



ВОЕННА АКАДЕМИЯ „ГЕОРГИ СТОЙКОВ РАКОВСКИ”

1504, София, бул. „Евлоги и Христо Георгиеви” № 82

УТВЪРЖДАВАМ:

ЗАМЕСТНИК-НАЧАЛНИК ПО УЧЕБНАТА И НАУЧНАТА ЧАСТ
НА ВА „Г. С. РАКОВСКИ”

ПОЛКОВНИК ДОЦ. Д.Н.

ПЕТЪР МАРИНОВ

___.___.2026 г.

ПРОГРАМА

**ЗА ПРОВЕЖДАНЕ НА ДЪРЖАВЕН ИЗПИТ СЪС СТУДЕНТИТЕ,
ОБУЧАВАЩИ СЕ ЗА ПРИДОБИВАНЕ НА ОКС „БАКАЛАВЪР“,
СПЕЦИАЛНОСТ „КИБЕРСИГУРНОСТ“
ВЪВ ВОЕННА АКАДЕМИЯ „ГЕОРГИ СТОЙКОВ РАКОВСКИ“
ЗА УЧЕБНАТА 2025/2026 г.**

**гр. София
2026 г.**

ЧАСТ I

ОБЩИ МЕТОДИЧЕСКИ УКАЗАНИЯ

1. Държавният изпит се провежда съгласно чл. 45, ал.1 от Закона за висшето образование в Република България, чл. 81, ал. 1, чл. 85 и чл. 90 от Правилника за учебната дейност на ВА „Г. С. Раковски” и Процедура по качество ПК - 08.03.15 „Ред за допускане и провеждане на държавен изпит със студенти, обучаващи се за придобиване на ОКС „бакалавър“ във Военна академия „Г. С. Раковски”.

2. Държавният изпит за придобиване на ОКС „бакалавър“ се провежда в две части - писмен и устен изпит по въпросник, включващ въпроси от задължителни учебни дисциплини от учебния план за специалността.

3. Писменият държавен изпит се провежда по въпроси от част II на настоящата програма, изтеглени от представител на студентите, намиращи се в залата, по които пишат всички явяващи се. Включва 2 (два) изпитни въпроса от въпросника – по един въпрос от всеки раздел, като общият брой на въпросите е 42 (четиридесет и два). Времето за писмения изпит е 4 (четири) астрономически часа.

4. До устен държавен изпит се допуска студент, получил не по-ниска оценка от среден (3,00) на писмения държавен изпит.

5. На устен държавен изпит всеки студент изтегля сам 2 (два) въпроса от въпросника, по един от всеки раздел, без тези, изтеглени на писмения изпит. В рамките на определеното му време от председателя на комисията се подготвя за устно изложение по тях и докладва пред държавната комисия в определената последователност по същите.

6. За успешно положен държавен изпит се смята изпитът с получена положителна оценка на всеки един от изпитите (писмен и устен).

7. Крайната оценка от държавния изпит на студентите, обучаващи се за придобиване на ОКС „Бакалавър“ по специалността „Киберсигурност“ се формира като средноаритметична от писмения и от устния изпит с точност до 0,50. Оценката е по шестобалната система, която включва: „Отличен“ (5,50 или 6,00), „Много добър“ (4,50 или 5,00), „Добър“ (3,50 или 4,00), „Среден“ (3,00) и „Слаб“ (2,00). За положителна оценка се приема оценка не по-ниска от „Среден“ (3,00).

ЧАСТ II
ИЗПИТНИ ВЪПРОСИ ЗА ПРОВЕЖДАНЕ НА ДЪРЖАВЕН ИЗПИТ СЪС
СТУДЕНТИТЕ, ОБУЧАВАЩИ СЕ ЗА ПРИДОБИВАНЕ НА ОКС
„БАКАЛАВЪР“, СПЕЦИАЛНОСТ „КИБЕРСИГУРНОСТ“

РАЗДЕЛ 1

1. Обща информационна среда в НАТО. Процес на избор на продукти за NCOE.
2. Функционално конфигуриране на общата информационната среда на системите в НАТО.
3. Техническо конфигуриране на информационната инфраструктура на системите в НАТО.
4. Софтуерно конфигуриране на информационната инфраструктура на системите в НАТО.
5. Вземане на решение в условия на неопределеност.
6. Наблюдение и управление на компютърните мрежи. Функции, задачи, принципи.
7. Концепция за управление на мрежовите възли. Архитектури OSI и TCP.
8. Основни аспекти на киберсигурността.
9. Уязвимости в информационните системи.
10. Заплахи и направления за несанкциониран достъп до ресурси на ИС.
11. Стандарти за информационна и киберсигурност.
12. Киберсигурността, като част от системите за управление.
13. Предоставяне на услуги за електронно управление.
14. Акредитация и одит на КИС.
15. Политика за защита на личните данни.
16. Роля, място, функции и задачи на КИС на въоръжените сили.
17. Организация на КИС във въоръжените сили - структура и състав.
18. Комуникационни мрежи и информационните системи във въоръжените сили.

19. Системи C4I (за командване, управление, комуникации, компютризация и разузнаване) във въоръжените сили.
20. Сигурността - същност, смисъл и съдържание.
21. Система за национална сигурност – понятие, структура и управление.

РАЗДЕЛ 2

22. Роля на компютърните мрежи в съвременния свят. Терминология, топологии и характеристики. Локални (LAN), глобални мрежи (WAN) и Интернет. Мрежата като платформа и тенденции за развитие.
23. Протоколи и модели за мрежова работа. Сравнителен анализ на седем-слоен OSI модел на Международната организация по стандартизация и 4 слоен TCP/IP модел.
24. Основи на Ethernet LANs. Ниво 2 от седем-слойния OSI модел - основни понятия. Ethernet технологии. 10, 100 Mbps, Gigabit и 10 Gigabit Ethernet. Формат на Ethernet рамката (фрейма). Работа на мрежовите комутатори (суичове). Таблица с MAC адреси. Протокол за намиране на MAC адреса на получателя по известен негов IPv4 адрес (ARP protocol).
25. IPv4 адреси. Класове IPv4 адреси. Публични и частни IPv4 адреси. Разделяне на IPv4 мрежи на подмрежи.
26. Мрежови концепции и архитектури.
27. Информационни системи и технологии – същност, класификации, характеристики и приложение.
28. Операционни системи. Функции, видове, характеристики, възможности и инструментални средства.
29. Създаване и обработване на свързани (хипертекстови) документи.
30. Процес на интегриране и средства за постигане на съвместимост на мрежите.
31. Определения и структура на модела OSI. Функционални слоеве на OSI модела и взаимодействие между тях.

32. Видове комутация в мрежите. Услуги в комуникационните мрежи.
33. Протоколи, съпътстващи протокола IP – предназначение, формати на съобщенията. Маршрутизиращи протоколи в IP мрежа.
34. Функции, задачи и възможности на OpenView – NNM.
35. Въведение в киберсигурността. Център за наблюдение и управление на киберсигурността.
36. Принципи за осигуряване на мрежовата сигурност. Анализ на атаките към мрежите.
37. Защита на мрежите. Водене на журнал за мрежовата активност и четене на журнала.
38. Защита и анализ на крайните устройства.
39. Въведение в теорията на защитените системи - криптосистеми.
40. Архитектура на криптосистема.
41. Ефективност на криптосистема.
42. Устойчиво криптиране.

ЧАСТ III

ЛИТЕРАТУРА

Задължителна литература:

1. Учебник “Организация и управление на комуникационно-Информационните системи в операциите, раздел 2.1.2.2. Информационен модел на процеса за вземане на решение за изграждане на КИС, стр. 89-98.
2. Учебник “Наблюдение и управление на мрежи“ – стр.7-18, 23-29, 54-59.
3. Учебник “Компютърни мрежи и комуникации”, стр. 5-8, 21-25, 34-40, 65-67.
4. Лекционен курс „CyberOps Associate”, Теми:1, 2, 13, 14, 22, 25.
5. Лекционен курс „Съвместимост на КИС”, Теми: 2, 3, 7.
6. Демиров П., Е. Енев, В. Александрова, Командване, управление и служба на щабовете, част първа Автоматизирани системи за командване и управление и мениджмънт на информацията, София, изд. "Авангард Прима", 2019, ISBN 978-619-239-213-0, 343 стр. (т. 7.7.1 и 7.7.2 стр. 252-272).
7. Александрова В., Съвременни технологии използвани в автоматизираните информационни системи в областта на сигурността и отбраната, учебник, Военна академия “Георги Стойков Раковски”, 2011г., стр. 207.
8. Калчев К., Учебно пособие (лекционен курс) „Теоретични основи на защитата на комуникационните и информационните системи“ – стр. 1-3, 4-9, 10-12, 20-27.
9. Доктрина за комуникационно-информационната система на въоръжените сили НП-06, 2022 (стр. 22 (2.7. Роля и място на КИС в СКУ); стр. 11-15, 45-47).
10. Калчев К., Организация и управление на комуникационно информационните системи в операциите, Учебник, ВА „Г. С. Раковски”, 2010 г. (стр. 105- 109, (2.2. Изисквания и ефективност на КИС)).
11. Лекционен курс „Основи на киберсигурността – I-ва и II-ра част“, Теми:8, 9, 10, 11, 12, 13, 14, 15.

Препоръчителна литература:

1. Наредба за минималните изисквания за мрежова и информационна сигурност. ПМС № 186 от 26.07.2019 г., обн., ДВ, бр. 59 от 26.07.2019 г.
2. Закон за защита на класифицираната информация, Обн. ДВ. бр.45 от 30 Април 2002 г., изм. ДВ. бр.17 от 26 Февруари 2019 г.
3. Серия стандарти БДС ISO/IEC 27000:2010 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Общ преглед и речник.
4. БДС ISO/IEC 27001:2006 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията
5. Димов, П., Иванов, Е. Фалшивите новини. Разпознаване на фалшивите новини и дезинформацията в съвременната хибридна среда за сигурност, 2020, Военна академия „Г. С. Раковски“ ISBN 978-619-7478-39-6.
6. Димов, П., SEO-оптимизация на сайтове за търсещи машини, 2019, Диомира, ISBN: 978-954-2977-56-8.

7. Регламент (ЕС) 2016/679 на Европейския парламент от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (GDPR).
8. Правилник за прилагане на закона за защита на класифицираната информация в сила от 10.12.2002 г. Приет с ПМС № 276 от 02.12.2002 г. Обн. ДВ. бр.115 от 10 Декември 2002г., изм. ДВ. бр.22 от 11 Март 2003г., изм. и доп., бр. 68 от 22.08.2017 г.
9. Серия стандарти NIST SP:800.
10. Колектив ВА., Система за разузнаване, София, издателство ВА, 2023 г., учебно помагало.
11. Закон за ДАР, София, 2015 г.

НАЧАЛНИК НА КАТЕДРА „КИС“:

ПОЛК. ДОЦ. Д-Р

ИВАН ЧАКЪРОВ

___.__.2026 г.

Програмата за провеждане на държавен изпит със студентите, обучаващи се за придобиване на ОКС „бакалавър“, специалност „Киберсигурност“ във Военна академия „Георги Стойков Раковски“ за учебната 2025/2026 г. е обсъдена и приета на заседание на катедрения съвет на катедра „Комуникационни и информационни системи“ с протокол № 2/10.02.2026г., на факултетния съвет на факултет „Командно-щабен“ с протокол № 52/17.02.2026г., и на Академичен съвет на Военна академия „Г. С. Раковски“ с протокол № 2/24.02.2026г.

СЪГЛАСУВАНО:

ДЕКАН НА ФАКУЛТЕТ „КОМАНДНО-ЩАБЕН“

ПОЛКОВНИК ПРОФ. Д-Р

ЕМИЛ ЕНЕВ

__.__.2026 г.

ДЕКАН НА ФАКУЛТЕТ „НАЦИОНАЛНА СИГУРНОСТ И ОТБРАНА

ПОЛКОВНИК ДОЦ. Д-Р

ЖИВКО ЖЕЛЕВ

__.__.2026 г.