МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”

Навчально-науковий інститут комп’ютерних наук та інформаційних технологій

ЗАТВЕРДЖУЮ
проректор
_____ Руслан МИГУЩЕНКО
«04» _____ 2024 р.

ПРОГРАМА

для проведення вступних випробувань за фахом
при зарахуванні на навчання за освітньо-кваліфікаційним рівнем «бакалавр» на
1 курс за скороченою формою навчання та на 2–3 курс за конкурсними пропозиціями
освітніх програм:

Кібербезпека

Директор інституту
_____ Михайло ГОДЛЕВСЬКИЙ

Харків 2024

ЗМІСТ

Кібербезпека

АНОТАЦІЯ

Програма фахового випробування за фахом розроблена для абітурієнтів, які вступають на скорочений термін навчання за освітньо-кваліфікаційним рівнем бакалавра на базі молодшого спеціаліста за спеціальністю 125 «Кібербезпека».

Таблиця 1. Основні компетентності, якими повинен володіти молодший спеціаліст за галуззю знань 12 “Інформаційні технології”.

Інтегральна компетентність	Здатність вирішувати типові спеціалізовані задачі інженерії програмного забезпечення, що вимагає застосування положень і методів відповідних наук (математики, інформатики, інформаційних технологій, тощо) та може характеризуватися певною невизначеністю умов; нести відповідальність за результати своєї діяльності; здійснювати контроль інших осіб у визначених ситуаціях.
Загальні компетентності	**КЗ 1.** 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.
	КЗ 2. 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.
	КЗ 3. Здатність спілкуватися державною мовою як усно, так і письмово.
	КЗ 4. Здатність спілкуватися іноземною мовою.
	КЗ 5. Знання та розуміння предметної області та розуміння професійної діяльності.
	КЗ 6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
	КЗ 7. Здатність застосовувати знання у практичних ситуаціях.
Фахові компетентності	**КФ 1.** Здатність алгоритмічно та логічно мислити.
	КФ 2. Здатність вдосконалювати знання і навички в галузі інформаційних технологій та усвідомлення важливості навчання протягом усього життя.
	КФ 3. Здатність застосовувати теоретичні та емпіричні знання для розроблення, тестування, впровадження та супроводу програмного забезпечення.

	КФ 4. Здатність дотримуватися стандартів при розробці програмного забезпечення.
	КФ 5. Здатність брати участь у визначенні та формулюванні вимог до програмного забезпечення.
	КФ 6. Здатність брати участь у проектуванні програмного забезпечення.
	КФ 7. Здатність розробляти модулі і компоненти програмного забезпечення за допомогою типових алгоритмів та інструментів.
	КФ 8. Здатність забезпечувати інформаційну та функціональну безпеку програмного забезпечення.
	КФ 9. Здатність вибирати та використовувати ефективні інструментальні засоби розробки програмного продукту.
	КФ 10. Здатність реалізовувати всі етапи життєвого циклу програмного забезпечення.

ЗМІСТ ПРОГРАМИ

ПЕРЕЛІК ПИТАНЬ ВСТУПНОГО ВИПРОБУВАННЯ

1. Яке з наведених визначень є визначенням криптографії?
а. Прикладна інженерно-технічна дисципліна, яка займається розробкою, аналізом і обґрунтуванням стійкості криптографічних засобів захисту інформації від загроз з боку супротивника.
б. Галузь дискретної математики або математичної кібернетики, що вивчає математичні моделі криптографічних схем.
в. Завдання щодо порушення конфіденційності, цілісності, невідстежуваності криптографічного протоколу, що стоїть перед супротивником.
г. Наука про протидію захисту інформації у персональних комп'ютерах.

2. Яке з наведених визначень є визначенням прикладного криптографічного протоколу?
а. Протокол, який сам по собі використовується, або потенційно може використовуватися, для вирішення практичних задач.
б. Протокол, який не має самостійного прикладного значення, але використовується як компонент при побудові більш складних прикладних криптографічних протоколів.
в. Основний тип криптографічних протоколів, призначених для забезпечення цілісності. Є дві основні різновиди - протокол автентифікації учасника, званий також просто протоколом автентифікації або протоколом ідентифікації, та протокол автентифікації повідомлень.
г. Протокол, який сам по собі використовується, або потенційно може використовуватися, для вирішення теоретичних задач.

3. Яке з наведених визначень є визначенням криптології?
а. Прикладна інженерно-технічна дисципліна, яка займається розробкою, аналізом і обґрунтуванням стійкості криптографічних засобів захисту інформації від загроз з боку противника, вирішуючи тим самим три завдання криптографії - забезпечення конфіденційності, цілісності, невідстежуваності.
б. Галузь дискретної математики або математичної кібернетики, що вивчає математичні моделі криптографічних схем.
в. Завдання щодо порушення конфіденційності, цілісності криптографічного протоколу, що стоїть перед противником.
г. Протокол, який не має самостійного прикладного значення, але використовується як компонент при побудові більш складних прикладних криптографічних протоколів.

4. Якої групи вірусів не існує?
а. Завантажувальної.
б. Файлової.
в. Файлово-текстової.
г. Поліморфної

5. Який із симптомів не пов'язаний з вірусним зараженням ПК?
а. Уповільнення роботи деяких програм.
б. Збільшення розмірів текстових файлів.
в. Поява не існуючих раніше дивних файлів.
г. Самовільне перезавантаження комп'ютера.

6. Яка з перелічених програм не є антивірусною?
а. Програма-фаг.

б. Програма-ревізор.
в. Програма-фільтрат.
г. Програма-імунізатор.

7. Комп’ютерний вірус це?
а. Спеціально написана програма, здатна самовільно приєднуватися до інших програм, створювати свої копії та впроваджувати їх у файли, системні області комп’ютера і в обчислювальні мережі з метою порушення роботи програм, псування файлів і каталогів, створення всіляких перешкод в роботі комп'ютера.
б. Спеціальний програмно-апаратний комплекс, здатний самовільно приєднуватися до інших програм, створювати свої копії та впроваджувати їх у файли, системні області комп'ютера і в обчислювальні мережі з метою порушення роботи програм, псування файлів і каталогів, створення всіляких перешкод в роботі комп'ютера.
в. Спеціальна системна програма, здатна самовільно приєднуватися до інших програм, створювати свої копії та впроваджувати їх у файли, заподіювати порчу файлів і каталогів, створювати всілякі перешкоди в роботі комп'ютера.
г. Програма, яка спотворює файли комп’ютера та видаляє інформацію про користувача.

8. У функції центру управління ключовою системою не входить?
а. Створення ключів.
б. Створення сертифікатів.
в. Створення алгоритмів електронних цифрових підписів.
г. Управління ключами.

9. Як називається структура служби безпеки Україні, що займається захистом інформації?
а. ФАПСІ.
б. ДСТСЗІ.
в. ЦРУ.
г. МАССАД

10. Який з алгоритмів не відноситься до класу хеш-функцій?
а. MD 5.
б. SHA.
в. MH 4.
г. MD 4.

11. Яке буквене позначення на даний момент має алгоритм по ГОСТ 28147-89 в Україні?
а. ДСТУ ГОСТ 28147: 2009
б. ДСТУ 28147:2010
в. ДСТУ ГОСТ 28147 – 2008
г. ДСТУ 28147-89.

12. Який з алгоритмів не відноситься до класу симетричних криптосистем (з закритим ключем)?
а. RSA.
б. DES.
в. AES.
г. TripleDES.

13. Можливість однозначного доказу належності при відмові відправника/одержувача від раніш переданого/прийнятого повідомлення для симетричних систем
а. Існує
б. Не існує

14. Можливість доказу факту підробки повідомлення у разі компрометації відправника зі сторони одержувача для асиметричних систем
а. Існує
б. Не існує

15. Можливість реалізації моделі взаємної недовіри для симетричних систем
а. Ні
б. Так

Тема 16. Відкритість алгоритмів шифрування/розшифрування для асиметричних систем
а. Так
б. Ні
в. Частково

17. Швидкодія апаратної та програмної реалізації для симетричних систем
а. Співпадає за швидкістю для **асиметричних** систем
б. Є нижчою за швидкістю ніж для **асиметричних** систем
в. Є вищою за швидкістю на 2-3 порядки ніж для **асиметричних** систем

18. Фактор, що зумовлює криптостійкість для асиметричних систем
а. Таємний ключ
б. Нездолання обчислювана проблема
в. Відкритий ключ

19. Можливість розкриття таємного ключа під час його передачі від відправника до одержувача повідомлення для асиметричних систем
а. Існує
б. Не існую

20. Механізм забезпечення цілісності та автентичності повідомлення для симетричних систем
а. Цифровий підпис
б. Формування імітовставки

21. Криптоаналіз методом «дня народження» - це
а. Імовірнісний метод
б. Аналітичний метод

22. Обчислювано-стійкі криптосистеми - це
а. Криптосистеми, що взагалі не можуть бути розкриті за допомогою криптоаналізу навіть за наявних необмежених обчислювано-часових можливостей криптоаналитика
б. Для зламування таких криптосистем потрібні величезні обчислювано-часові можливості для проведенні криптоатаки, що заснована на повному переборі варіантів

23. Запропонована у 1917 році система Вернама є:
а. Безумовно-стійкою (теоретично-недешифруємою);

б. Обчислювано-стійким (гарантованої стійкості);
в. Імовірно-стійким (доказово-стійкі);
г. Обчислювано-нестійким(часової стійкості)

24. Шифрування - це
а. Перестановка та підстановка
б. Постстановка
в. Смислове кодування

25. Вимоги, що пред'являються до шифрів:
а. Низька криптостійкість
б. Простота процедур шифрування и дешифрування
в. Чутливість до найменших помилок

26. Принципи, що реалізуються у шифрах
а. Розсіювання та перемішування
б. Розділення
в. Підмішування

27. Довжина ключа для симетричного блочного шифру DES
а. 256
б. 128
в. 56
г. 32

28. Кількість циклів перетворення даних для симетричного блочного шифру DES
а. 64
б. 16
в. 32

29. **Режим Електронної кодової книги застосовується**
а. У алгоритмах симетричного шифрування
б. У алгоритмах асиметричного шифрування

30. У якому з режимів шифрування з використанням блочних алгоритмів існує можливість розпаралелювання обчислень
а. ECB
б. CBC
в. CFB
г. OFB

31. В якому алгоритмі шифрування застосовується функція Ейлера?
а. RSA
б. DES
в. ГОСТ 28147-89
г. TripleDES

32. Криптостійкість RSA основана на
а. Труднощі факторизації великих чисел
б. Труднощі знаходження дискретного логарифму

33. Основи p та q для алгоритму RSA повинні бути

а. Великими простими числами однакової довжини
б. Взаємно простими числами різної довжини
в. Будь-якими великими числами

34. Ідентифікація користувачів и ресурсів мережі - це:
а.Надання їм унікальних імен
б. Встановлення справжності суб'єктів та об'єктів

35. Процедури ініціалізації включають
а. Процедури рекурсії
б. Процедури аутентифікації
в. Процедури перевірки повноважень

36. Розв'яжіть математичне рівняння (X*4) mod 11=1
а. X=3.
б. X=2.
в. X=5.
г. X=6.

37. До атрибутивних методів встановлення дійсності належать
а. Магнітні карти
б. Банківська картка
в. Відбитки пальців

38. Метод функціонального перетворення для автентифікації - це
а. Введення паролю
б. Обчислення виразу виду X=3+6
в. Вибір паролю з визначеного набору

39. Протоколи автентифікації з нульовою передачею знань були створені для:
а. автентифікації користувача
б. автентифікації інтелектуальних карт

40. Яку процедури передбачає цифровий підпис
а. Постанови
б. Постперевірки
в. Ідентифікації

41. Яку з перерахованої інформації не містить цифровий підпис:
а. дату формування підпису
б. час закінчення дії таємного ключа даного підпису
в. час начала дії секретного ключа даного підпису
г. інформацію о тому, хто підписав документ
д. власне ЦП

42. Хеш-функція –
а. призначена для збільшення якості підписаного документу

б. приймає у якості аргументу повідомлення довільної довжини та повертає хеш-значення фіксованої довжини
в. Значення хеш-функції не залежить від тексту та дозволяє відновити сам документ

43. Безпека інформації – це:
а. Стан збережуваної, оброблюваної чи передаваної інформації
б. Сукупність цілеспрямованих дій та заходів

44. Цілісність інформації – це:
а. Дані спотворені ненавмисно
б. Дані у системі не відрізняються від даних у вихідних документах
в. Дані спотворені навмисно, але не дуже

45. Шкода безпеці – це:
а. Порушення стану захищеності інформації
б. Атака на засоби обробки інформації
в. Пошук та використання тієї чи іншої уразливості

46. Фундаментальна загроза – це:
а. Витік інформації
б. Порушення якості
в. Відмова в використанні мови
г. Використання ресурсів авторизованим суб’єктом

47. Порушення повноважень – це:
а. Загроза проникнення
б. Загроза впровадження
в. Базові загрози

48. Який з алгоритмів не відноситься до класу асиметричних криптосистем (з відкритим ключем)?
а. RSA.
б. DES.
в. DSA.
г El Gamal.

49. Розв’яжіть рівняння (X+12) mod 23=0
а. X=10.
б. X=25
в. X=11.
г. X=12.

50. Який алгоритм шифрування використовує в своїй основі мережа Фейстеля?
а. ГОСТ 28147-89.
б. RSA.
в. DSA.
г. Еліптичні криві.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Євсеєв С.П. Кібербезпека: сучасні технології захисту. / Євсеєв С.П, Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: “Новий Світ- 2000”, 2019. – 678. – Режим доступу: http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf.

2. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування: Монографія. Харків. Видавництво “Форт”. 2012. 870 с.

3. Євсєев С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. “Новий Світ-2000”, 2023. – 657 с.

4. Р.В. Грищук, та Ю. Г. Даник. Основи кібернетичної безпеки: Монографія /; за заг. ред. Ю. Г. Данника. Житомир: ЖНАЕУ, 2016.

5. Євсеєв С.П., Ткачов А.М., Алексієв В.О., Рябуха Ю.М. КІБЕРБЕЗПЕКА: WEB-технології . Навчально-довідковий посібник / С.П. Євсеєв, А.М. Ткачов, В.О. Алексієв, Ю.М. Рябуха – Харків : ХНЕУ ім. С. Кузнеця, – Львів: Видавництво «Новий Світ –2000», 2021. – 390 с.

КРИТЕРІЇ ОЦІНЮВАННЯ ВСТУПНОГО ВИПРОБУВАННЯ, СТРУКТУРА ОЦІНКИ, І ПОРЯДОК ОЦІНЮВАННЯ ПІДГОТОВЛЕННОСТІ ВСТУПНИКІВ

Завдання з кібербезпеки є діагностичним і являє собою тест, що містить 50 питань. Тестові питання вимагають від абітурієнта знання основ з безпеки інформації. За правильну відповідь на одне питання абітурієнт отримує 2 бали.

Підсумкова оцінка фахового вступного випробування з кібербезпеки є сумою балів, отриманих за кожне питання.

Рейтингова оцінка, бали	Оцінка ECTS та її визначення	Національна оцінка	Критерії оцінювання	
			позитивні	негативні
90–100	A	Відмінно	– **глибоке знання** навчального матеріалу, що міститься в **літературних джерелах;** – **вміння аналізувати** явища, які вивчаються, в їхньому взаємозв'язку і розвитку; – **вміння** проводити **теоретичні розрахунки**.	
82–89	B	Добре	– **глибокий рівень знань** в обсязі **обов'язкового матеріалу**; – вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**.	
75–81	C	Добре	– **міцні знання** матеріалу, що вивчається, та його **практичного застосування;** – вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**.	
64–74	D	Задовільно	– знання **основних фундаментальних положень** матеріалу, що вивчається, та їх **практичного застосування**; – вміння розв'язувати прості **практичні задачі.**	
60–63	E	Задовільно	– знання **основних фундаментальних положень** матеріалу, – вміння розв'язувати найпростіші **практичні задачі.**	

Рейтингова оцінка, бали	Оцінка ECTS та її визначення	Національна оцінка	Критерії оцінювання	
			позитивні	негативні
35–59	FX	Незадовільно	–	– незнання **основних фундаментальних положень** навчального матеріалу; – **істотні помилки** у відповідях на запитання.
1-34 (на комісії)	F	Незадовільно	–	– повна **відсутність знань** значної частини навчального матеріалу; – **істотні помилки** у відповідях на запитання; – незнання основних фундаментальних положень.

Переведення позитивної оцінки фахового вступного випробування для вступу на навчання для здобуття ступеня бакалавра на основі молодшого спеціаліста та магістра в шкалу 100-200, згідно Додатку 3 Правил прийому до НТУ «ХПІ» в 2024 році.

ТАБЛИЦЯ

переведення позитивної оцінки вступного випробування замість НМТ та фахового іспиту для вступу на навчання для здобуття ступеня **бакалавра** в шкалу 100–200

Тестовий бал	Бал за шкалою 100-200	Тестовий бал	Бал за шкалою100-200	Тестовий бал	Бал за шкалою 100-200
0	не склав	34	129	68	163
1	не склав	35	130	69	164
2	не склав	36	131	70	165
3	не склав	37	132	71	166
4	не склав	38	133	72	167
5	100	39	134	73	168
6	101	40	135	74	169
7	102	41	136	75	170
8	103	42	137	76	171
9	104	43	138	77	172
10	105	44	139	78	173
11	106	45	140	79	174
12	107	46	141	80	175
13	108	47	142	81	176
14	109	48	143	82	177
15	110	49	144	83	178
16	111	50	145	84	179
17	112	51	146	85	180
18	113	52	147	86	181
19	114	53	148	87	182
20	115	54	149	88	183
21	116	55	150	89	184
22	117	56	151	90	185
23	118	57	152	91	186
24	119	58	153	92	187
25	120	59	154	93	188
26	121	60	155	94	189
27	122	61	156	95	190
28	123	62	157	96	192
29	124	63	158	97	194
30	125	64	159	98	196
31	126	65	160	99	198

Тестовий бал	Бал за шкалою 100-200	Тестовий бал	Бал за шкалою100-200	Тестовий бал	Бал за шкалою 100-200
32	127	66	161	100	200
33	128	67	162		

Схвалено на засіданні вченої ради інституту ННІ комп'ютерних наук та інформаційних технологій.

Протокол № 3 від 19.03.2024 р.

Голова вченої ради інституту _____ Михайло ГОДЛЕВСЬКИЙ

Голова фахової атестаційної комісії _____ Сергій ЄВСЄЄВ