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 АНАЛІЗУ ТА СИНТЕЗУ ПОЛІТИК БЕЗПЕКИ

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 аналізу та синтезу політик безпеки»
3 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=21434
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. Передумови необхідності застосування організаційних методів забезпечення безпеки інформації. 2. Базові поняття політики інформаційної безпеки. 3. Визначення основних причин та цілей створення політики безпеки.

4. Основна група нормативно-правових документів, стандартів, що використовуються при формуванні політики безпеки.
5. Міжнародний стандарт ISO/IEC 27002:2022 «Information security, cybersecurity and privacy protection – Information security controls».
6. Комплексний міжнародний стандарт ISO 15408.
7. Стандарт BSI (Німеччина) «Керівництво щодо захисту інформаційних технологій для базового рівня захищеності».
8. Стандарт COBIT (Control Objectives for Information and related Technology).
9. Функціональні критерії НД ТЗІ 2.5-004-99.
10. Концептуальний підхід компанії IBM.
11. Концептуальний підхід компанії Cisco Systems.
12. Концептуальний підхід компанії Microsoft.
13. Концептуальний підхід інституту SANS.
14. Головні аспекти обстеження середовища функціонування ІКС та визначення об’єктів захисту.
15. Інвентаризація інформаційних активів, як основний механізм визначення об’єктів захисту.
16. Визначення та аналіз поняття загрози безпеці інформації.
17. Основні підходи до формування моделі загроз.
18. Підходи до формування моделі порушника.
19. Поняття ризиків ІБ.
20. Основні способи оцінки інформаційних ризиків.
21. Організаційні аспекти формування політики безпеки.
22. Особливості процедури формування політики безпеки.
23. Основні аспекти вироблення офіційної політики ІБ підприємства.
24. Основні аспекти вироблення процедур для попередження порушення безпеки.
25. Організаційні аспекти щодо реакція на порушення безпеки.

Приклад екзаменаційного завдання

1. На який нормативний документ опирається концептуальний підхід компанії IBM при формуванні корпоративної політики інформаційної безпеки? Оберіть лише один варіант відповіді.
   a. Міжнародний стандарт ISO 15408.
   b. Стандарт CobiT.
   c. Міжнародний стандарт ISO 17799: 2005.
   d. Міжнародний стандарт ISO / IEC TR 13335.

2. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу» включають наступні групи критеріїв:
   Формат відповіді: *назва групи критеріїв* та *назва групи критеріїв*
   Відповідь: _____

Екзаменатор  Роман КИРИЧОК

Завідувач кафедри  Павло СКЛАДАННИЙ