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

ПРОГРАМНІ КОМПЛЕКСИ ЗАХИСТУ АС ВІД НСД

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 «Програмні комплекси захисту АС від НСД»
3 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**
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. Екзамен оцінюється у 40 балів за розподілом: 20 балів – письмова відповідь; 20 балів – захист проекту згідно обраної теми. Студент дає письмову відповіді на два теоретичні питання. Перевірка у ручному режимі. При дистанційному проведенні екзамену студент повинен розмістити відповідь на білет окремим файлом в системі Moodle; ці завдання передбачають ручну перевірку викладачем. **Критерії оцінювання завдань відкритого типу (задач)**: 10 балів: Відмінний рівень знань (умінь), відповідь повна, вичерпна й достатньо обґрунтована, правильні відповіді на додаткові питання; 9 балів: Відмінний рівень знань (умінь), відповідь повна, вичерпна й достатньо обґрунтована з, можливими, незначними недоліками; 8 балів: Високий рівень знань (умінь), відповідь повна, достатньо обґрунтована з, можливими, незначними недоліками або помилками; 7 балів: Достатній рівень знань (умінь), але відповідь містить недоліки та / або незначну кількість помилок у розрахунках; 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; 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; 4 бали: Посередній рівень знань (умінь), відповідь не повна, містить багато недоліків та / або значну кількість помилок;

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. Структура законодавства України в області захисту інформації.
2. Нормативно-правова база захисту АС від НСД.
3. Побудова і структура критеріїв захищеності інформації.
4. Критерії конфіденційності.
5. Критерії цілісності.
6. Критерії доступності.
7. Критерії спостереженості.
8. Критерії гарантій.
9. Класифікація автоматизованих систем.
10. Функціональні профілі захищеності.
11. Визначення і призначення функціонального профілю захищеності.
12. Семантика профілю захищеності.
13. Стандартні функціональні профілі захищеності.
14. Вибір профілю захищеності залежно від призначення автоматизованих систем.
15. Стандартні функціональні профілі захищеності в КС, що входять до складу автоматизованих систем, призначених для автоматизації діяльності органів державної влади.
16. Стандартні функціональні профілі захищеності КС, що входять до складу автоматизованих систем, які призначені для автоматизації банківської діяльності.
17. Стандартні функціональні профілі захищеності в КС, що входять до складу автоматизованих систем, які призначені для керування технологічними процесами.
18. Стандартні функціональні профілі захищеності в КС, що входять до складу довідково-пошукових систем.
19. Загальні відомості програмного комплексу «ЛОЗА-1»
18. Основні характеристики програмного комплексу «ЛОЗА-1».

19. Профіль та рівень гарантій програмного комплексу «ЛОЗА-1».

20. Конфігурації та вимоги до умов експлуатації програмного комплексу «ЛОЗА-1».

21. Загальні відомості програмного комплексу «ЛОЗА-2».

22. Основні характеристики програмного комплексу «ЛОЗА-2».

23. Профіль та рівень гарантій програмного комплексу «ЛОЗА-2».

24. Конфігурації та вимоги до умов експлуатації програмного комплексу «ЛОЗА-2».

25. Комплекс захисту інформації від несанкціонованого доступу «Гриф-ХР».

26. Комплекс захисту інформації від несанкціонованого доступу «Гриф» версії 3.

27. Комплекс захисту інформації від несанкціонованого доступу «Гриф» версії 4.

28. Комплекс захисту інформації від несанкціонованого доступу «Гриф-Мережа».

29. Комплекс захисту інформації від несанкціонованого доступу «Рубіж-РСО».

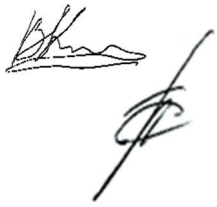
30. . Комплекс захисту інформації від несанкціонованого доступу «VTI-Рубіж».

31. Порівняльний аналіз комплексів захисту інформації від несанкціонованого доступу АС класу 1 та АС класу 2.

32. Надбудований КЗЗ над стандартними операційними системами.

33. Надбудований мережний комплекс засобів захисту інформації.

34. Вимоги до середовища експлуатації, системи та персоналу.

Екзаменатор  Валерій КОЗАЧОК

Завідувач кафедри Павло СКЛАДАННИЙ