Bezpieczeństwo systemów i danych - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Bezpieczeństwo systemów i danych
Kod przedmiotu	11.3-WP-PEDD-BSD-L_pNadGen2E0RO
Wydział	Wydział Nauk Społecznych
Kierunek	Pedagogika / Edukacja medialna i informatyczna
Profil	ogólnoakademicki
Rodzaj studiów	drugiego stopnia z tyt. magistra
Semestr rozpoczęcia	semestr zimowy 2016/2017

Informacje o przedmiocie

Semestr	4
Liczba punktów ECTS do zdobycia	2
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
Laboratorium	15	1	9	0,6	Zaliczenie na ocenę

Cel przedmiotu

Wykazanie iż ochrona danych i praw autorskich jest obowiązkiem każdego obywatela i wynika z obowiązującego w Polsce prawa. Uświadomienie studentom, iż bez specjalnych zabezpieczeń komputery, systemy operacyjne oraz dane są łatwo dostępne dla osób do tego niepowołanych. Wyposażenie studentów w kompetencje umożliwiające ochronę komputera i danych, a także do odzyskiwania danych utraconych w wyniku zaniedbania lub awarii. Wyposażenie w kompetencje umożliwiające diagnozowanie systemu operacyjnego pod kontem poziomu jego zabezpieczeń.

Wymagania wstępne

Podstawowa wiedza z zakresu przedmiotu obowiązkowego „technologie informacyjne”.

Zakres tematyczny

Ochrona danych i systemów komputerowych. Konstytucja jako akt nadrzędny do całości porządku prawnego. Ochrona danych osobowych – ustawa i komentarze. Prawa autorskie i prawa pokrewne: pojęcie utworu, prawo do korzystania z utworu, dozwolony użytek osobisty utworu, umowa o przeniesienie autorskich praw majątkowych, utwór audiowizualny, nadawanie wykonań artystycznych przez organizacje radiowe i telewizyjne. Licencje: Open Source i GNU. Wolne oprogramowanie – wady i zalety z punktu widzenia bezpieczeństwa i ochrony danych. System Windows – sposoby na obejście zapieczeń i możliwości przeciwdziałania utracie danych. Niebezpieczeństwa związane z szyfrowaniem NTFS oraz eksport i import kopii zapasowej certyfikatu i klucza szyfrowania plików. Mechanizmy szyfrujące w pakietach biurowych. Przykład zabezpieczeń w arkuszu kalkulacyjnym. Archiwa chronionych hasłem. Aplikacje szyfrujące i niszczące pliki. Szyfrowanie partycji oraz ukrywanie partycji. Aplikacje do odzyskiwania danych z różnych nośników. Praca w chmurze jako alternatywny sposób ochrony danych – wady i zalety; Gromadzenie danych w chmurze: Dokumenty Google, Microsoft SkyDrive, DropBox oraz rozwiązania komercyjne. Systemy bootujące (CD i USB) jako narzędzia do odzyskiwania oraz kradzieży danych. Sposoby zabezpieczenia komputera przed systemami bootujacymi. Mechaniczne – sprzętowe zabezpieczenia przed utratą danych – kieszenie i dyski przenośne. Punkt przywracania systemu. Podział dysku na partycje. Tworzenie obrazu partycji systemowej na partycji z danymi – aplikacje. Odzyskiwanie systemu z obrazu dysku. Anonimowość w sieci – aplikacje. Sieć Wi-Fi – niebezpieczeństwa i zabezpieczenia.

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
Student określa zalety i wady wolnego oprogramowania. Wskazuje sposoby obchodzenia zabezpieczeń systemowych oraz ich blokowania. Określa wady i zalety szyfrowania NTFS. Wskazuje alternatywne sposoby szyfrowania danych. Określa sposoby odzyskiwania danych oraz trwałego ich niszczenia. Określa możliwości i ograniczenia systemów bootujacych (CD, USB). Omawia możliwości archiwizowania danych w chmurze. Wymienia aplikacje i sposoby tworzenia obrazu partycji systemowej oraz jej odzyskiwania. Wymienia zasady bezpiecznego korzystania z sieci Wi-Fi	• K_W05 • K_W17	• Test z progami punktowymi (zadania otwarte i zamknięte)	• Laboratorium

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
Prezentuje wiadomości na temat podstawowych aspektów prawnych: ochrony danych osobowych, prawa autorskiego i praw pokrewnych, korzystania z aplikacji na licencjach Open Source i GNU	• K_W16	• Test z progami punktowymi (zadania otwarte i zamknięte)	• Laboratorium
Stosuje wolne oprogramowanie, np. system Linux współpracujące z nim narzędzia. Przeciwdziała próbom łamania zabezpieczeń systemowych. Uzyskuje dostęp do danych (szyfrowanie NTFS) w przypadku awarii systemu Windows. Szyfruje dane. Odzyskuje dane z różnych nośników oraz dokonuje trwałego ich niszczenia. Uzyskuje (oraz blokuje) dostęp do komputera i danych z zastosowaniem systemów bootujących (CD, USB). Archiwizuje zaszyfrowane dane w chmurze. Tworzy obraz partycji systemowej oraz w przypadku awarii systemu wykonuje jego odzyskiwanie. Zabezpiecza sieć Wi-Fi oraz unika sytuacji, w których korzystanie z otwartych sieci jest ryzykowne	• K_U10 • K_U13	• Ocena jakości wykonania zadań praktycznych; Ocena prac – progi punktowe (jakość wykonania, zgodność z instrukcją)	• Laboratorium
Rozumie potrzebę poszanowania cudzej własności intelektualnej, prawa autorskiego i praw pokrewnych. Rozumie potrzebę dbałości o ochronę danych osobowych współpracowników i uczniów	• K_K05	• Ocena jakości wykonania zadań praktycznych; Ocena prac – progi punktowe (jakość wykonania, zgodność z instrukcją)	• Laboratorium

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. Flisak D., *Utwór multimedialny w prawie autorskim*, Warszawa 2008.
3. Hetman J., *Ustawa o prawie autorskim i prawach pokrewnych z przepisami wykonawczymi*, 2007.
4. Mozgawa M., Poźniak-Niedzielska M., Szczotka J., *Prawo autorskie i prawa pokrewne*, Bydgoszcz 2006.
5. http://staff.uz.zgora.pl/jjedrycz//elearning/bezpieczenstwo/pliki/index.html

Literatura uzupełniająca

1. Jędryczkowski J., *http://www.uz.zgora.pl/~jjedrycz/elearning/html/00bezp.htm*.
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. Szaradowski R., *Ochrona danych osobowych: komentarz do ustawy z dnia 29.08.1997*, Zielona Góra 2000.

Uwagi

Zmodyfikowane przez dr Jacek Jędryczkowski (ostatnia modyfikacja: 15-07-2016 18:30)