МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЗАТВЕРДЖУЮ
Голова приймальної комісії
Харківського національного
економічного університету
імені Семена Кузнеця
_____ Володимир ПОНОМАРЕНКО
«10» березня 2021 р.

ПРОГРАМА ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

освітній ступінь «МАГІСТР»

спеціальність 125 «Кібербезпека»
освітньо-професійна програма «Кібербезпека»

Харків
2021

Програма фахового випробування розроблена для абітурієнтів, які вступають на навчання за освітньо-кваліфікаційним рівнем магістр за спеціальністю 125 "Кібербезпека".

Завдання фахового випробування складено з метою виявлення знань, вмінь, компетентностей, якими володіє бакалавр за галуззю знань 12 "Інформаційні технології", спеціальність "Кібербезпека" (табл. 1).

Таблиця 1

Основні компетентності, якими повинен володіти бакалавр за галуззю знань 12 "Інформаційні технології", спеціальність "Кібербезпека"

Інтегральна компетентність	
	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності	
	Здатність застосовувати знання у практичних ситуаціях
	Знання та розуміння предметної області та розуміння професії.
	Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
	Вміння виявляти, ставити та вирішувати проблеми.
	Здатність до пошуку, оброблення та аналізу інформації.
	Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні
	Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Фахові компетентності	
	Здатність застосовувати законодавчу та нормативно- правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
	Здатністьдо використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
	Здатність до використання програмних та програмно- апаратних

	комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
	Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
	Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.
	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
	Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

ЗМІСТ ФАХОВИХ ВСТУПНИХ ВИПРОБУВАНЬ

Тема 1. **Базові поняття криптології**.

Основні поняття криптографії.

Задачі криптографічного захисту інформації в інформаційних та телекомунікаційних системах.

Визначення та загальна математична модель симетричної криптосистеми.

Основні класи симетричних криптосистем (транзитивні, регулярні та мінімальні криптосистеми).

Визначення та математичні моделі шифрів простої заміни та перестановки.

Методика дешифрування простої заміни та перестановки.

Визначення та математичні модель табличного шифру гамування.

Шифри Цезаря, Віжінера, Вернама.

Розв'язання задач зашифрування та розшифрування повідомлень з використанням табличних шифрів гамування.

Тема 2. **Теоретичні основи побудови та аналізу симетричних криптосистем.**

Ймовірнісна модель шифру. Теоретична стійкість криптографічних систем, критерії теоретичної стійкості симетричних криптосистем. Обчислювальна стійкість криптосистем. Показники та критерії обчислювальної стійкості.

Основні класи симетричних криптосистем. Математична модель та принципи побудови потокових шифрів. Принципи побудови та критерії стійкості шифрів гамування.

Основні типи сучасних генераторів псевдовипадкових послідовностей (ПВП). Алгебраїчні та структурні властивості псевдовипадкових послідовностей (поняття періоду та еквівалентної лінійної складності ПВП). Статистичні властивості ПВП.

Основні властивості лінійних регістрів зсуву. Розв'язання задач визначення функції зворотного зв'язку та початкового заповнення лінійного регістру зсуву. Моделювання лінійних регістрів зсуву з використанням ПЕОМ. Моделювання нелінійних вузлів ускладнення з використанням ПЕОМ.

Принципи побудови та класифікація сучасних блокових шифрів. Огляд методів криптографічного аналізу та обґрунтування стійкості блокових шифрів. Схема алгоритму шифрування та математична модель блокового шифру ДСТУ ГОСТ-28147:2009. Режими використання алгоритму шифрування даних ДСТУ ГОСТ-28147:2009.

Rijndael: принципи побудови, математична модель та схема алгоритму шифрування. Криптографічні властивості блокового шифру Rijndael.

Принципи побудови, функціонування та криптоаналізу блокових шифрів DES, IDEA. Основні режими роботи сучасних блокових шифрів.

Тема 3. **Теоретичні основи побудови та аналізу асиметричних криптосистем.**

Загальні принципи побудови та використання асиметричних криптографічних систем. Основні класи задач, що вирішуються з використанням асиметричних криптографічних систем.

Задачі факторизації цілих чисел та дискретного логарифмування. Поняття про складність сучасних алгоритмів факторизації та дискретного логарифмування. Огляд сучасних методів обгрунтування обчислюваної стійкості асиметричних криптосистем.

Система відкритого шифрування RSA. Схема цифрового підпису RSA. Розв'язання задач зашифрування, розшифрування та цифрового підпису повідомлень з використанням криптосистеми RSA.

Алгоритми відкритого шифрування та розшифрування інформації в криптосистемі Ель-Гамаля. Розв'язання задач зашифрування та розшифрування повідомлень з використанням криптосистеми Ель-Гамаля. Алгоритми формування та перевірки підпису в схемі цифрового підпису Ель-Гамаля. Розв'язання задач формування та перевірки підпису з використанням схеми Ель-Гамаля.

Протокол Діффі – Геллмана. Розв'язання задачі узгодження ключу за протоколом Діффі – Геллмана.

Криптографічні протоколи STS та MTI. Розв'язання задач узгодження ключів за протоколами STS та MTI.

Тема 4. Протоколи автентифікації. Цифрові підписи**.** Комплексні системи захисту даних

Принципи захисту інформації на мережевому рівні. Протоколи захисту та цілісності *IPSec*, *SSL*, *TLS*, їх сутність.

Класифікація механізмів автентифікації. *MDC*-коди, основні алгоритми. *MAC*-коди, основні способи формування. Класифікація стандартів електронних цифрових підписів. Основні стандарти цифрового підпису.

Основні функції систем захисту *PGP* і *CS MIME.* Принципи сумісності на рівні електронної пошти. Принципи побудови захищеної електронної пошті.

Тема 5. Основи криптоаналізу

Формальне математичне визначення криптосистеми.

Критерії та показники ефективності.

Класифікація криптоаналітичних атак.

Принципи лінійного та диференціального криптоаналізу.

Тема 6. **Основи цифровій стеганографії**

Основні принципи приховування повідомлення на основі методів стеганографії.

Класифікація и принципи приховування алгоритмів цифровій стеганографії.

Тема 7. **Основи технології відкритих ключів (PKI).**

Основні компоненти та сервіси інфраструктури відкритих ключів.

Архітектура та топологія PKI.

Сертифікати відкритих ключів X.509.

Тема 8. **Захист програмного забезпеченні в Інтернет-технологіях**

Основні принципи захисту інформації під час підключення до мережі Інтернет.

Використання паролів і механізмів контролю.

Тема 9. **Захист персональних даних**

Основні принципи захисту персональних даних на основі програмного коду.

Моделі захисту персональних даних.

Приклад
завдань екзаменаційного білету

Завдання 1

1. Що не є метою безпеки
a) конфіденційність
b) цілісність
c) готовність
d) надійність

2. Вкажіть відповідність між цілями безпеки інформації та групами атак

Група атак	Цілі безпеки інформації
1) втручання 2) спостереження за трафіком і його аналіз 3) модифікація 4) імітація джерела 5) повторна передача інформації 6) відмова від повідомлення 7) припинення обслуговування запиту	a) конфіденційність b) цілісність c) готовність d) надійність

3. Вкажіть відповідність між атаками, характером (пасивність, активність) і цілями загроз

атаки	Пасивні / активні	Загроза
1) втручання 2) спостереження за трафіком і його аналіз 3) модифікація 4) імітація джерела 5) повторна передача інформації 6) відмова від повідомлення 7) припинення обслуговування запиту	Пасивні - П Активні - А	a) конфіденційність b) цілісність c) готовність d) надійність

4. Установіть відповідність між службою безпеки і послугою

Служба безпеки	послуги безпеки
1) конфіденційність даних 2) цілісність 3) аутентифікація 4) виключення відмови від повідомлень 5) управління доступом	a) Захист даних від спроби їх розкриття b) Захист даних від модифікації, вставки, видалення і повторної передачі противником c) Встановлення автентичності оператора на іншому кінці лінії d) Захищає від відмови від повідомлення передавачем або приймачем даних e) Забезпечує захист від неправомірного доступу до даних

5. Технічний захист інформації це:

a) діяльність, спрямована на забезпечення інженерними заходами конфіденційності, цілісності та доступності інформації, важливої для особи, суспільства і держави;

b) діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації, важливої для особи, суспільства і держави;

c) вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації з обмеженим доступом, важливої для особи, суспільства і держави;

d) діяльність, спрямована на забезпечення інженерними, технічними, організаційними, програмними, оперативними заходами цілісності та доступності інформації з обмеженим доступом, важливої для особи, суспільства і держави;

e) діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації з обмеженим

доступом, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави;

f) діяльність, спрямована на забезпечення конфіденційності, цілісності та доступності інформації.

Завдання 2

Ви є користувачем розподіленої захищеної системи з 6 користувачами. У даній системі користувачі можуть здійснювати асиметричне зашифрування (розшифрування) RSA і виробляти або перевіряти цифровий підпис на основі RSA для повідомлень.

Користувачі системи

Користувач	Параметр системи n		Ключі користувачів	
	p	q	Особливий (секретний) d	Відкритий (публічний) e
A	11	23	19	
B	17	19		137
C	11	17	37	
D	13	19		67
E	17	23	111	
F	13	17		25

Ви користувач "A".

Перевірити, що ваші ключі (відкритий і особливий) відібрані правильно.

Розшифруйте повідомлення M, яке отримано від користувача "F".

Формат повідомлення

Тип алгоритму	Відправник	Отримувач	Повідомлення	геш-значення	ЦП
Шифрування RSA	F	A	67	--	--

РОЗВ'ЯЗАННЯ

Завдання 1

Питання 1: Відповідь: d

Питання 2: Відповіді: 1-a; 2-a; 3-b; 4-b; 5-b; 6-b; 7-c.

Питання 3: Відповіді: 1-П-a; 2-П-a; 3-A-b; 4-A-b; 5-A-b; 6-A-b; 7-A-c.

Питання 4: Відповіді: 1-A; 2-B; 3-C; 4-D; 5-E.

Питання 5: Відповідь: 1 - e.

Завдання 2

1. Знаходимо ключі абонента A:

$n = p \times q = 11 \times 23 = 253$, $\varphi(n) = (p-1) \times (q-1) = 10 \times 22 = 220$

$KR_A = (19,253)$, $KU_A = (139,253)$,

2. Знаходимо ключі абонента F:

$n = p \times q = 13 \times 17 = 221$, $\varphi(n) = (p-1) \times (q-1) = 12 \times 16 = 192$

$KR_A = (169,220)$, $KU_A = (25,220)$,

3. Абонент F знаходить криптограму шляхом шифрування відкритого тексту особистим ключем (забезпечується автентичність):

$C = 67^{169} \bmod 220 = 67$

4. Абонент А знаходить відкритий текст шляхом розшифрування криптограми відкритим ключем абонента F

$C = 67^{25} \bmod 220 = 67$

Відповідь: відкритий текст – 67.

КРИТЕРІЇ ОЦІНЮВАННЯ

Кожен білет складається з двох завдань, їх бездоганне виконання оцінюється 100 балами (максимальна оцінка) за шкалою ХНЕУ ім. С. Кузнеця.

Перше завдання є діагностичним і являє собою тест, що містить 5 питань. Тестові питання вимагають від абітурієнта знання основ з безпеки інформації в межах тем Програми. Перше завдання оцінюється від 0 до 40 балів. За кожну правильну відповідь питання абітурієнт отримує 2 бали.

Друге завдання – задача на формування відповідного механізму безпеки (конфіденційність, цифровий підпис, автентифікація) за допомогою несиметричної криптосистеми RSA. Передбачається використовувати наступні критерії для виставлення оцінок:

Завдання 1.

Теоретичні питання у кількості 5 питань з основних положень дисципліни. Перше питання оцінюється в 2 бали. Питання з 2-4 оцінюються по 2 бали за кожну правильну відповідь (сумарно 17 відповідей), яка необхідна для відповіді на питання, питання 5 оцінюється у 4 балів.

Завдання 2.

Оцінка 60 балів. Практичне завдання виконано бездоганно з повним обґрунтуванням кожного етапу виконання завдання, зроблені повні висновки та узагальнення. Приведений протокол обміну відповідає вимогам відповідного стандарту, приведені алгоритми шифрування/розшифрування з повними поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), визначені достоїнства і недоліки обґрунтовані, проведений порівняльний аналіз обґрунтований. Наведені механізми та послуги в яких використовуються відповідні протоколи (схеми шифрування).

Оцінка 50 балів. Практичне завдання виконано повністю з обґрунтуванням кожного етапу виконання завдання. Приведений протокол обміну відповідає вимогам відповідного стандарту, приведена структурна схема

протоколу з повними поясненнями процедур шифрування/розшифрування, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), визначені основні достоїнства і недоліки обґрунтовані, в цілому проведений порівняльний аналіз обґрунтований.

Оцінка 40 балів. Практичне завдання виконано повністю. Приведений протокол обміну відповідає вимогам відповідного стандарту, приведені основні процедури шифрування/розшифрування з поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), але не в повному обсязі визначені основні достоїнства і недоліки, в цілому проведений порівняльний аналіз обґрунтований.

Оцінка 30 балів. Практичне завдання виконано повністю. Приведений протокол обміну відповідає вимогам відповідного стандарту, приведені основні процедури шифрування/розшифрування з поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), але не в повному обсязі визначені достоїнства і недоліки, проведений порівняльний аналіз не обґрунтований.

Оцінка 20 балів. Практичне завдання виконано повністю. Приведений протокол обміну відповідає вимогам відповідного стандарту, приведені основні процедури шифрування/розшифрування з поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), але не в повному обсязі визначені достоїнства і недоліки, не проведений порівняльний аналіз.

Оцінка 15 балів. Практичне завдання виконано неповністю. Приведений протокол обміну відповідає вимогам відповідного стандарту, приведені алгоритми шифрування/розшифрування, але сформована криптограма або повідомлення не відповідають алгоритму шифрування або розшифрування, не визначені основні достоїнства і недоліки, не проведений порівняльний аналіз.

Оцінка 10 балів. Практичне завдання виконано неповністю. Приведений протокол обміну в цілому відповідає вимогам відповідного стандарту, приведені алгоритми шифрування/розшифрування, але сформована криптограма і повідомлення не відповідають алгоритму шифрування/розшифрування, не визначені основні достоїнства і недоліки, не проведений порівняльний аналіз.

Оцінка 5 балів. Практичне завдання не виконано. Приведений протокол обміну не відповідає вимогам відповідного стандарту, не приведені алгоритми шифрування/розшифрування, сформована криптограма і повідомлення не відповідають алгоритму шифрування/розшифрування, пояснень процедур не має, не визначені достоїнства і недоліки, не проведений порівняльний аналіз.

Оцінка 0 балів. Практичне завдання не виконано. Протокол обміну не приведений, не приведені алгоритми шифрування/розшифрування, сформована криптограма і повідомлення не відповідають алгоритму шифрування/розшифрування, не визначені достоїнства і недоліки, не проведений порівняльний аналіз.

Підсумкова оцінка за екзамен з кібербезпеки є сумою оцінок (балів), отриманих за кожне завдання.

Обмеження в часі на реалізацію завдань – 45 хвилин.

Рекомендована література

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" (1994);
2. Закон України "Про захист персональних даних" (2010)
3. СТРАТЕГІЯ національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015)
4. Закон України "Про національну безпеку (2018)
5. Стратегія кібербезпеки України" (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016)
6. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229;
7. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення;
8. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;
9. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.
10. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ, К: 1999. – 34с.
11. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
12. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.
13. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
14. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
15. 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

16. ISO/IEC 27001. "Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью.

17. ISO/IEC 27002. "Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью."

18. ISO/IEC 27005. "Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности

19. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсеєв С. П., Король О. Г., Остапов С. Е., Коц Г. П. – Х.: ХНЕУ ім. С. Кузнеця, 2016. – 1013 Мб. ISBN 978-966-676-624-6

20. С. П. Євсеєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці. – Видавничий дом "Родовід", 2014. – 428 с.

21. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 672 с.: ил. – Парал. тит. англ.

Голова атестаційної комісії _____ Олександр Мілов

(підпис)