

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

Затверджено на засіданні кафедри
інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
(протокол № 5 від 03.04.24)

РОБОЧА ПРОГРАМА ІСПИТУ

ПРИКЛАДНІ АСПЕКТИ ПОБУДОВИ КТЗІ

галузь знань	12 Інформаційні технології
спеціальність	125 Кібербезпека
освітня програма	125.00.01 Безпека інформаційних і комунікаційних систем

2023-2024 навчальний рік

Опис програми іспиту

Київський столичний університет імені Бориса Грінченка	
Кафедра інформаційної та кібернетичної безпеки імені професора Володимира Бурячка	
Програма іспиту з дисципліни «Прикладні аспекти побудови КТЗІ»	
2 курс – освітній рівень – перший (бакалаврський)	
Спеціальність 125 Кібербезпека	
Освітня програма: 125.00.01 Безпека інформаційних і комунікаційних систем	
Форма проведення: на платформі Moodle в ЕНК дисципліни: https://elearning.kubg.edu.ua/course/view.php?id=21815	
Тривалість проведення	1 год. 20 хв.
Максимальна кількість балів:	40 балів
<p>Екзамен проводиться в університетській аудиторії у комбінованій формі із використанням персональних комп'ютерів, якщо ситуація дозволяє проведення освітнього процесу у традиційній формі. Якщо освітній процес проходить дистанційно, то екзамен проводиться в режимі відеоконференції засобами Google Meet.</p> <p>Екзамен оцінюється у 40 балів за розподілом: 20 балів – письмова відповідь; 20 балів – захист проекту згідно обраної теми.</p> <p>Студент дає письмову відповіді на три теоретичні питання. Перевірка у ручному режимі.</p> <p>При дистанційному проведенні екзамену студент повинен розмістити відповідь на білет окремим файлом в системі Moodle; ці завдання передбачають ручну перевірку викладачем.</p> <p>Критерії оцінювання завдань відкритого типу (задач):</p> <p>10 балів: Відмінний рівень знань (умінь), відповідь повна, вичерпна й достатньо обґрунтована, правильні відповіді на додаткові питання;</p> <p>9 балів: Відмінний рівень знань (умінь), відповідь повна, вичерпна й достатньо обґрунтована з, можливими, незначними недоліками;</p> <p>8 балів: Високий рівень знань (умінь), відповідь повна, достатньо обґрунтована з, можливими, незначними недоліками або помилками;</p> <p>7 балів: Достатній рівень знань (умінь), але відповідь містить недоліки та / або незначну кількість помилок у розрахунках;</p> <p>6 балів: Достатній рівень знань (умінь), але відповідь містить недоліки у тлумаченні фізичної суті величин та інформаційних процесів або законів та / або незначну кількість помилок у розрахунках;</p> <p>5 балів: Посередній рівень знань (умінь), відповідь містить багато недоліків у тлумаченні фізичної суті величин та інформаційних процесів або законів та / або значну кількість помилок у розрахунках і визначенні мірності величин;</p> <p>4 бали: Посередній рівень знань (умінь), відповідь не повна, містить багато недоліків та / або значну кількість помилок;</p>	

- 3 бали: Мінімально допустимий рівень знань (умінь), що характеризується недостатньою обґрунтованістю, фрагментарністю; відповідь неповна, містить значну кількість недоліків та помилок;
- 2 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;
- 1 бал: Незадовільний рівень знань (умінь), що виявляється у неспроможності відтворити означення понять та формулювання фізичних законів, 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 екзамену із підсумковою оцінкою Fx за дисципліну.

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 питань, які виносяться на іспит:

1. Загальна класифікація видів інформації, що може бути об'єктом злочинних посягань.
2. Надати визначення терміну «Технічний канал витоку інформації».
3. Класифікація технічних каналів витоку інформації.
4. Що собою представляють візуально-оптичні канали витоку інформації?
5. Класифікація способів прихованого відео спостереження та зйомки.
6. Надати визначення терміну «Захист інформації від витоку по візуально-оптичному каналу».
7. Рекомендації щодо захисту інформації від витоку по візуально-оптичному каналу.
8. Комбіновані методи та засоби зняття акустичної інформації.
9. Методи та засоби зняття акустичної інформації з будівельних конструкцій.
10. Методи та засоби зняття акустичної інформації з засобів та ліній зв'язку.
11. Види радіомікрофонів для зняття акустичної інформації.
12. Методи та засоби захисту інформації від витоку акустичними каналами.
13. Пасивні методи захисту акустичної (мовної) інформації.
14. Активні методи захисту акустичної (мовної) інформації.
15. Основні вимоги та рекомендації щодо захисту мовної інформації, яка циркулює в приміщенні.
16. Класифікація електромагнітних каналів витоку інформації.
17. Методи та засоби зняття електромагнітної та електронної інформації.
18. Пасивні методи захисту електромагнітної інформації.
19. Активні методи захисту електромагнітної інформації.

- 20.Захист інформації в телекомунікаційних системах за рахунок структурної скритності сигналів.
- 21.Захист інформації в телекомунікаційних системах за рахунок інформаційної скритності.
- 22.Що собою представляють матеріально-речові канали витоку інформації?
- 23.Методи та засоби захисту інформації від витоку матеріально-речовими каналами.
- 24.В яких випадках передбачається створення комплексу ТЗІ на ОІД?
- 25.Основні етапи створення комплексу ТЗІ на ОІД.
- 26.Які об'єкти підлягають обов'язковому категоріюванню?
- 27.Які види категоріювання ОІД ви знаєте?
- 28.Порядок категоріювання об'єктів.
- 29.Мета обстеження ОІД.
- 30.Що аналізується під час проведення обстеження на ОІД?
- 31.Послідовність проведення робіт з обстеження на ОІД.
- 32.Зміст технічного завдання на виконання робіт зі створення комплексу технічного захисту інформації на ОІД.
- 33.Склад «Програми і методики випробувань» КТЗІ.
- 34.Форма та зміст Акту атестацій комплексу ТЗІ.
- 35.Структура паспорта на комплекс ТЗІ.

Екзаменатор



Валерій КОЗАЧОК

Завідувач кафедри



Павло СКЛАДАННИЙ