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

ІНФРАСТРУКТУРА ВІДКРИТИХ КЛЮЧІВ

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 «Інфраструктура відкритих ключів»
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=20190
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. Сутність симетричних та асиметричних криптосистем, цифровий конверт та цифровий підпис. 2. Генерація та управління ключами.

3. Життєвий цикл криптографічних ключів, практичні вимоги та рекомендації щодо забезпечення їх безпеки.
4. Поняття про модель порушника безпеки криптосистем.
5. Принцип Керкхофса щодо безпеки шифрів та основні види атак на криптосистеми.
6. Державна класифікація засобів КЗІ за рівнями безпеки та практичні вимоги з безпеки.
7. Підходи ЄС щодо захисту інформації та електронного цифрового підпису.
8. Правове регулювання електронних довірчих послуг (ЕДП) в України.
9. Правове регулювання захисту інформації в інформаційно-комунікаційних системах (ІКС).
10. Нормативні акти КМ України щодо захисту інформації в ІТС та ЕДП.
11. Основні органи зі стандартизації у галузі ІВК.
12. Класифікація стандартів ISO/IEC, ITU-T, IEEE, ISOC у галузі ІВК.
13. Узагальнена характеристика напрямків стандартизації в галузі ІВК.
14. Призначення сертифікату відкритого ключа та його структура за стандартом X.509.
15. Поняття довіри в контексті електронних комунікацій.
16. Концепція довіри в ІВК.
17. Політика безпеки і способи її реалізації.
18. Політика застосування сертифікатів.
19. Регламент засвідчувального центру.
20. Етапи розробки політики застосування сертифікатів.
21. Набір положень політики ІВК.
22. Труднощі розробки політики та регламенту.
23. Основні компоненти ІВК та їх характеристики.
24. Основні сервіси ІВК та їх характеристика.
25. Основні типи архітектури ІВК.
26. Попередній етап розгортання ІВК.
27. Проєктування ІВК.
28. Створення прототипу, пілотний проект і впровадження.
29. Підготовка системи ІВК до роботи.
30. Управління сертифікатами і ключами.
31. Реагування на інциденти під час функціонування ІВК.
32. Процедура анулювання цифрових сертифікатів.
33. Відновлення, резервне копіювання та зберігання ключів в архіві.
34. Основні проблемні аспекти інтеграції ІВК.

35. Основні проблемні аспекти функціональної сумісності продуктів різних постачальників.
36. Основні проблемні аспекти репозиторія ІВК.
37. Практичне застосування технології ІВК.
38. Проблеми вибору постачальника технології або окремих сервісів ІВК.

Приклад екзаменаційного завдання

1. В чому полягає основне призначення сертифікату відкритого ключа? Оберіть лише один варіант відповіді.
   a. Встановлення терміну дії відкритого ключа.
   b. Однозначна ідентифікація суб'єкта сертифіката відкритого ключа.
   c. Однозначна ідентифікація власника сертифіката відкритого ключа.
   d. Мінімізація ризиків атак на ІВК.
2. Одним із етапів інформаційного процесу – управління криптографічними ключами є генерація, назвіть ще 2 етапи:
   Формат відповіді: *eman*, *eman*
   Відповідь: _____

Екзаменатор Роман КИРИЧОК

Завідувач кафедри Павло СКЛАДАННИЙ