuje narzędzia sztucznej inteligencji do wspomagania procesu raportowania i analizy wyników pracy zespołu (np. notatka

	z podsumowaniem i listą zadań do wykonania) 6) ocenia skuteczność wdrożonych zabezpieczeń i procedur na podstawie wyników zespołu 7) dba o systematyczność i dokładność w gromadzeniu dowodów działań naprawczych
4) zarządza odpowiedzialnością i etyką pracy w zespole IT	1) egzekwuje od członków zespołu zachowanie poufności informacji i danych 2) promuje postawy etyczne i przestrzeganie zasad prawa w obszarze cyberbezpieczeństwa 3) wykazuje się odpowiedzialnością za powierzone zespołowi dane i systemy informatyczne 4) motywuje członków zespołu do ciągłego aktualizowania wiedzy i rozwoju zawodowego 5) monitoruje przestrzeganie zasad bezpieczeństwa i higieny pracy na stanowiskach komputerowych 6) nadzoruje prawidłowość stosowania mechanizmów kontroli dostępu przez członków zespołu 7) ocenia wkład poszczególnych osób w realizację celów bezpieczeństwa organizacji

WARUNKI REALIZACJI KSZTAŁCENIA W ZAWODZIE TECHNIK CYBERBEZPIECZEŃSTWA

Szkoła prowadząca kształcenie w zawodzie zapewnia pomieszczenia dydaktyczne z wyposażeniem odpowiadającym technologii i technice stosowanej w zawodzie, aby umożliwić osiągnięcie wszystkich efektów kształcenia określonych w podstawie programowej kształcenia w zawodzie szkolnictwa branżowego oraz umożliwić przygotowanie absolwenta do

wykonywania zadań zawodowych.

Wyposażenie szkoły niezbędne do realizacji kształcenia w kwalifikacji INF.11. Zarządzanie bezpieczeństwem systemów i sieci komputerowych

Pracownia bezpieczeństwa systemów i sieci komputerowych wyposażona w:

- stanowisko komputerowe dla nauczyciela z urządzeniem wielofunkcyjnym oraz z projektorem multimedialnym lub tablicą interaktywną
- stanowiska komputerowe dla uczniów (jedno stanowisko dla jednego ucznia), wszystkie komputery podłączone do sieci lokalnej z dostępem do internetu, do urządzeń wielofunkcyjnych, pakiet programów biurowych, program do wspomagania projektowania i wykonywania diagramów,
- oprogramowanie do wirtualizacji systemów operacyjnych, systemy operacyjne z rodziny Linux oraz Windows, środowisko do konteneryzacji (Docker),
- środowisko programistyczne Python w wersji wspieranej na dany rok kalendarzowy, zintegrowane środowiska programistyczne dla języka Python, narzędzia systemu kontroli wersji oparte o Git, narzędzia wspierane przez sztuczną inteligencję do generowania i weryfikacji kodu,
- system zarządzania relacyjną bazą danych PostgreSQL oraz narzędzia do obsługi baz nierelacyjnych MongoDB, oprogramowanie do administracji i wersjonowania schematów baz danych,
- analizator ruchu sieciowego Wireshark, skanery sieciowe i skanery podatności (np. nmap, OpenVAS),
- systemy wykrywania i zapobiegania włamaniom typu IDS/IPS,
- oprogramowanie do centralnego monitorowania, korelacji i analizy zdarzeń bezpieczeństwa typu Security Information and Event Management (SIEM),
- oprogramowanie do projektowania, symulacji i emulacji sieci komputerowych, oprogramowanie do monitorowania i analizy zdarzeń,
- narzędzia kryptograficzne do generowania kluczy i certyfikatów, oprogramowanie do szyfrowania danych i wolumenów, systemy do zarządzania sekretami,
- zestaw zarządzalnych fizycznych przełączników (warstwa 2 i 3) oraz routerów (jeden zestaw na dwóch uczniów),
- bezprzewodowe punkty dostępowe (WAP) obsługujące standardy WPA2/WPA3,
- sprzętowa zapora sieciowa (firewall),

- serwer lub stacje robocze o zasobach pamięci RAM umożliwiających uruchomienie środowiska wielosystemowego,
- zewnętrzne nośniki danych do kopii zapasowych,
- testery okablowania i zestaw narzędzi monterskich,
- zestaw do udzielania pierwszej pomocy, opisy procedur postępowania podczas udzielania pomocy poszkodowanym i postępowania w sytuacji zagrożenia życia lub zdrowia.

Ponadto szkoła zapewnia uczniowi dostęp do:

- platformy chmurowej (publicznej lub hybrydowej) umożliwiającej praktyczne wykorzystanie modeli serwisowych (IaaS, PaaS) oraz zarządzanie bezpieczeństwem w chmurze, w tym:
  - dostęp do konsoli administracyjnej umożliwiającej samodzielne tworzenie wirtualnych sieci prywatnych, maszyn wirtualnych Linux oraz grup bezpieczeństwa,
  - środowiska pozwalającego na wdrażanie i orkiestrację kontenerów wraz z prywatnym rejestrem obrazów,
  - narzędzi do nauki kreowania ról, uprawnień i wdrażania uwierzytelniania wieloskładnikowego dla użytkowników i usług,
  - dostępu do usług bezpiecznego przechowywania kluczy,
  - chmurowych systemów zbierania logów i analizy zdarzeń, pozwalających na wykrywanie incydentów w czasie rzeczywistym.

Wyposażenie szkoły niezbędne do realizacji kształcenia w kwalifikacji INF.12. Programowanie bezpiecznych aplikacji webowych

Pracownia programowania i testowania aplikacji webowych wyposażona w:

- stanowisko komputerowe dla nauczyciela, z urządzeniem wielofunkcyjnym oraz z projektorem multimedialnym lub tablicą interaktywną,
- stanowiska komputerowe dla uczniów (jedno stanowisko dla jednego ucznia), wszystkie komputery podłączone do sieci lokalnej z dostępem do internetu, do urządzeń wielofunkcyjnych, pakiet programów biurowych, program do wspomagania projektowania i wykonywania diagramów,
- oprogramowanie do wirtualizacji systemów operacyjnych, systemy operacyjne z rodziny Linux oraz Windows, środowisko do konteneryzacji (Docker),
- zintegrowane środowiska programistyczne do tworzenia aplikacji w języku Java lub C#, środowisko programistyczne Python w wersji wspieranej na dany rok kalendarzowy, zintegrowane środowiska programistyczne dla języka Python, narzędzia systemu kontroli

wersji oparte o Git, narzędzia wspierane przez sztuczną inteligencję do generowania i weryfikacji kodu,

- systemy kontroli wersji oraz narzędzia do automatyzacji budowania projektów, oprogramowanie do tworzenia stron WWW i skryptów po stronie klienta (HTML5, CSS3, JavaScript), środowiska uruchomieniowe oraz narzędzia sztucznej inteligencji wspomagające generowanie i weryfikację kodu pod kątem bezpieczeństwa,
- system zarządzania relacyjną bazą danych PostgreSQL, serwery WWW i serwery typu reverse proxy umożliwiające wymuszanie protokołu HTTPS i konfigurację nagłówków bezpieczeństwa (CSP, HSTS) wraz z oprogramowaniem do automatycznego testowania podatności SQL Injection,
- oprogramowanie do konteneryzacji (Docker) wykorzystywane do budowania i izolacji bezpiecznych środowisk uruchomieniowych aplikacji oraz baz danych wraz z oprogramowaniem umożliwiającym zarządzaniem kontenerami i skanowaniem ich podatności,
- narzędzia typu intercepting proxy do analizy i manipulacji ruchem HTTP/HTTPS, skanery podatności aplikacji webowych oraz narzędzia do statycznej i dynamicznej analizy kodu pod kątem luk (np. SQL Injection, XSS, oprogramowanie do testowania interfejsów API, analizator ruchu sieciowego Wireshark oraz oprogramowanie do przeprowadzania symulacji ataków typu Man-in-the-Middle (MiTM)),
- zestaw do udzielania pierwszej pomocy, opisy procedur postępowania podczas udzielania pomocy poszkodowanym i postępowania w sytuacji zagrożenia życia lub zdrowia.

Ponadto szkoła zapewnia uczniowi dostęp do:

- edukacyjnych platform typu Capture The Flag (CTF) oraz projektów demonstracyjnych z celowo zaimplementowanymi podatnościami do celów treningowych, stacje robocze o zasobach sprzętowych (min. 16 GB RAM) umożliwiających równoległe uruchamianie kontenerów aplikacyjnych i narzędzi testowych, lokalny serwer repozytoriów dla projektów zespołowych oraz dokumentacja techniczna online,
- platformy chmurowej (publicznej lub hybrydowej) umożliwiającej praktyczne wykorzystanie modeli serwisowych (IaaS, PaaS) oraz zarządzanie bezpieczeństwem w chmurze, w tym:
  - konsoli administracyjnej umożliwiającej samodzielne tworzenie wirtualnych sieci prywatnych, maszyn wirtualnych Linux oraz grup bezpieczeństwa,

- środowiska pozwalającego na wdrażanie i orkiestrację kontenerów wraz z prywatnym rejestrem obrazów,
- narzędzi do nauki kreowania ról, uprawnień i wdrażania uwierzytelniania wieloskładnikowego dla użytkowników i usług,
- usług bezpiecznego przechowywania kluczy,
- chmurowych systemów zbierania logów i analizy zdarzeń, pozwalających na wykrywanie incydentów w czasie rzeczywistym.

Miejsce realizacji praktyk zawodowych: jednostki samorządu terytorialnego w komórkach organizacyjnych odpowiedzialnych za rozwój i utrzymanie sieci i usług IT, przedsiębiorstwa usługowe zajmujące się projektowaniem, tworzeniem i obsługą systemów informatycznych, przedsiębiorstwa zajmujące się rozwojem i administracją sieci, centra danych, przedsiębiorstwa zajmujące się hostingiem oraz projektowaniem, tworzeniem i administracją witryn internetowych oraz innych technologii webowych, przedsiębiorstwa zajmujące się tworzeniem programów desktopowych i aplikacji internetowych, przedsiębiorstwa zajmujące się tworzeniem aplikacji mobilnych, operatorzy infrastruktury krytycznej, oraz inne podmioty stanowiące potencjalne miejsce zatrudnienia absolwentów szkół prowadzących kształcenie w zawodzie lub branżowe centra umiejętności w dziedzinach informatyka i programowanie lub telekomunikacja.

Liczba tygodni przeznaczonych na realizację praktyk zawodowych: 8 tygodni (280 godzin), z tym że w przypadku realizacji praktyk w branżowym centrum umiejętności ich wymiar zrealizowany w tym centrum nie może przekroczyć 50% łącznego wymiaru praktyk.

MINIMALNA LICZBA GODZIN KSZTAŁCENIA ZAWODOWEGO DLA KWALIFIKACJI WYODRĘBNIONYCH W ZAWODZIE[1)]

INF.11. Zarządzanie bezpieczeństwem systemów i sieci komputerowych	
Nazwa jednostki efektów kształcenia	Liczba godzin
INF.11.1. Bezpieczeństwo i higiena pracy	30
INF.11.2. Podstawy cyberbezpieczeństwa systemów IT	120
INF.11.3. Programowanie w języku Python	120
INF.11.4. Projektowanie i administracja relacyjnymi bazami danych	150

INF.11.5. Administrowanie sieciami TCP/IP	150
INF.11.6. Użytkowanie, konfiguracja i utwardzanie systemu Windows i Linux	180
INF.11.7. Testowanie bezpieczeństwa sieci TCP/IP	90
INF.11.8. Język angielski zawodowy	60
Razem	900
INF.11.9. Kompetencje personalne i społeczne[2)]	
INF.11.10. Organizacja pracy małych zespołów[3)]	

INF.12. Programowanie bezpiecznych aplikacji webowych	
Nazwa jednostki efektów kształcenia	Liczba godzin
INF.12.1. Bezpieczeństwo i higiena pracy	30
INF.12.2. Podstawy cyberbezpieczeństwa systemów IT[4)]	120[4)]
INF.12.3. Implementacja aplikacji webowych	210
INF.12.4. Weryfikowanie bezpieczeństwa implementacji aplikacji webowych	120
INF.12.5. Przeprowadzanie testów penetracyjnych aplikacji webowych w środowisku testowym	180
INF.12.6. Język angielski zawodowy	60
Razem	600 + 120[4)]
INF.12.7. Kompetencje personalne i społeczne[2)]	
INF.12.8. Organizacja pracy małych zespołów[3)]	

[1)] W szkole liczbę godzin kształcenia zawodowego należy dostosować do wymiaru godzin określonego w przepisach w sprawie ramowych planów nauczania dla publicznych szkół, przewidzianego dla kształcenia zawodowego w danym typie szkoły, zachowując minimalną liczbę godzin wskazanych w tabeli dla efektów kształcenia właściwych dla kwalifikacji wyodrębnionej w zawodzie.

[2)] Nauczyciele wszystkich obowiązkowych zajęć edukacyjnych z zakresu kształcenia zawodowego powinni stwarzać uczniom warunki do nabywania kompetencji personalnych i społecznych.

[3)] Nauczyciele wszystkich obowiązkowych zajęć edukacyjnych z zakresu kształcenia zawodowego powinni stwarzać uczniom warunki do nabywania umiejętności w zakresie organizacji pracy małych zespołów.

[4)] Wskazana jednostka efektów kształcenia nie jest powtarzana w przypadku, gdy kształcenie zawodowe odbywa się w szkole prowadzącej kształcenie w tym zawodzie.”;