Київський університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

ПРОГРАМА ЕКЗАМЕНУ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВЕДЕННЯ КІБЕРДІЙ І КІБЕРКОНФЛІКТІВ»

Змістові модулі:

«Тенденції розвитку і застосування методів і засобів захисту інформації на об’єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів»
«Проблеми захисту державної інформаційної сфери від стороннього кібернетичного впливу»
«Технології та інструменти забезпечення безпеки інформації на об’єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів»
«Технології адміністрування та експлуатації об’єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів»

для аспірантів

спеціальності 125 Кібербезпека
освітнього рівня третього (освітньо-наукового)
освітньо-наукової програми “Інформаційна безпека держави”

Київ 2022

Форма опису програми екзамену

Поля форми	Опис поля форми
Екзамен складається з тестування. Тести охоплюють всі теми навчальної дисципліни. Тести розміщено в рубриці «Екзамен» ЕНК «Забезпечення безпеки об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів» (3 курс, АСП, денна, заочна).	
Рік навчання	3
Спеціальність	125 Кібербезпека
Форма проведення: письмова/усна, комбінована	Письмова (електронне тестування)
Тривалість проведення	1 год. 20 хвилин
Максимальна кількість балів	40
Критерії оцінювання	Кожна правильна відповідь на 40 тестових питань по 1 балу
Перелік допоміжних матеріалів	Персональний комп’ютер або смартфон або інший електронний пристрій та доступ до мережі Інтернет
Орієнтовний перелік питань	1. Тенденції розвитку методів і засобів ведення кібердій і кіберконфліктів 2. Застосування методів і засобів захисту інформації на об’єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів 3. Основні методології проектування систем захисту інформації на об’єктах критичної інфраструктури 4. Проблеми захисту державної інформаційної сфери від стороннього кібернетичного впливу 5. Забезпечення інформаційної безпеки державної інформаційної сфери від стороннього кібернетичного впливу 6. Алгоритми, моделі, методи оцінки характеристик і стану систем інформаційної та кібербезпеки державної інформаційної сфери 7. Технології забезпечення безпеки інформації в системах і мережах 8. Технологічна модель безпеки інформації на об’єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів

	9. Концепція захисту інформації, організації й забезпечення інформаційної та кібербезпеки ОІД 10. Адміністрування процесів введення в експлуатацію захищених ІТ систем і мереж 11. Адміністрування процесів експлуатації захищених ІТ систем і мереж 12. Удосконалення систем, засобів і технологій забезпечення безпеки ІТ систем та мереж 13. Завдання своєчасного виявлення інцидентів інформаційної безпеки 14. Перспективні напрямки державної політики у галузі кібернетичної безпеки 15. Встановлення повноважень і прав суб'єктів щодо об'єктів 16. Моделювання стратегій захисту інформації від стороннього кібернетичного впливу 17. Завдання та функції суб'єктів державної інформаційної інфраструктури 18. Основні суб'єкти державної інформаційної інфраструктури 19. Методи контролю доступу 20. Профіль безпеки стандарту ISO/IEC 15408 21. Тенденції розвитку і застосування методів і засобів захисту інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів. 22. Тенденції розвитку методів і засобів захисту інформації. 23. Тенденції побудови архітектури безпеки інформації. Захист інформації в корпоративних мережах. 24. Основи і мета політики безпеки в корпоративних мережах. 25. Принципи та методи надання доступу до інформаційних ресурсів. 26. Принципи забезпечення доступу до інформаційних ресурсів. 27. Методи ідентифікації і аутентифікації користувачів. 28. Технологічна модель забезпечення безпеки інформації на об'єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів. 29. Технології захисту інформації в системах інформаційної та/або кібербезпеки.

	30. Концепція захисту інформації, організації й забезпечення інформаційної та кібербезпеки ОІД. 31. Адміністрування процесів введення в експлуатацію та експлуатації об’єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів. 32. Перевірка і підтримка цілісності даних на об’єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів. 33. Розмежування прав доступу та правила забезпечення безпеки даних на об’єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів 34. Удосконалення, модернізація та уніфікація систем, засобів і технологій забезпечення безпеки на об’єктах критичної інфраструктури в умовах ведення кібердій і кіберконфліктів. 35. Задачі централізованого і децентралізованого адміністрування доступом до ІР і процесів в ІКС та реалізовувати заходи з протидії отриманню несанкціонованого доступу до них 36. Проведення аудиту безпеки ІКС, а також науковими методами та практичними навичками щодо створення систем моніторингу безпеки в ГГ системах та мережах. 37. Неструктуровані, структуровані, гібридні і ієрархічні протоколи P2P. Типи атак. Напади та їх пом’якшення. 38. Стилі координації систем. 39. Надійне та безпечне групове спілкування. Координаційні властивості. 40. Схема керування та координації реплікації: основа пом'якшення атак.
Екзаменатор: *Аносов Андрій Олександрович*, кандидат військових наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики.	