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

МОНІТОРИНГ, АУДИТ ТА АДМІНІСТРУВАННЯ ЗАХИЩЕНИХ ІТ СИСТЕМ І МЕРЕЖ

галузь знань	12 Інформаційні технології
спеціальність	125 Кібербезпека та захист інформації
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 «Моніторинг, аудит та адміністрування захищених ІТ систем і мереж»

1 курс – освітній рівень – другий (магістерський)

Спеціальність 125 Кібербезпека та захист інформації

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=18091

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 та індивідуальної конференції засобами TeamViewer+ Viber.

Студент дає відповіді на запитання та завдання білету. Білет містить 2 теоретичних питання та 1 практичне завдання. Екзамен оцінюється у 40 балів за розподілом: 20 балів – теоретичний тест з дисципліни; 20 балів – виконання практико-орієнтованого завдання. Відповіді на питання та порядок розв'язання практичного завдання студент має надати особисто, засобами TeamViewer+ Viber, ці завдання передбачають ручну перевірку викладачем.

Критерії оцінювання теоретичних питань:

10 балів: Відмінний рівень знань, відповідь повна, вичерпна й достатньо обґрунтована

9 балів: Відмінний рівень знань, відповідь повна, вичерпна й достатньо обґрунтована з, можливими, незначними недоліками

8 балів: Добрий рівень знань, відповідь містить недоліки та / або незначну кількість помилок

7 балів: Посередній рівень знань, відповідь містить багато недоліків та незначну кількість помилок

6 балів: Мінімально допустимий рівень знань, що характеризується недостатньою обґрунтованістю, фрагментарністю; відповідь неповна, містить недоліки та помилки

5 балів: Низький рівень знань понять і фактів, без належного їх розуміння, що характеризується недостатньою обґрунтованістю; відповідь неповна, містить недоліки та помилки

4 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.

0-3 бал: Незадовільний рівень знань, що виявляється у неспроможності відтворити означення понять та формулювання теорем, невмінні розв'язувати задачі.

0 балів: Відповідь відсутня.

Критерії оцінювання практичного завдання (задачі):

20-17 балів: Відмінний рівень умінь, розв'язання задачі повне, вичерпне володіння програмним забезпеченням, можливими, незначними недоліками

16-13 балів: Добрий рівень умінь, розв'язання задачі містить небагато недоліків та / або незначну кількість помилок

12-9 балів: Мінімально допустимий рівень умінь, що характеризується недостатнім рівнем володіння програмним забезпеченням, розв'язання задачі неповне, містить недоліки та помилки

8-5 бали: Незадовільний рівень умінь, що виявляється у нездатності застосувати знання при розв'язанні задач.

4-1 бал: Незадовільний рівень умінь, що виявляється у неспроможності володіння програмним забезпеченням, 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 екзаменаційного тесту із підсумковою оцінкою Fx за дисципліну. При виконанні завдань допускається користування довідковою літературою, таблицями значень функції, критеріїв та ін.

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. Основні завдання моніторингу ІТ систем.
2. Основні функції та властивості систем моніторингу безпеки.
3. Вимоги до систем моніторингу захищених ІТ систем і мереж.
4. Загальні відомості про DLP системи.
5. Основні функції DLP системи.
6. Основні типи DLP систем.
7. Архітектура DLP-систем.
8. Типовий склад DLP систем.
9. Базовий набір функцій агента DLP-системи.
10. Загальні відомості про виявлення мережевих атак шляхом аналізу трафіка.
11. Основні методи виявлення мережевих атак шляхом аналізу трафіка.
12. Основні механізми перехоплення трафіка .
13. Протокол простого мережевого моніторингу (SNMP), RFC 1157.
14. Ключові компоненти протоколу SNMP.
15. Програмні засоби аналізу трафіка.
16. Загальна характеристика функціонування програмного комплексу SearchInform.
17. Взаємодія основних компонентів програмного комплексу SearchInform.
18. Можливості індексованого пошуку програмного комплексу SearchInform.
19. Призначення продуктів DataCenter та ReportCenter.
20. Призначення клієнт-серверного компонента AlertCenter.

21. Призначення серверу NetworkSniffer та EndpointSniffer.
22. Загальні положення забезпечення безпеки інформаційних систем.
23. Функція керування інформаційною системою.
24. Визначення та зміст Політики безпеки.
25. Зміст правил розмежування доступу.
26. Регламент доступу до інформаційних ресурсів мережі.
27. Підходи до проведення аудиту.
28. Визначення та зміст моніторингу безпеки інформаційних систем.
29. Внутрішній та зовнішній аудит інформаційної безпеки.
30. Завдання, що вирішує моніторинг інформаційної безпеки.
31. Технічний аудит інформаційної безпеки:
32. Основні механізми моніторингу безпеки інформаційної системи.
33. Стандарти безпеки ISO 27001, ISO 27002.
34. Сканування, як механізм пасивного аналізу.
35. Зміст аудиторського звіту.
36. Зондування, як механізм активного аналізу.
37. Призначення та склад системи моніторингу подій інформаційної безпеки.
38. Основні форми і способи забезпечення інформаційної безпеки держави.
39. Склад системи моніторингу подій інформаційної безпеки.
40. Визначення поняття аудит інформаційної безпеки.
41. Можливості системи моніторингу подій інформаційної безпеки.
42. Джерела інформації, що використовують SIEM-системи.

Приклади екзаменаційного завдання *(задачі)*

1. Основні функції DLP системи.
2. Підходи до проведення аудиту.

   Практичне питання
3. Моніторинг стану ІТ систем і мереж з використанням сканерів безпеки.

Екзаменатор  Андрій АНОСОВ

Завідувач кафедри  Павло СКЛАДАННИЙ