



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Zarządzanie bezpieczeństwem w systemach IT

Przedmiot

Kierunek studiów

Informatyka

Studia w zakresie (specjalność)

Technologie przetwarzania danych

Poziom studiów

drugiego stopnia

Forma studiów

stacjonarne

Rok/semestr

2/3

Profil studiów

ogólnoakademicki

Język oferowanego przedmiotu

polski

Wymagalność

obieralny

Liczba godzin

Wykład

30

Laboratoria

30

Inne (np. online)

Ćwiczenia

Projekty/seminaria

Liczba punktów ECTS

4

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:

dr inż. Anna Grocholewska-Czuryło

Odpowiedzialny za przedmiot/wykładowca:

mgr inż. Michał Apolinarski

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać wiedzę w zakresie architektury systemów komputerowych, zasad działania systemów operacyjnych, sieci komputerowych oraz mechanizmów ochrony danych. Powinien potrafić pozyskiwać informacje z literatury, baz danych i innych źródeł oraz integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie.

Cel przedmiotu

Studenci zapoznają się z projektowaniem systemów zarządzania bezpieczeństwem teleinformatycznym w nowoczesnej firmie, a więc w oparciu o normy i standardy, przeprowadzaniem analizy ryzyka, audytów (w tym testów penetracyjnych) i zaproponowaniem odpowiedniego doboru zabezpieczeń i metod reagowania na incydenty.

Przedmiotowe efekty uczenia się

Wiedza

Student/ka ma szczegółową wiedzę na temat:



- jakie kryteria powinien spełniać bezpieczny system informatyczny, jak ocenić bezpieczeństwo danego systemu informatycznego i jak zarządzać określonym poziomem bezpieczeństwa,
- jak przeprowadzać analizę ryzyka w systemie informatycznym (wg różnych metodologii),
- jak dobierać zabezpieczenia w systemie informatycznym chcąc osiągnąć określony poziom bezpieczeństwa,
- jak przeprowadzać testy penetracyjne i jakich narzędzi używać,
- jak sformułować politykę bezpieczeństwa dla przykładowej firmy.

Umiejętności

Student/ka potrafi:

- przeprowadzić analizę ryzyka wg. wybranej metodologii (sklasyfikować aktywa systemu informatycznego, zagrożenia i oszacować czy system informatyczny jest podatny na te zagrożenia),
- dokonać analizy i oszacowania poziomu bezpieczeństwa zastosowanych mechanizmów zabezpieczających,
- zaproponować i zaprojektować politykę bezpieczeństwa całego systemu informatycznego.

Kompetencje społeczne

Student/ka rozumie:

- jak ważnym aspektem jest zastosowanie odpowiednich zabezpieczeń i metod ochrony (fizycznych, kryptograficznych, organizacyjno-administracyjnych i prawnych),
- jak ważne jest stosowanie standardów i norm bezpieczeństwa,
- konieczne jest aktualizowanie wiedzy w dziedzinie bezpieczeństwa oraz ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżyniera-informatyka i związaną z tym odpowiedzialność za podejmowane decyzje.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza nabyta w ramach wykładu weryfikowana jest podczas pisemnego 45-minutowego egzaminu, składającego się z 8 pytań. Próg zaliczeniowy: ponad 50% punktów. Zagadnienia zaliczeniowe, na podstawie których opracowywane są pytania są przysyłane studentom pocztą elektroniczną na początku semestru.

Umiejętności nabyte w ramach zajęć projektowych weryfikowane są na bieżąco podczas zajęć (przy omawianiu kolejnych etapów i części projektu) oraz przez dokonanie końcowej oceny projektu i jego dokumentacji przez prowadzącego zajęcia.



Treści programowe

Wykład

1. Wprowadzenie - określenie co oznacza, że system informatyczny jest systemem bezpiecznym, wiarygodnym, jak oceniamy bezpieczeństwo, relacje pomiędzy elementami bezpieczeństwa, standardy, miary, normy i najlepsze praktyki (TCSEC, ITSEC, ISO, CC).
2. Klasyfikacja zagrożeń zarówno sieciowych, kryptograficznych jak i eksploatacyjnych systemów komputerowych. Określanie stopnia podatności systemów na zagrożenia (metody ilościowe i jakościowe).
3. Analiza i zarządzanie ryzykiem. Definiowanie oraz dyskusja nad sposobami osiągania i utrzymywania założonego poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności. Dobór odpowiednich środków zabezpieczających. Przykłady procesów zarządzania ryzykiem w firmie, w konkretnym systemie informatycznym.
4. Polityka bezpieczeństwa - przykładowe dokumenty wchodzące w skład polityki bezpieczeństwa
5. Audyt - przykład wdrożenia systemu zarządzania bezpieczeństwem (COBIT, MARION, TISM, OSSTM, LP-A)
6. Testy penetracyjne - techniki i dobór odpowiednich narzędzi do przeprowadzania testów penetracyjnych
7. W oparciu o normy i zalecenia projektowanie i eksploatacja bezpiecznych systemów. Na podstawie znajomości z wcześniejszych przedmiotów mechanizmów ochrony, projektowanie zintegrowanych systemów zarządzania bezpieczeństwem.

Laboratorium

Opracowanie projektu i implementacji oraz dokumentacji systemu zarządzania bezpieczeństwem w wybranym środowisku informatycznym uwzględniając m.in. inwentaryzację zasobów IT, typ przetwarzanych danych (analiza systemu pod kątem wymagań UODO); analizę zagrożeń i oszacowanie podatności systemu na te zagrożenia, zaproponowanie mechanizmów zabezpieczających, minimalizujących ryzyko; analizę powdrożeniową; kosztorys projektu. Opracowanie dokumentacji polityki bezpieczeństwa analizowanego systemu.

Metody dydaktyczne

Wykład prowadzony jest w sposób interaktywny (z formułowaniem pytań do studentów) przy użyciu prezentacji multimedialnych. Materiały udostępniane są studentom w wersji elektronicznej.

Laboratorium prowadzone jest w formie konsultacji i weryfikacji kolejnych etapów projektowania i implementowania. Zadania wykonywane są w zespołach.

Literatura



Podstawowa

Białas A., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa 2017 (sygnatura w Bibliotece PP W 113481)

Pieprzyk J., Hardjono T., Seberry J., Teoria bezpieczeństwa systemów komputerowych, Helion, 2003 (sygnatura w Bibliotece PP W 110215)

Książopolski B., Szałachowski P., Audyt bezpieczeństwa systemów IT - ścieżka techniczna (rekonesans i skanowanie), Wyd. Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2011 (sygnatura w Bibliotece PP A 174729)

Uzupełniająca

Normy ISO (13335, 2700x) (w czytelni Biblioteki PP)

Weidman G., Bezpieczny system w praktyce. Wyższa szkoła hackingu i testy penetracyjne, Helion 2014. (sygnatura w Bibliotece PP W 155592)

Bilans nakładu pracy przeciętnego studenta

| | Godzin | ECTS |
|---|--------|------|
| Łączny nakład pracy | 100 | 4,0 |
| Zajęcia wymagające bezpośredniego kontaktu z nauczycielem | 60 | 2,0 |
| Praca własna studenta (studia literaturowe, przygotowanie projektu i implementacja, przygotowanie do egzaminu) ¹ | 40 | 2,0 |

¹ niepotrzebne skreślić lub dopisać inne czynności