Bezpieczeństwo systemów informatycznych - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Bezpieczeństwo systemów informatycznych
Kod przedmiotu	11.3-WK-MATP-BSI-W-S14_pNadGenVYT50
Wydział	Wydział Matematyki, Informatyki i Ekonometrii
Kierunek	Mathematics
Profil	ogólnoakademicki
Rodzaj studiów	pierwszego stopnia z tyt. licencjata
Semestr rozpoczęcia	semestr zimowy 2020/2021

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

Cel przedmiotu

The student be becomes introduced in problems of protection of data and the computer systems as well as method of solving these problems.

Wymagania wstępne

Computers system projecting and programming. Computer Nets.

Zakres tematyczny

Lecture

1. Legal conditioning of safety and security. (2h)
2. The acts about protection of data as well as the personal data protection. (2h)
3.The danger of computer systems: confidentiality, integrality accessibility. (4h)
4. The models and the class of safety for computer systems. (2h)
5. Cryptology as cryptography and crypt-analysis. (6h)
6. Telecommunicational law and act about digital signature. (2h)
7. The models of authenticating and the strategies of ACL. (2h)
8. Viruses, trojany, rotkity - the method of defence. (2h)
9. Environment about raised safety and tool services. (2h)
10. Incidents and attacks - the systems of detecting as well as the protection. (2h)
11. Defining the policy of safety. (2h)
12. The Public Key Infrastructure and the electronic signature. (2h)

Laboratory

1. The operating system - the functions in range of protection of data (2h)
2. Operating system and configuration the accounts of users (2h)
3. Advanced services of operating system (2h)
4. Cryptographical tools in protecting data and users accounts (2h)
5. ACL and VPN - the tools configuration to " the work remote" and the access control (2h)
6. Improvement of coding efficiency - the examples (2h)
7. "Buffer overflow" - results and counteraction (2h)
8. Protection before: "SQL Injection", "Phishing", ... (2h)
9. The "Port-knocking" counteraction as well as the control of activity in net (4h)
10. Antivirus - installation and the configuration (4h)
11. Defining the policy of safety (2h)
12 Certificates - the examples of installing and the use (2h)
13. Passive and active systems of network protections (2h)

Metody kształcenia

The lecture with multimedia presentations, talk, the students' studies, laboratory practice, discussion.

Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
Student knows basic conditioning the legal protections as well as the threat of safety of data in computer systems.		• aktywność w trakcie zajęć • egzamin - ustny, opisowy, testowy i inne • projekt • test	• Wykład • Laboratorium
Student is able prepare the safe profile for user of computer system as well as the computer system; protect the suitable programme.		• aktywność w trakcie zajęć • egzamin - ustny, opisowy, testowy i inne • projekt • test	• Wykład • Laboratorium
Student knows to choose tool for remote work and to configure the safe VPN channel; the meaning of intellectual property in own and different persons workings as well as know the warnings and the law for personal data protection.		• aktywność w trakcie zajęć • egzamin - ustny, opisowy, testowy i inne • projekt • test	• Wykład • Laboratorium
Student knows basic techniques and the tools used in counteraction the threats of computer safety and the data security.		• aktywność w trakcie zajęć • egzamin - ustny, opisowy, testowy i inne • projekt • test	• Wykład • Laboratorium

Warunki zaliczenia

Lecture: Written examination use to verifying the education outcome in area of knowledge and skills.
Laboratory: Final grade is granted based on receipt for: written tests, activity, completed project and documentation.
Final course grade consists of laboratory (50%) and examination (50%) by presumption, that student obtained all the founded effects of education in sufficient degree.

Literatura podstawowa

1. J. Pieprzyk, T. Hardjono, J. Seberry, Teoria bezpieczeństwa systemówomputerowych, Helion, Gliwice 2005.
2. A. Lukatsky, Wykrywanie włamań i aktywna ochrona danych, Helion, Gliwice 2004.
3. A. Białas, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa 2006.
4. W. Stallings, Computer Security: Principles and Practice, Prentice Hall; 2011

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: 18-09-2020 13:45)