Bezpieczeństwo systemów informatycznych - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Bezpieczeństwo systemów informatycznych
Kod przedmiotu	11.3-WK-IiEP-BSI-L-S14_pNadGenNI2CA
Wydział	Wydział Matematyki, Informatyki i Ekonometrii
Kierunek	Computer science and econometrics
Profil	ogólnoakademicki
Rodzaj studiów	pierwszego stopnia z tyt. licencjata
Semestr rozpoczęcia	semestr zimowy 2019/2020

Informacje o przedmiocie

Semestr	6
Liczba punktów ECTS do zdobycia	5
Typ przedmiotu	obieralny
Język nauczania	polski
Sylabus opracował	• dr inż. Janusz Jabłoński

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	30	2	-	-	Zaliczenie na ocenę
Wykład	30	2	-	-	Egzamin

Cel przedmiotu

To acquaint the Students with selected elements of Information Security in the context of formal, legal and technical conditions of Cybersecurity

Wymagania wstępne

Information technology and computer protocols and networks.

Zakres tematyczny

lecture

1 .The basic informations about data safety and security and cybersecurity (2 hours)
2. The law about the protection of personal data other cybersecurity guidelinesand (2 hours)
3. Attributes and threats of IT systems: confidentiality, integrity, availability. (4 hours)
4. Models and classes of security for information systems. (2 hours)
5. Cryptography and crypto-analysis. (6 hours)
6. The telecommunications Law and the Digital Signature Act. (2 hours)
7. Authentication models and access control strategies. (2 hours)
8. Viruses, Trojans, Rotkits ... - methods of defense. (2 hours)
9. Increased security environments and utility services. (2 hours)
10. Local and network attacks - systems of attack detection and protection. (2 hours)
11. Introduction to defining security policy. (2 hours)
12. Security of BlockChain technology (2 hours)

Laboratory

1. Operating system - data protection functions. (2 hours.)
2. Configuring operating system user accounts. (2 hours.)
3. Advanced operating system services. (2 hours.)
4. Cryptographic tools in securing user data and accounts. (2 hours.).
5. ACL and VPN - configuring "remote work" tools and resource control. (4 hours).
6. Improving the efficiency of encryption and crypto-analysis methods - examples (4 hours)
7. "Buffer overflow" effects and countermeasures. (2 hours.)
8. Protection against "SQL Injection", "spoofing" and phishing. (2 hours.)
9. Counteracting "port scanning" and network activity control. (2 hours.)
10. Installation and configuration of anti-virus programs. (2 hours.).

11. Defining the security policy. (2 hours.)
12. Installing and using certificates - examples of use (2 hours)
13. Passive and active network security systems. (2 hours.)

Metody kształcenia

Lecture with the use of presentation techniques, laboratory exercises, presentations of students' studies, a talk.

Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
The student has general knowledge of the methods, techniques and tools used in counteracting threats to IT security and data protection.	• K_W14	• egzamin - ustny, opisowy, testowy i inne	• Wykład
The student is able to prepare a safe profile for the user of the computer system and can secure the computer workstation with an appropriate program	• K_U33	• aktywność w trakcie zajęć • konspekt • wykonanie sprawozdań laboratoryjnych	• Laboratorium
The student understands the importance of intellectual honesty in the activities of their own and others, and is aware of the need to comply with data protection law.	• K_K04 • K_K07	• bieżąca kontrola na zajęciach • kolokwium • wykonanie sprawozdań laboratoryjnych	• Laboratorium
Student umie dobrać narzędzia dla pracy zdalnej i skonfigurować bezpieczny kanał VPN.	• K_U21	• wykonanie sprawozdań laboratoryjnych	• Laboratorium
The student knows the basic legal conditions of protection and data security threats in information systems	• K_W02	• egzamin - ustny, opisowy, testowy i inne	• Wykład

Warunki zaliczenia

The final grade in the subject includes the laboratory grade (50%) and the exam grade (50%), assuming that the student has achieved all the assumed learning outcomes sufficiently. The condition for passing the course is obtaining a positive grade from the lecture and laboratory.

Literatura podstawowa

1. J. Pieprzyk, T. Hardjono, J. Seberry, Teoria bezpieczeństwa systemów komputerowych, Helion, Gliwice 2005.
2. Lukatsky, Wykrywanie włamań i aktywna ochrona danych, Helion, Gliwice 2004.
3. Białas, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa 2006.

Literatura uzupełniająca

1. E. Cole, R.L. Krutz, J. Conley, Bezpieczeństwo sieci, Helion, Gliwice 2005.
2. R. Anderson, Inżynieria zabezpieczeń, WNT Warszawa 2005
3. M. Sokół, R. Sokół, Internet. Jak surfować bezpiecznie, Helion Łódz 2005
4. D.E. Denning, Wojna informacyjna i bezpieczeństwo informacji, WNT Warszawa 2002

Uwagi

Zmodyfikowane przez dr Alina Szelecka (ostatnia modyfikacja: 21-11-2020 06:10)