МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ, ПРОГРАМНОЇ ІНЖЕНЕРІЇ ТА КОМП'ЮТЕРНИХ НАУК
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Голова приймальної комісії
Міжнародного гуманітарного університету
Ректор
_____ К.В. Громовенко
_____ 2023 р.

ПРОГРАМА
фахового вступного випробування
для здобуття другого (магістерського) рівня вищої освіти на основі раніше здобутого першого (бакалаврського) рівня, другого (магістерського) рівня освіти або освітньо-кваліфікаційного рівня спеціаліста

ГАЛУЗЬ ЗНАНЬ 12 Інформаційні технології
(шифр та назва галузі знань)

СПЕЦІАЛЬНІСТЬ 125 Кібербезпека та захист інформації
(шифр та назва спеціальності)

ОСВІТНЯ ПРОГРАМА 125 Кібербезпека та захист інформації
(назва освітньої програми)

Розглянуто та схвалено:
на засіданні кафедри комп'ютерної інженерії та інноваційних технологій
Протокол № _7_ від 28 березня 2023 р.

Розглянуто та схвалено:
на засіданні Вченої ради Міжнародного гуманітарного університету
Протокол № _6/1_ від 7 квітня 2023 р.

Введено в дію Наказом Міжнародного гуманітарного університету № 574а від 07.04.2023

Одеса 2023

Програма фахового вступного випробування для здобуття другого (магістерського) рівня вищої освіти зі спеціальності 125 Кібербезпека та захист інформації.

Розробник:

Йона Л. Г., к.т.н., доцент кафедри комп'ютерної інженерії та інноваційних технологій Міжнародного гуманітарного університету;

Завідувач кафедри
кафедри комп'ютерної
інженерії та інноваційних технологій,
к.т.н., доцент В.І. Гура

Програма розглянута та схвалена на засіданні кафедри комп'ютерної інженерії та інноваційних технологій Протокол № 7 від 28 березня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Мета фахового вступного випробування полягає в комплексній перевірці знань абітурієнтів, отриманих ними в результаті вивчення циклу дисциплін, на основі раніше здобутого першого (бакалаврського) рівня, другого (магістерського) рівня освіти або освітньо-кваліфікаційного рівня спеціаліста зі спеціальності 125 Кібербезпека та захист інформації. Абітурієнт повинен на фаховому вступному випробуванні продемонструвати фундаментальні та професійно-орієнтовані уміння та знання передбачені для спеціальності 125 Кібербезпека та захист інформації.

Фахове вступне випробування базується на матеріалах з навчальних дисциплін «Інформаційні технології в інформаційній та/або кібербезпеці», «Безпека інформаційно-комунікаційних систем», «Комплексні системи захисту інформації», «Управління інформаційною та / або кібербезпекою», «Криптографічний захист інформації», «Технічний захист інформації».

МЕТА ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

Визначення рівня підготовки абітурієнтів з метою проведення конкурсного відбору для навчання в Міжнародному гуманітарному університеті (далі: Університет) зі спеціальності 125 Кібербезпека та захист інформації.

ФОРМА ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

Згідно з чинним «Порядком прийому до Міжнародного гуманітарного університету у 2023 році», для охочих продовжити навчання за другим (магістерським) рівнем вищої освіти передбачено обов'язкове складання фахового вступного випробування, який може проводитися очно та/або дистанційно . Нижче наведена структура даного випробування та навчальні матеріали, які рекомендовані для опрацювання в ході підготовки до нього. (Додаток 1).

1. Фахове вступне випробування проводиться у вигляді тестового завдання. Абітурієнт відповідає на двадцять тестових завдань, кожне з яких має 4 варіанти відповіді. Вступнику необхідно вибрати одну правильну відповідь з кожного тестового завдання. Питання взято з дисциплін відповідних до програм підготовки бакалаврів, спеціалістів або магістрів 125 Кібербезпека та захист інформації: «Інформаційні технології в інформаційній та/або кібербезпеці», «Безпека інформаційно-комунікаційних систем», «Комплексні системи захисту

інформації», «Управління інформаційною кібербезпекою», «Криптографічний захист інформації», «Технічний захист інформації».

2. Перелік запитань, покладених в основу фахового вступного випробування з фахових дисциплін, наведено в Додатку 1.

КРИТЕРІЇ ОЦІНЮВАННЯ

Фахове вступне випробування проводиться у вигляді тестового завдання. Тестове завдання складається з 20 питань, кожне з яких оцінюється в 10 балів.

При оцінюванні знань абітурієнта, вихідними критеріями є такі:

– кожна вірна відповідь на тестове завдання оцінюється у 10 балів;

– оцінку «відмінно» абітурієнт отримує, якщо він набрав 180 або 190, або 200 балів;

– оцінку «добре» абітурієнт отримує, якщо він набрав 150 або 160, або 170 балів;

– оцінку «задовільно» абітурієнт отримує, якщо він набрав 100 або 110, або 120, або 130, або 140 балів;

– оцінку «незадовільно» абітурієнт отримує, якщо він набрав менше ніж 100 балів.

Додаток 1

Перелік питань для фахового вступного випробування для осіб, що виявили бажання продовжити навчання для здобуття другого (магістерського) рівня вищої освіти зі спеціальності
125 Кібербезпека та захист інформації

1. Властивості інформації, яку необхідно захищати.
2. Схема секретної системи зв'язку.
3. Що визначає поняття «криптостійкість» в інформаційних системах?
4. Як вирішується питання автентифікації в телекомунікаціях?
5. Принципи побудови шифрів на базі мережі Фейстеля.
6. З яких процедур складається процес керування ключами?
7. Які складові частини включає криптологія і в чому їх зміст?
8. У чому сутність шифрів простої заміни? Різновиди шифрів простої заміни.
9. Які існують канали несанкціонованого витоку інформації в системах телекомунікації?
10. Поясніть сутність понять "перемішування" та "розсіювання" за К. Шенноном?
11. З яких простих перетворювань складається складний шифр?
12. Принципи керування ключовою системою.
13. Поясніть сутність методів шифрування: підставляння, переставляння та гамування.
14. Які питання вивчає стеганографія?
15. Що називають атаками на інформаційні об'єкти?
16. Пояснити поняття "активної атаки " в інформаційних системах.
17. Пояснити поняття "пасивної атаки" в інформаційних системах.
18. Принцип рівноміцного захисту в інформаційних системах.
19. Принципи шифрування за допомогою операції перестановки.
20. Які алгоритми називають блоковими?
21. Що визначає поняття "ключ" в інформаційних системах? Види ключів.
22. Вимоги щодо стійкого шифру, які сформулював К.Шеннон.
23. На які основні класи поділяють сучасні алгоритми шифрування.
24. Які криптографічні алгоритми називають симетричними?
25. Які криптографічні алгоритми називають несиметричними?
26. Розподілення криптоалгоритмів за призначенням.
27. Призначення електронного цифрового підпису.
28. Які процедури включає електронний цифровий підпис і в чому їх зміст?
29. Що містить в собі електронний цифровий підпис?
30. Привести алгоритм розподілення ключів за методом Диффі – Хеллмана.
31. Дати характеристику криптосистеми AES.

32. Дати характеристику криптосистеми ДСТУ 7624:2014 "Калина".
33. Дати характеристику алгоритму шифрування RSA.
34. Дати характеристику алгоритму цифрового підпису RSA.
35. Дати характеристику алгоритму шифрування Ель Гамаля.

ПЕРЕЛІК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. ДСТУ 33960-96 Захист інформації. Технічний захист інформації. Основні положення.

2. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

3. НД ТЗІ 1.6-005-2013. Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

4. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

5. Про внесення змін до Закону України "Про захист інформації в автоматизованих системах " № 2594-IV від 31.05.2005. – Відомості Верховної Ради України 2005, № 26, ст. 347. – (Серія видань "Законодавство України").

6. Антіпов І.Є., Олейніков А.М., Ликов Ю.В., Кукуш В.Д., Милютченко І.О. Засоби та системи технічного захисту інформації. Навчальний посібник для студентів ЗВО// Харків: ФОП Панов А.М., 2019.- 216 с.

7. Онацький О.В., Йона Л.Г. Криптографічні системи. Навчальний посібник з дисципліни «Криптографія», «Криптоаналіз» для освітньо-професійної підготовки бакалаврів з галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека» 2020. 157с.

8. Йона Л.Г., Онацький О.В., Швець О.В. Системи банківської безпеки: Навч.посібник.- Одеса: ДУІТЗ. 2021.