KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Ochrona danych [S2IBiJ1-BiZK>OD]

Przedmiot

Kierunek studiów
Inżynieria bezpieczeństwa i jakości

Rok/Semestr
1/2

Studia w zakresie (specjalność)
Bezpieczeństwo i zarządzanie kryzysowe

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
0

Laboratorium
0

Inne (np. online)
0

Ćwiczenia
30

Projekty/seminaria
0

Liczba punktów ECTS

2,00

Koordynatorzy

dr inż. Marek Goliński
marek.golinski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student posiada podstawową wiedzę, niezbędną do zrozumienia społecznych i prawnych uwarunkowań prowadzenia działalności inżynierskiej. Student posiada umiejętność wykorzystania wskazanych źródeł oraz interpretacji zjawisk społecznych. Student rozumie konieczność poszerzania swoich kompetencji w ramach nauk społecznych.

Cel przedmiotu

Przekazanie studentom wiedzy w zakresie wymogów stawianych przedsiebiorcom i innym organizacjom w zakresie gromadzenia i przetwarzania danych osobowych oraz zasady odpowiedzialności prawnej stąd wynikającej.

Przedmiotowe efekty uczenia się

Wiedza:
1. Student zna w pogłębionym stopniu tendencje rozwojowe oraz dobre praktyki dotyczące zarządzania bezpieczeństwem w szczególności bezpieczeństwem danych w ogranizacjach w ujęciu lokalnym i globalnym [K2_W04].
2. Student zna w pogłębionym stopniu zasady przepływu informacji, komunikacji, uwarunkowań

prawnych i regulacyjnych wpływających na ochronę danych charakterystyczne dla obszaru zarządzania bezpieczeństwem organizacji [K2_W14].

Umiejętności:
1. Student potrafi stosować metody i narzędzia rozwiązywania złożonych i nietypowych problemów oraz zaawansowane techniki informacyno-komunikacyjne charakterystyczne dla środowiska zawodowego związanego z zarządzaniem i ochroną danych w organizacjach [K2_U02].
2. Student potrafi dobrać i zastosować narzędzia komputerowego wspomagania rozwiązywania problemów charakterystycznych dla zarządzania sferą ochrony danych w ogranizacjach [K2_U08].

Kompetencje społeczne:
1. Student jest krytyczny wobec swojej wiedzy, jest gotów do zasięgania opinii ekspertów podczas rozwiązywania problemów poznawczych i praktycznych, ciągłego dokształcania z branży IT i regulacji prawnych, w szczególności związanych z ochroną danych w obszarze zarządzania bezpieczeństwem w organizacjach [K2_K01].
2. Student prawidłowo identyfikuje i rozstrzyga dylematy związane z szeroko pojętym bezpieczeństwem, szczególnie w obszarze danych, rozumie konieczność uświadamiania społeczeństwa w zakresie potrzeby kształtowania bezpieczeństwa w różnych obszarach funkcjonowania organizacji [K2_K02].

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Ocena formująca: dyskusje podsumowujące poszczególne ćwiczenia, rozwiązywane w trakcie zajęć problemy prawne, dające możliwość oceny zrozumienia problematyki przez studenta.
Wiedza nabyta w ramach ćwiczeń jest weryfikowana przez dwa 15-minutowe kolokwia, z których każde składa się z 5- 10 pytań, różnie punktowanych, konieczność zaliczenia obu kolokwiów.
Ocena podsumowująca: pisemne zaliczenie przedmiotu w formie testu realizowanego na ostatnich zajęciach ćwiczeniowych. Kolokwium składa się z ok. 10 pytań. Próg zaliczeniowy: 51% punktów. Skala ocen jest zgodna z zasadami opisanymi w regulaminie studiów.

Treści programowe

Ćwiczenia:
Case study - procesy przetwarzania danych osobowych w firmie. Rodzaje dokumentów związanych z wybranymi procesami przetwarzania danych w firmie. Umowa o dzieło/zlecenie, umowa powierzenia przetwarzania danych osobowych, zgoda na wykorzystanie wizerunku, przetwarzanie danych zwykłych i sensytywnych. Ochrona danych osobowych w miejscu pracy. Ochrona i bezpieczeństwo danych osobowych z punktu widzenia osoby fizycznej i osoby prawnej, z uwzględnieniem wyzwań wynikających z funkcjonowania w świecie cyfrowym.

Tematyka zajęć

Ćwiczenia
Case study - Procesy przetwarzania danych osobowych w firmie
Ćwiczenia w formie studium przypadku obejmują analizę i ocenę procesów przetwarzania danych osobowych w konkretnej firmie. Uczestnicy zapoznają się z praktycznymi aspektami przetwarzania danych, identyfikują potencjalne problemy i proponują rozwiązania zgodne z przepisami o ochronie danych osobowych. Analiza obejmuje cały cykl życia danych osobowych, od momentu ich zbierania, przez przechowywanie, aż po usuwanie.

Rodzaje dokumentów związanych z wybranymi procesami przetwarzania danych w firmie
Ćwiczenia te koncentrują się na różnych typach dokumentów, które są niezbędne do prawidłowego zarządzania procesami przetwarzania danych osobowych w firmie. Uczestnicy uczą się tworzyć i zarządzać dokumentacją, która obejmuje:

Umowa o dzieło/zlecenie: dokumenty regulujące współpracę z wykonawcami zewnętrznymi, które mogą obejmować klauzule dotyczące przetwarzania danych osobowych.
Umowa powierzenia przetwarzania danych osobowych: umowy między administratorem danych a podmiotem przetwarzającym, które określają zasady i warunki przetwarzania danych w imieniu administratora.

Zgoda na wykorzystanie wizerunku: dokumenty, które pozwalają firmie na legalne używanie wizerunku pracowników lub klientów do celów marketingowych lub promocyjnych.
Przetwarzanie danych zwykłych i sensytywnych: procedury i polityki dotyczące różnic w przetwarzaniu danych zwykłych (np. imię, nazwisko, adres) i sensytywnych (np. dane zdrowotne, dane biometryczne).
Ochrona danych osobowych w miejscu pracy
Ćwiczenia obejmują analizę polityk i procedur dotyczących ochrony danych osobowych pracowników w miejscu pracy. Uczestnicy uczą się, jak firmy powinny zarządzać danymi osobowymi pracowników, jakie środki bezpieczeństwa wdrażać oraz jakie prawa mają pracownicy w kontekście ochrony ich danych osobowych.

Ochrona i bezpieczeństwo danych osobowych z punktu widzenia osoby fizycznej i osoby prawnej, z uwzględnieniem wyzwań wynikających z funkcjonowania w świecie cyfrowym
Ćwiczenia koncentrują się na ochronie danych osobowych z dwóch perspektyw:

Osoba fizyczna: analiza, jakie prawa mają jednostki w kontekście ochrony ich danych osobowych, jakie ryzyka i zagrożenia wiążą się z przetwarzaniem danych w cyfrowym świecie oraz jakie środki mogą podjąć, aby chronić swoje dane.
Osoba prawna: omówienie obowiązków i odpowiedzialności firm w zakresie ochrony danych osobowych, z naciskiem na zarządzanie ryzykiem, zgodność z regulacjami prawnymi, wprowadzenie odpowiednich polityk i procedur oraz reagowanie na incydenty naruszenia danych. Uczestnicy analizują także wyzwania związane z cyfryzacją, takie jak cyberbezpieczeństwo, zarządzanie danymi w chmurze oraz zgodność z międzynarodowymi przepisami ochrony danych.

Metody dydaktyczne

prezentacja informacyjna, dyskusja z rozwiązywaniem problemów, dyskusja z wykorzystaniem prezentacji multimedialnej, metoda przypadków, dyskusja.

Literatura

Podstawowa:
1. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. Nr 78, poz. 483 ze zm.)
2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
3. Ustawa o ochronie danych osobowychz dnia 10 maja 2018 r. (Dz. U. z 2019 r. poz. 1781 t.j.)
4. Ustawa Kodeks pracy z dnia 26 czerwca 1974 r. (Dz. U. z 2020 r. poz. 1320 t.j.)
5. Fajgielski P. (2019), Prawo ochrony danych osobowych. Zarys wykładu, Wydawnictwo Wolters Kluwer, Warszawa.

Uzupełniająca:
1. Ustawa Kodeks cywilny z dnia 23 kwietnia 1964 r. (Dz. U. 2020 r. poz. 1740 t.j.)
2. Ustawa o prawie autorskim i prawach pokrewnych z dnia 4 02 1994 r. (Dz. U. 2021 r. poz. 1062 t.j.)
3. Ustawa o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2020 r. (Dz. U. 2020 r. poz. 344 t.j.)
4. Majchrzak J., Goliński M., Matura W., The concept of the qualitology and grey system theory application in marketing information quality cognition and assessment, Central European Journal of Operations Research, 2020, Vol. 28, No. 2

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	60	2,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	30	1,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	30	1,00