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

ОСНОВИ ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ

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 «Основи захисту конфіденційних даних»
4 курс – освітній рівень – перший (бакалаврський)
Спеціальність 125 Кібербезпека
Освітня програма: 125.00.01 Безпека інформаційних і комунікаційних систем
Форма проведення: тестування на платформі Moodle в ЕНК дисципліни: https://elearning.kubg.edu.ua/course/view.php?id=21056
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. Студент дає відповіді на запитання електронного тесту в системі Moodle. Тест містить 32 тестових завдання з яких 24 завдання закритої форми (вибір правильної відповіді із запропонованих варіантів), кожне оцінюється 1 балом, а також 8 завдань відкритої форми, кожне оцінюється 2 балами. Всі завдання передбачають автоматичну (комп'ютерну) перевірку. 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. 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. Характеристика конфіденційної інформації як підвиду інформації з обмеженим доступом. 2. Основні загрози та дії що призводять до втрати конфіденційної інформації.

3. Канали несанкціонованого отримання конфіденційної інформації.
4. Методи несанкціонованого отримання конфіденційної інформації.
5. Комплексний підхід до побудови системи захисту від загроз порушення конфіденційності інформації.
6. Нормативно-правові засади забезпечення безпеки конфіденційної інформації.
7. Створення власних нормативно-правових документів організації.
8. Основні організаційні аспекти забезпечення захисту конфіденційних даних.
9. Методи роботи з персоналом.
10. Політика інформаційної безпеки.
11. Процес реалізації організаційних заходів.
12. Особливості інформаційно-аналітичної робота у контексті забезпечення захисту конфіденційної інформації.
13. Ключові поняття розмежування та контролю доступу до інформаційних ресурсів.
14. Основні механізми контролю доступу до інформаційних ресурсів автоматизованої системи.
15. Особливості побудови та функціонування систем ідентифікації/аутентифікації.
16. Парольні системи ідентифікації/аутентифікації.
17. Апаратна ідентифікація/аутентифікація.
18. Біометричні методи ідентифікації/аутентифікації.
19. Розмежування доступу, як складова частина системи управління доступом до інформаційних ресурсів.
20. Концепція ізолювання автоматизованої системи для роботи з конфіденційною інформацією.
21. Особливості дискреційного управління доступом.
22. Особливості мандатного управління доступом.
23. Особливості рольового управління доступом.
24. Поняття про моделювання розмежування доступу.
25. Модель Харрісона-Руззо-Ульмана.
26. Модель Белла-ЛаПадули.
27. Технологія виявлення та попередження витоку конфіденційних даних.
28. Методи розпізнавання конфіденційної інформації.
29. Базові компоненти DLP-систем та їх характеристика.
30. Інтелектуалізовані механізми виявлення та попередження витоку конфіденційних даних.

31. Технологія забезпечення захисту зовнішнього периметру.

Приклад екзаменаційного завдання

1. Визначне основу мандатного управління доступом. Оберіть лише один варіант відповіді.
   a. Права та повноваження доступу розподіляються лише адміністратором системи.
   b. Права та повноваження доступу розподіляються на основі визначеної політики ІБ.
   c. Права та повноваження доступу розподіляються на основі матриці доступу.
   d. Права та повноваження доступу розподіляються на основі класифікації за рівнем секретності.
2. Назвіть три основних механізми контролю доступу до інформаційних ресурсів захищеної автоматизованої системи:
   Формат відповіді: *назва механізму, назва механізму, назва механізму*
   Відповідь: _____

Екзаменатор  Роман КИРИЧОК

Завідувач кафедри  Павло СКЛАДАННИЙ