ФАКУЛТЕТ ПО ИКОНОМИЧЕСКИ И СОЦИАЛНИ НАУКИ
КАТЕДРА „ПОЛИТИЧЕСКИ НАУКИ И НАЦИОНАЛНА СИГУРНОСТ“

Конспект за държавен изпит за придобиване на ОКС „Магистър” по КИБЕРСИГУРНОСТ

1. Ролята на открити източници в интернет за разследването на един киберинцидент.
2. Методи, средства и стъпки при изследването на дигиталните веществени доказателства”
3. Право на зачитане на личния живот и право на защита на личните данни. Основни принципи и правила, свързани с обработването на лични данни. Управление и защита на личните данни в Европейския съюз. Правна уредба на защитата на личните данни в Европейския съюз. Основни органи в областта на защитата на личните данни в Европейския съюз.
4. Политика за защита на личните данни в Република България. Правна уредба на защитата на личните данни в Република България. Основни органи в областта на защитата и управлението на личните данни.
5. Общи правила при обработване на лични данни. Особени случаи на обработване на лични данни. Права на субекта на лични данни. Администратор на лични данни и обработващ лични данни. Надзор за спазване на правилата за защита на личните данни. Средства за правна защита, отговорност за причинени вреди и санкции.
6. Системата за киберсигурност, важен елемент на Националната система за сигурност. Управление и организация на системата за Киберсигурност. Консултативни и координиращи органи.
7. Стратегическа и нормативна рамка на Системата за Киберсигурност. Видове Киберсигурност. Цели, принципи и обхват. Организация на взаимодействието между държавата, бизнеса и обществото
8. Защитни стени. Функционалност. Класификация. Планове на защитни стени.
9. Криптография. Цел. Видове криптиране. Механизми за автентикация.
10. Защита на информацията в мрежова среда. Защита от отказ и възстановяване. Мрежова сигурност. Външни и вътрешни заплахи. Мерки за сигурност. Основни принципи, гарантиращи сигурността на информацията.
11. Тунелиране на канален и мрежов слой от OSI. Виртуални частни мрежи (VPN) - принцип на работа. Класификация, надеждност и сигурност на VPN мрежите.
12. Екип за реагиране при инциденти. Security Operation Center - SOC
13. Заплахи за информационните системи (ИС). Видове заплахи. Уязвимост на информационните системи и злоупотреба. Информационна сигурност.
14. Мерки за защита на информационните системи. Управленски мерки за защита на класифицирана информация в ИС и компютърни мрежи. Организационни мерки. Програмно-технически мерки.
15. Какво представлява Социалното инженерство и какви са рисковете свързани с него. Видове социално инженерство. Видове технически атаки . Видове нетехнически атаки. Характеристики на техническите и един нетехнически методи на атака. Мерки за защита срещу Социално инженерство.
16. Малуери, видове и характеристика. Вируси, същност и начини на разпространение. Червеи, определение и начин на разпространение. Сравнителен анализ между Вирусите и Червеите. Троянския кон определение и начин на работа. Видове софтуери за защита има срещу Вируси, Червеи и Троянски коне. Мерки за защита срещу Малуери.

ФАКУЛТЕТ ПО ИКОНОМИЧЕСКИ И СОЦИАЛНИ НАУКИ
КАТЕДРА „ПОЛИТИЧЕСКИ НАУКИ И НАЦИОНАЛНА СИГУРНОСТ“

Литература:

1. Александър Цокев, Етично хакерство, БАРЗИКТ, 2017, ISBN: 978-619-7382-00-6
2. Бояджиев, Д. Основи на MikroTik RouterOS, Издателство „За буквите – О писменехъ“ ISBN 978-619-185-252-9, София, 2016
3. Д. Арнаудов, А. Крумова: Сигурност и защита на информационните системи, унив. изд. на ВСУ „Черноризец Храбър”, Варна, 2007.
4. Кевин Бийвър, Хакерство, Акекс-Софт, 2016, ISBN 9546562947
5. Стоицов, Г., Локални компютърни мрежи и примерни виртуални топологии, Университетско издателство „Паисий Хилендарски“, Пловдив, 2016, ISBN 978-619-202-127-6;
6. Стоицов, Г., Мрежово администриране, (Online, последно актуализирано 2020), http://kmk.fmi-plovdiv.org/lekcii.zip;
7. Стоицов, Г., Мрежова сигурност, (Online, последно актуализирано 2020), http://kmk.fmi-plovdiv.org/InfAndComSecurity.pdf
8. Ц. Семерджиев: Сигурност и защита на информацията, изд. „Класика и стил”, София, 2007.
9. Ц. Семерджиев: Информационна сигурност, изд. Софттрейд, София, 2004.
10. http://www.bds-bg.org/images/upload/Izdania/Brochures_OP_2013/Brochure_IT.pdf, 2017
11. https://cyberbg.eu/, 2017
12. http://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:32016R0679&from=EN, 2017
13. https://www.govcert.bg/BG/Documents/%D0%97%D0%90%D0%9A%D0%9E%D0%9D%20%D0%B7%D0%B0%20%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D1%81%D0%B8%D0%B3%D1%83%D1%80%D0%BD%D0%BE%D1%81%D1%82.pdf, 2020
14. https://www.mtitc.government.bg/sites/default/files/nar_minimalnite_iziskvaniq_mrejova_info_sigurnost-072019.pdf, 2020
15. https://www.researchgate.net/publication/340301223_Open_Source_Intelligence_OSINT_issues_and_trends
16. https://bird.tools/wp-content/uploads/2019/12/13082019_Osint-guide_v2fin.1.pdf
17. https://www.guru99.com/digital-forensics.html
18. https://www.researchgate.net/publication/300474145_Digital_Forensics

Конспектът е обсъден и приет на КС на катедра ПННС с протокол № 58/5.02.2021 г. и влиза в сила от държавна изпитна сесия м. юни, 2021 г.

Ръководител-катедра „ПННС“

доц. д-р Ал. Петров