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

ЗАТВЕРДЖУЮ
Голова приймальної комісії
_____ В. С. Пономаренко
«30» 23 травня 2019р.

ПРОГРАМА
фахового вступного випробування
освітній ступінь «МАГІСТР»

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

Харків, 2019

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, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності	
	Здатність застосовувати знання у практичних ситуаціях
	Знання та розуміння предметної області та розуміння професії.
	Здатність спілкуватися рідною та другою іноземною мовою як усно, так і письмово
	Здатність здійснювати професійну діяльність згідно з вимогами санітарно-гігієнічного режиму, охорони праці, техніки безпеки та протипожежної безпеки
	Вміння виявляти, ставити та вирішувати проблеми.
	Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
	Навички міжособистісної взаємодії.
	Прагнення до збереження навколишнього середовища
	Здатність діяти соціально відповідально та громадянсько свідомо.
	Здатність вчитися і бути сучасно навченим.
	Здатність приймати обґрунтовані рішення.
	Здатність до адаптації та дії в новій ситуації.
	Дотримання та пропагування здорового способу життя.
	Здатність бути критичним та самокритичним
Спеціальні компетентності	
	Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності.
	Здатність до використання інформаційних і комунікаційних технологій з метою пошуку нової інформації, створення баз даних, аналізу розподілених АС, каналів зв’язку, систем управління процесами, баз даних, оперативного планування роботи систем на основі аналізу інформаційних потоків та їх оптимізації.
	Здатність здійснювати проектування (розробку) систем, технологій і засобів інформаційної безпеки

Спеціальні компетентності	
	Здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об’єктів і систем
	Здатність відновлювати нормальне функціонування ІТ систем і мереж після здійснення кібернападів, збоїв та відмов
	Здатність виконувати спеціальні дослідження технічних і програмно-апаратних засобів захисту обробки інформації в ІТС
	Здатність проводити техніко-економічного аналіз й обґрунтовувати проектні рішення з забезпечення кібербезпеки
	Здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою
	Здатність здійснювати управління інцидентами інформаційної та кібербезпеки
	Здатність здійснювати управління ризиками інформаційної та кібербезпеки
	Здатність виконувати моніторинг даних, комп’ютерних зловживань та аномалій
	Здатність прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави та дестабілізуючі чинники
	Здатність проводити дослідження у практичній професійній діяльності

ЗМІСТ ФАХОВИХ ВСТУПНИХ ВИПРОБУВАНЬ

Тема 1. **Базові поняття криптології**.

Задачі криптографічного захисту інформації в інформаційних та телекомунікаційних системах. Основні поняття криптографії. Визначення та загальна математична модель симетричної криптосистеми. Основні класи симетричних криптосистем (транзитивні, регулярні та мінімальні криптосистеми). Розв'язання задач обчислення суми, різниці та добутку цілих чисел за модулем n. Обернені елементи в кільці лишків за модулем n. Алгоритм Евкліда. Знаходження обернених елементів за модулем n з використанням алгоритму Евкліда. 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. Технічний захист інформації це:

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

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

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

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

д) 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;

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

2. Система технічного захисту інформації це:

а) сукупність технічних засобів, об’єднаних цілями та завданнями захисту інформації;

б) сукупність організацій, об’єднаних цілями та завданнями захисту інформації, нормативно-правова та матеріально-технічна база;

в) сукупність суб’єктів, об’єднаних цілями та завданнями захисту інформації інженерно-технічними заходами, нормативно-правова та матеріально-технічна база:

г) сукупність об’єктів, об’єднаних цілями та завданнями захисту інформації, нормативно-правова та матеріально-технічна база;

д) сукупність суб’єктів, об’єднаних цілями та завданнями захисту інформації, нормативно-правова та матеріально-технічна база;

е) сукупність об’єктів захисту інформації, інженерно-технічними заходами, нормативно-правова та матеріально-технічна база.

3. **Таємна інформація**, це:

а) інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. [Закон України “Про доступ до публічної інформації”]

б) інформація, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною.

в) інформація, доступ до якої обмежується відповідно до частини другої статті 6 Закону України "Про доступ до публічної інформації", розголошення якої може завдати шкоди особі, суспільству і державі.

г) інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, утвореним відповідно до законів України, державним підприємствам, установам та організаціям, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень.

4. **Технічний захист інформації**, це:

а) діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності інформації.

б) діяльність, спрямована на забезпечення інженерними заходами конфіденційності, цілісності та доступності інформації.

в) діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

г) діяльність, спрямована на забезпечення інженерно-технічними, програмними та організаційними заходами конфіденційності, цілісності та доступності інформації.

5. **Система ТЗІ**, це:

а) сукупність об'єктів ТЗІ, нормативно-правової бази та матеріально-технічної бази, об'єднаних цілями та завданнями захисту інформації організаційними, інженерними та технічними заходами.

б) сукупність органів та об'єктів, де здійснюється ТЗІ, нормативно-правової бази та матеріально-технічної бази, об'єднаних цілями та завданнями захисту інформації організаційними, інженерними та технічними заходами.

в) сукупність суб'єктів системи ТЗІ та матеріально-технічної бази, об'єднаних цілями та завданнями захисту інформації організаційними, інженерними та технічними заходами.

г) сукупність організаційної інфраструктури (об'єкту захисту, органів та об'єктів, де здійснюється ТЗІ, суб'єктів системи ТЗІ,), нормативно-правової бази та матеріально-технічної бази, об'єднаних цілями та завданнями захисту інформації організаційними, інженерними та технічними заходами.

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: Відповіді: 1 – д, 2 – в, 3 – в, 4 – в, 5 – г

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 200 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 100 балів. За правильну відповідь на одне питання абітурієнт отримує 20 балів.

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. Кожне питання оцінюється в 20 балів.

Завдання 2.

Оцінка 100 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 80 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 60 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 50 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 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 достоїнства і недоліки, не проведений порівняльний аналіз.

Оцінка 30 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 20 бали. 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 15 бали. 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 10 бали. 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 _____ С. П. Євсеєв

(підпис)