КОНСПЕКТ
ЗА ДЪРЖАВЕН ИЗПИТ НА МАГИСТЪРСКА ПРОГРАМА КИБЕРСИГУРНОСТ

1. Структура и съдържание на системата за национална сигурност на Р България и на подсистемата й за киберсигурност.
2. Същностни характеристики, предимства и недостатъци на организационно-управленската структура и модел за противодействие на кибертероризма, както и на основните съвещателни и координиращи органи на подсистемата за киберсигурност.
3. Право на зачитане на личния живот и на защита на личните данни. Политика за защита на личните данни в Р България. Общи правила при обработване на личните данни.
4. Стандарт за управление сигурността на информацията ISO 27001: цел, структура, обхват.
5. Подход за управление на риска в киберсигурността съответствие с международни стандарти за сигурност.
6. Визия на Европейската екосистема за киберсигурност. Елементи необходими за изграждането на здравословна кибер екосистема.
7. Правни основи за противодействие на компютърните престъпления. Закон за кибер-сигурност, Закон за електронните съобщения, Конвенция за престъпленията в киберне-тичното пространство. Регл. 2019/881, Директива (ЕС) 2022/2555 на ЕП и на СЕ от 14.12. 2022 г., мерки за високо общо ниво на киберсигурност, за изм. на Регл. (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148, НМИМИС.
7. Видове компютърни престъпления. Обект, обективна страна, субект и субекти на на компютърните престъпления.
8. Оперативно-издирвателни служби ангажирани с противодействие на киберпрестъпността. Видове оперативно-издирвателни органи и линии на работа при разкриване и разследване на компютърни престъпления.
9. Социалното инженерство и рисковете свързани с него. Видове социално инженерство. Мерки за защита срещу социалното инженерство.
10. Системи за разкриване и превенция на проникване. (IPS/IDS). Специфики на работа и най-добри практики при тяхната употреба.

11. Криптография - синхронно и асинхронно криптиране. Хеширане. Подписване на информацията.

12. (D)DoS атаки. Видове атаки в зависимост от нивото на OSI модела, на които биват предприемани. Мрежови атаки. Атаки към услуги.

13. Защитни стени. Функционалност. Класификация. Планове на защитни стени.

14. 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.

15. Ролята на открити източници в интернет за разследването на киберинцидент.

16. Методи, средства и стъпки при изследването на дигиталните веществени доказателства.

17. Тунелиране на канален и мрежов слой в Базов референтен модел за взаимно свързване на отворени системи (OSI). Виртуални частни мрежи (VPN) - принцип на работа. Класификация, надеждност и сигурност на VPN мрежите.

18. Екип за реагиране при инциденти. Security Operation Center - SOC. План за реакция при инциденти.

19. Заплахи за информационните системи (ИС). Видове заплахи. Уязвимост на информационните системи и злоупотреба. Информационна сигурност.

20. Мерки за защита на информационните системи. Управленски мерки за защита на класифицирана информация в ИС и компютърни мрежи. Организационни мерки. Програмно-технически мерки.

21. Малуери, видове и характеристика. „Вирус“, същност и начини на разпространение. „Червей“, определение и начин на разпространение. Сравнителен анализ между Вируси“ и „Червеи. „Троянски кон „определение и начин на работа. Видове софтуери за защита срещу Вируси, Червеи и Троянски коне. Мерки за защита срещу Малуери.

22. План за реагиране при киберинциденти. Структура, целите и стъпките в процеса на реагиране при инциденти. Роля и отговорности на екипа за реакция.

23. Роля и значение на информацията при защитата на националната сигурност. Възможности за създаване и съхраняване на трафични данни в съобщителните системи. Използване и контрол на трафичните данни от структурите за сигурност. Основни трафични данни в стационарните и мобилните съобщителни системи.

24. Анализиране и изследване организационната среда, процесите, явленията и събитията влияещи на системата за защита на кибератките. Намиране и прилагане благоприятните възможности за повишаване степента на защита на кибератките.

25. Проектиране и изграждане на корпоративна система за управление на риска за киберактивите. Приложими управленски функции, принципи и подходи в процеса на управление на риска за киберактивите.

26. Мероприятия за установяване на принадлежността и местоположението на IP адрес, принадлежност на име на домейн, принадлежност на адрес на електронната поща. Уникалност на IP адреса. Регистратори. Установяване на принадлежност на IP адреси чрез whois клиент. Установяване на принадлежност на IP адреси чрез Уеб форма.

27. Тактика на обиска при компютърни престъпления. Стандарти при обиска. Обекти, които съдържат улики, доказателства. Методи за скриване на такива данни. Лог-файлът като доказателство. Коректност при изземването на лог-файл. Принципи и общи правила за изземване на компютърна техника при обиск.

Основна литература:

1. Цокев, Ал. Етично хакерство, София, Баркзит, 2017.
2. Бояджиев, Д. Основи на MikroTik RouterOS, изд. „За буквите“. София, 2016.
3. Демирев, В. Основи на киберсигурността. София, 2022.
4. Калчев, К., Цветков , К.Кибирсигурност.София, 2022.
5. Каракънева, Ю.Киберсигурност. София, 2013.
6. Минчев, З. Анализ на киберзаплахите в интернет социални мрежи. С., 2012
7. Петров, Р. Основи на етичното хакерство 1 и 2 част. С., 2016
8. Кевин Бийвър, Хакерство, Акекс-Софт, София, 2016.
9. Стоицов, Г., Локални компютърни мрежи и примерни виртуални топологии, Университетско издателство „Паисий Хилендарски“, Пловдив, 2016, ISBN 978619-202-127-6.
10. Стоицов, Г., Мрежово администриране, (Online, последно актуализирано 2020), http://kmk.fmi-plovdiv.org/lekcii.zip.
11. Стоицов, Г., Мрежова сигурност, (Online, последно актуализирано 2020), http://kmk.fmi-plovdiv.org/InfAndComSecurity.pdf.
12. Ц. Семерджиев: Сигурност и защита на информацията, София, 2007.
13. Д. Арнаудов, А. Крумова: Сигурност и защита на информационните системи, изд. на ВСУ „Черноризец Храбър”, Варна, 2007.
14.С. Станев, С. Железов: Компютърна и мрежова сигурност, унив. изд. „Епископ Константин Преславски”, Шумен, 2005.
15.Methods with Forensic Analysis. 2016.
16.Kevin Mandia. Incident Response & Computer Forensics, 3rd Edition. 2014.

Нормативни актове и концептуални документи:

1.Директива (ЕС) 2022/2555 на ЕП и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изм. на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148

1. Национална стратегия за киберсигурност“Киберустойчива България 2020“, Реш. МС от 2016.
2. Закон за киберсигурност, първо Обн. ДВ. бр.94 от 13 Ноември 2018г., спосл. изм. и доп. изм.
3. Закон за електронните съобщения, първо Обн. ДВ. бр.41 от 22 Май 2007г. с посл. изм. и доп.
4. Наредба за минималните изисквания мрежова и информационна сигурност. Приета с ПМС № 186 от 26.07.2019 г., обн., ДВ, бр. 59 от 26.07.2019 г.

Допълнителни източници:

1. http://www.bds-bg.org/images/upload/Izdania/Brochures_OP_2013/Brochure_IT.pdf, 2017.
2. https://cyberbg.eu/, 2017
3. http://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:32016R0679&from=EN
4. 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
5. https://www.mtitc.government.bg/sites/default/files/nar_minimalnite_iziskvaniq_mrejova_info_sigurnost-072019.pdf, 2020
6. https://www.researchgate.net/publication/340301223_Open_Source_Intelligence_OSINT_issues_and_trends
7. https://bird.tools/wp-content/uploads/2019/12/13082019_Osint-guide_v2fin.1.pdf
8. https://www.guru99.com/digital-forensics.html
9. https://www.researchgate.net/publication/300474145_Digital_Forensics
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

Държавният изпит включва два компонента: писмен отговор на един въпрос от конспекта и тест с въпроси, съдържащи по един верен отговор. Студентите трябва да имат положителна оценка (минимум среден 3) на двата компонента. Крайната оценка е средно аритметичната от оценките на двата компонента.

Конспектът е приет с решение на КС на катедра „Политически науки и национална сигурност“ (протокол №121/12.03.2025 г.) и утвърден от ФС на Факултета по икономически и социални науки (протокол № 200/21.03.2025 г.).

Пловдив
21.03.2025 г.