КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
ім. професора Володимира Бурячка

ПРОГРАМА ЕКЗАМЕНУ

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

для здобувачів третього (освітньо-наукового) рівня вищої освіти

спеціальності F5 Кібербезпека та захист інформації

освітньо рівня третього (освітньо-наукового)

освітньо-наукової програми «Інформаційна безпека держави»

Київ - 2025

Опис програми іспиту

Київський столичний університет імені Бориса Грінченка

Кафедра інформаційної та кібернетичної безпеки ім. професора Володимира Бурячка

Програма екзамену з дисципліни «Забезпечення безпеки об'єктів критичної інфраструктури в умовах ведення кібердій і кіберконфліктів»

1 рік навчання – освітній рівень - третій (освітньо-науковий)

Спеціальність F5 Кібербезпека та захист інформації

Освітньо-наукової програми «Інформаційна безпека держави»

Форма проведення: тестування на платформі Moodle в ЕНК дисципліни: https://elearning.kubg.edu.ua/course/view.php?id=23030

Тривалість проведення **1 год. 20 хв.**

Максимальна кількість балів: **40 балів**

Екзамен проводиться в університетській аудиторії у тестовій формі із використанням персональних комп'ютерів, якщо ситуація дозволяє проведення освітнього процесу офлайн. Якщо ж освітній процес проходить дистанційно, то екзамен проводиться онлайн в режимі відеоконференції засобами Google Meet та індивідуальної конференції засобами TeamViewer+ Viber.

Студент дає відповіді на запитання та завдання білету. Білет містить 2 теоретичних питання та 1 практичне завдання. Екзамен оцінюється у 40 балів за розподілом: 20 балів – теоретичний тест з дисципліни; 20 балів – виконання практико-орієнтованого завдання. Відповіді на питання та порядок розв'язання практичного завдання студент має надати особисто, засобами TeamViewer+ Viber, ці завдання передбачають ручну перевірку викладачем.

Критерії оцінювання теоретичних питань:

10 балів: Відмінний рівень знань, відповідь повна, вичерпна й достатньо обґрунтована

9 балів: Відмінний рівень знань, відповідь повна, вичерпна й достатньо обґрунтована з, можливими, незначними недоліками

8 балів: Добрий рівень знань, відповідь містить недоліки та / або незначну кількість помилок

7 балів: Посередній рівень знань, відповідь містить багато недоліків та незначну кількість помилок

6 балів: Мінімально допустимий рівень знань, що характеризується недостатньою обґрунтованістю, фрагментарністю; відповідь неповна, містить недоліки та помилки

5 балів: Низький рівень знань понять і фактів, без належного їх розуміння, що характеризується недостатньою обґрунтованістю; відповідь неповна, містить недоліки та помилки

4 бали: Незадовільний рівень знань, що виявляється у формальному запам'ятанні деяких понять і фактів, без належного їх розуміння, нездатності застосувати такі знання при розв'язанні задач.

0-3 бал: Незадовільний рівень знань, що виявляється у неспроможності відтворити означення понять та формулювання теорем, невмінні розв'язувати задачі.

0 балів: Відповідь відсутня.

Критерії оцінювання практичного завдання (задачі):

20-17 балів: Відмінний рівень умінь, розв'язання задачі повне, вичерпне володіння програмним забезпеченням, можливими, незначними недоліками

16-13 балів: Добрий рівень умінь, розв'язання задачі містить небагато недоліків та / або незначну кількість помилок

12-9 балів: Мінімально допустимий рівень умінь, що характеризується недостатнім рівнем володіння програмним забезпеченням, розв'язання задачі неповне, містить недоліки та помилки

8-5 бали: Незадовільний рівень умінь, що виявляється у нездатності застосувати знання при розв'язанні задач.

4-1 бал: Незадовільний рівень умінь, що виявляється у неспроможності володіння програмним забезпеченням, невмінні розв'язувати задачі.

0 балів: Відповідь відсутня.

Екзамен проводиться із суворим дотриманням принципів академічної доброчесності, що передбачає недопустимість списування, фальсифікацій та обману. При порушенні студент відсторонюється від подальшого проходження екзаменаційного тесту із підсумковою оцінкою Fx за дисципліну. При виконанні завдань допускається користування довідковою літературою, таблицями значень функції, критеріїв та ін.

Підсумкова оцінка в балах (максимально 100 балів) за дисципліну є сумою результату поточного контролю за семестр (60 балів) та відповіді на екзамені (40 балів).

Перелік тем, які виносяться на іспит:

1. Передумови розвитку методів і засобів ведення кібердій і кіберконфліктів.
2. Особливості кібероборони.
3. Основні характеристики кіберзагроз.
4. Упорядкування можливих кіберзагроз за певними класифікаційними ознаками.
5. Обов'язкові ознаки будь-якої кіберзагрози.
6. Кібердії, як специфічний вид протиборства.
7. Класифікація форм і способів кібердій.
8. Засоби і способи кіберрозвідки.
9. Засоби OSINT-розвідки.
10. Засоби аналізу та подолання систем захисту.
11. Засоби добування розвідувальної інформації та ведення віддалених атак.
12. Спеціалізовані програмні засоби відключення систем захисту.
13. Засоби і способи кіберзахисту.
14. Основні групи апаратно-програмного захисту у кіберпросторі.
15. Організаційні заходи захисту у кіберпросторі.
16. Передумови виникнення загроз для державної інформаційної сфери від стороннього кібернетичного впливу..
17. Проблеми захисту державної інформаційної сфери від стороннього кібернетичного впливу.
18. Глобальний (транскордонний) характер кіберзагроз.
19. Основні форми і способи стороннього кібернетичного впливу на державну інформаційну сферу.
20. Напрями забезпечення кібербезпеки України.
21. Національна система кібербезпеки як сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру.
22. Моделі забезпечення безпеки інформації в системах і мережах державної інформаційної сфери.

23. Стандарт ISO 7498-2 Security Architecture для забезпечення безпеки розподілених систем.
24. Механізми керування послугами безпеки в системах і мережах державної інформаційної сфери.
25. Порядок оцінювання кіберзагроз національним інтересам та національній безпеці в інформаційній сфері.
26. Формування політики безпеки інформації об’єктах критичної інфраструктури.

Приклад екзаменаційного завдання *(задачі)*

1. Проблеми захисту державної інформаційної сфери від стороннього кібернетичного впливу.
2. Механізми керування послугами безпеки в системах і мережах державної інформаційної сфери.

Практичне питання

1. Визначити сукупність функціональних послуг захисту інформації для обраного функціонального профілю захисту інформації на об’єкті критичної інфраструктури.

Екзаменатор:

Аносов А.О., кандидат військових наук, доцент кафедри інформаційної та кібернетичної безпеки ім. професора Володимира Бурячка Факультету інформаційних технологій та математики