Bezpieczeństwo w Sieci - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Bezpieczeństwo w Sieci
Kod przedmiotu	11.3-WP-AKTAS-BwS
Wydział	Wydział Nauk Społecznych
Kierunek	Animacja kultury i twórczej aktywności w sieci
Profil	ogólnoakademicki
Rodzaj studiów	pierwszego stopnia z tyt. licencjata
Semestr rozpoczęcia	semestr zimowy 2022/2023

Informacje o przedmiocie

Semestr	3
Liczba punktów ECTS do zdobycia	1
Typ przedmiotu	obowiązkowy
Język nauczania	polski
Sylabus opracował	• dr Jacek Jędryczkowski

Formy zajęć

Forma zajęć	Liczba godzin w semestrze (stacjonarne)	Liczba godzin w tygodniu (stacjonarne)	Liczba godzin w semestrze (niestacjonarne)	Liczba godzin w tygodniu (niestacjonarne)	Forma zaliczenia
Ćwiczenia	15	1	9	0,6	Zaliczenie na ocenę

Cel przedmiotu

Celem przedmiotu jest przygotowanie użytkownika współczesnych mediów cyfrowych do dokonywania świadomej analizy bezpieczeństwa informacji, w tym bezpieczeństwa danych – przede wszystkim w komunikacji sieciowej. Zwrócenie uwagi na prawa autorskie i regulacje prawne dotyczące ochrony danych, a także przygotowanie do samodzielnego diagnozowania i modyfikowania zabezpieczeń wykorzystywanego oprogramowania.

Wymagania wstępne

Podstawowa wiedza z zakresu wykorzystania technologii informacyjnych w komunikacji za pośrednictwem mediów elektronicznych.

Zakres tematyczny

Problematyka bezpieczeństwa informacji. Ochrona danych i systemów informatycznych. Techniki i technologie zapewnienia bezpieczeństwa informacji i danych osobowych. Zrozumienie zasad zarządzania ryzykiem na potrzeby bezpieczeństwa informacyjnego. Bezpieczeństwo przesyłu danych i transakcji finansowych. Anonimowość i ochrona danych w sieci (aplikacje – TOR). Ochrona danych osobowych – RODO, ustawa i komentarze. Prawa autorskie i prawa pokrewne: pojęcie utworu, prawa do korzystania z utworu, dozwolony użytek osobisty utworu, umowa o przeniesienie autorskich praw majątkowych, utwór audiowizualny, nadawanie wykonań artystycznych.

Podział dysku na partycje. Punkt przywracania systemu. Tworzenie obrazu partycji systemowej na partycji z danymi – aplikacje. Odzyskiwanie systemu z obrazu dysku. Szyfrowanie oraz ukrywanie partycji. Wolne oprogramowanie – wady i zalety. Mechanizmy szyfrujące w pakietach biurowych (zabezpieczenia w edytorze tekstu, arkuszu kalkulacyjnym i in.). Archiwa chronione hasłem. Aplikacje szyfrujące i niszczące pliki. Odzyskiwanie danych z różnych nośników. Praca w chmurze jako alternatywny sposób ochrony danych – wady i zalety; Archiwizacja danych – rozwiązania lokalne QNAP i Synology oraz umieszczanie danych w chmurze: Dokumenty Google, Microsoft SkyDrive, DropBox. Sieć Wi-Fi – niebezpieczeństwa i zabezpieczenia.

Przeglądarki internetowe: konfiguracja pod kątem bezpieczeństwa korzystania w Sieci, ochrona danych lokalnych, blokowanie możliwości profilowania.

Metody kształcenia

Pokaz, demonstracja, korzystanie z multimedialnych kursów online: blended learning oraz e-learning, metoda zajęć praktycznych, metoda laboratoryjna.

Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
Student posiada wiedzę praktyczną, pozwalającą zdefiniować istotę bezpieczeństwa informacji, zarządzania tym bezpieczeństwem oraz wykazuje się wiadomościami na temat formalnych przesłanek ochrony danych osobowych, prawa autorskiego i praw pokrewnych. Rozumie potrzebę szanowania cudzej własności intelektualnej i praw autorskich. Rozumie potrzebę dbałości o ochronę danych osobowych własnych i współuczestników interakcji społecznych. Posiada wiedzę nt. blokowania dostępu do danych, szyfrowania danych, korzystania z oprogramowania komercyjnego i wolnego (aplikacji na licencjach Open Source i GNU). Wskazuje metody i sposoby zabezpieczania danych na poziomie systemu operacyjnego i aplikacji użytkowych. Omawia możliwości archiwizowania danych lokalnie, w sieci i w chmurze. Zna aplikacje i sposoby tworzenia obrazu partycji systemowej i jej odzyskiwania. Rozumie i stosuje zasady bezpiecznego korzystania z sieci Wi-Fi.	• K_W07	• aktywność w trakcie zajęć • praca kontrolna • test z pytaniami zamkniętymi i otwartymi • Ocena jakości wykonania zadań praktycznych; Ocena prac – progi punktowe (zgodność wykonania z wytycznymi).	• Ćwiczenia
Dokonuje świadomego wyboru stosowanych rozwiązań komercyjnych bądź wolnych (open source) np. system operacyjny (Windows, OS czy Linux) i zależne od nich oprogramowania. Potrafi przewidywać próby łamania zabezpieczeń systemowych. Zabezpiecza dostęp do danych (szyfrowanie np. NTFS, bitlocker). Odzyskuje dane z różnych nośników oraz potrafi trwale je niszczyć. Blokuje dostęp do komputera i danych na poziome sprzętowym i programowym. Archiwizuje zaszyfrowane dane w sieci lokalnej i w chmurze. Tworzy obraz partycji systemowej oraz w przypadku awarii systemu wykonuje jego odzyskiwanie. Zabezpiecza sieć Wi-Fi. Eliminuje zagrożenia wynikające z przechwytywania danych w przeglądarek internetowych. Blokuje dostęp do danych pozwalających profilować i ograniczać dostęp do informacji.	• K_U08	• aktywność w trakcie zajęć • praca kontrolna • test z pytaniami zamkniętymi i otwartymi • Ocena jakości wykonania zadań praktycznych; Ocena prac – progi punktowe (zgodność wykonania z wytycznymi).	• Ćwiczenia
Student posiada ugruntowaną wiedzę o znaczeniu i modelach oraz dokumentowaniu systemu ochrony informacji, prawach (przywilejach) wynikających z ustaw i rozporządzeń, sposobach zabezpieczania informacji, w tym danych osobowych. Zna metody szyfrowania informacji, blokowania dostępu do danych behawioralnych oraz potrafi zabezpieczać dane lokalne i w sieci.	• K_K03	• aktywność w trakcie zajęć • bieżąca kontrola na zajęciach • test z pytaniami zamkniętymi i otwartymi • Ocena jakości wykonania zadań praktycznych; Ocena prac – progi punktowe (zgodność wykonania z wytycznymi).	• Ćwiczenia

Warunki zaliczenia

Wiadomości z zajęć realizowanych zastosowaniem metody samodzielnej pracy z książką lub kursem online będą sprawdzane z zastosowaniem testów z progami punktowymi. Umiejętności praktyczne oraz kompetencje społeczne są oceniane na podstawie oceny prac wykonywanych na zajęciach – progi punktowe.

Laboratoria

Zaliczenie wszystkich kolokwiów (progi punktowe; warunkiem uzyskania oceny pozytywnej jest zdobycie minimum 60% punktów) oraz wszystkich innych podlegających ocenie zadań i prac. Ocena końcowa jest średnią arytmetyczną wszystkich ocen cząstkowych.

Ocena końcowa

Ocena końcowa jest oceną z laboratorium (średnia arytmetyczna wszystkich ocen).

Literatura podstawowa

1. Jędryczkowski J., *Bezpieczeństwo systemu operacyjnego i ochrona danych osobowych*, [w:] *Technologie informacyjne w warsztacie pracy nauczyciela*, red. M. Furmanek, Zielona Góra 2008.
2. Jędryczkowski J., Materiały online: http://staff.uz.zgora.pl/jjedrycz/bezpieczenstwo_sd.html, https://www.youtube.com/c/JJKursy
3. Flisak D., *Utwór multimedialny w prawie autorskim*, Warszawa 2008.
4. Hetman J., *Ustawa o prawie autorskim i prawach pokrewnych z przepisami wykonawczymi*, 2007.
5. Mozgawa M., Poźniak-Niedzielska M., Szczotka J., *Prawo autorskie i prawa pokrewne*, Bydgoszcz 2006.

6. Stallings W., *Kryptografia i bezpieczeństwo sieci komputerowych*, Gliwice 2012.

Literatura uzupełniająca

1. Jędryczkowski J., *http://staff.uz.zgora.pl/jjedrycz*
2. Karpowicz A., Podręcznik prawa autorskiego dla studentów uczelni artystycznych, Warszawa 2001.
3. *Konstytucja Rzeczypospolitej Polskiej.*
4. *Prawo autorskie i prasowe z wprowadzeniem*, Warszawa 2007.
5. 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) (Tekst mający znaczenie dla EOG): https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016R0679

Uwagi

Zmodyfikowane przez mgr inż. Maciej Jackowski (ostatnia modyfikacja: 22-04-2022 10:57)