МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАВАТВЕРДЖУЮ
Перший проректор Державного університету інформаційно - комунікаційних технологій

Олександр КОРЧЕНКО
"29" квітня 2024 р.

ПРОГРАМА ДОДАТКОВОГО ВСТУПНОГО ВИПРОБУВАННЯ ЗІ СПЕЦІАЛЬНОСТІ 125 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

для здобуття третього (освітньо-наукового) рівня вищої освіти

Київ – 2024

Розробники:

Завідувач кафедри — Галина ГАЙДУР
Професор кафедри — Андрій КОЖУХІВСЬКИЙ

Гарант:

Директор ННІЗІ — Віталій САВЧЕНКО

Завідувач кафедри ІКБ — Галина ГАЙДУР

Директор ННІЗІ — Віталій САВЧЕНКО

Завідувач відділу організації Проведення підготовки та атестації Аспірантів та докторантів Наукового центру — Юрій ПОКАНЄВИЧ

Директор Наукового центру — Олександр ДРОБИК

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Програма додаткового вступного випробування для здобуття освітньо-наукового ступеня доктора філософії за спеціальністю «125 – Кібербезпека та захист інформації» розроблена на базі освітньо-кваліфікаційного рівня магістра або спеціаліста, здобутого за іншою спеціальністю.

Абітурієнти, які вступають до ДУІКТ на навчання для здобуття освітньо-наукового ступеня доктора філософії на основі освітньо-кваліфікаційного рівня магістра або спеціаліста, здобутого за іншою спеціальністю, попередньо складають додаткове вступне випробування.

Додаткове вступне випробування проводиться з метою перевірки якості загально-професійної й спеціальної підготовки потенційних аспірантів і дозволяє виявити й оцінити готовність вступника до вирішення професійних завдань та до науково-практичної діяльності.

Програма і форма додаткового вступного випробування є єдиною для всіх осіб, які не мають фахової освіти зі спеціальності «125 – кібербезпека та захист інформації».

1. Зміст дисциплін, які виносяться для кандидатів на навчання в аспірантурі за спеціальністю «125 Кібербезпека та захист інформації»:

Прикладна криптологія – математичні основи криптології; симетричні криптосистеми; асиметричні криптосистеми; методи автентифікації інформації; цифровий підпис; криптографічний аналіз.

Захист інформації в інформаційно-комунікаційних системах і мережах - комплекси засобів захисту інформаційно-комунікаційних систем; механізми та засоби захисту операційних систем; механізми та засоби захисту систем управління базами даних; механізми та засоби захисту від потенційно небезпечних програм; механізми та засоби захисту розподілених обчислювальних мереж і середовищ; механізми та засоби захисту програм та електронного документообігу; перспективні напрями розвитку комплексів засобів захисту.

Технічний захист інформації – технічний захист інформації, суб'єкти системи технічного захисту інформації, матеріально-технічна база системи технічного захисту інформації, оцінювання захищеності інформації, інформація з обмеженим доступом, комплекс технічного захисту інформації, об’єкт інформаційної діяльності, комплексна система захисту інформації.

Система управління інформаційною безпекою (СУІБ) – частина загальної системи управління, яка ґрунтується на підході, що враховує ризики інформаційної безпеки як бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

2. Форма додаткового вступного випробування – тест. Складання тесту протягом однієї академічної години.

3. Теми, які виносяться на випробування

Тема 1. Основні поняття криптології.

Тема 2. Основи побудови комплексів засобів захисту для інформаційнотелекомунікаційних систем та мереж.

Тема 3. Основи технічного захисту інформації.

Тема 4. Основи управління інформаційною безпекою

4. Перелік питань та тести додаткового вступного випробування

ТЕСТ

1. Криптографія вивчає:

а) проблеми захисту інформації шляхом приховування каналу її передачі/збереження;

б) захист інформації шляхом блокування технічних каналів витоку;

в) методи захисту інформації шляхом її математичних перетворень за допомогою секретних параметрів - ключів.

2. Зашифрування – це:

а) стискання відкритого тексту в короткий дайджест з використанням секретного алгоритму;

б) перетворення відкритого тексту в шифрований текст із використанням ключів згідно з алгоритмом;

в) математичне перетворення шифрованого тексту в відкритий текст із використанням ключу.

3. Firewall – це:

а) система, що забезпечує регістрацію користувачів, формування матриці та доступ до обчислювальних та інформаційних ресурсів мережі;

б) комплекс апаратних чи програмних засобів, здійснює контроль і фільтрацію мережевих пакетів, що проходять через нього відповідно до заданих правил;

в) головний комп’ютер мережі, виконуючий програмне забезпечення як сервер-посередник;

г) всі відповіді не вірні.

4. Скільки рівнів взаємодії систем реалізовано в моделі OSI?

а) 3;

б) 5;

в) 7;

г) 9;

5. Комплексна система захисту інформації (КСЗІ) – це:

а) сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації;

б) сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС;

в) комп’ютерна система, яка здатна забезпечувати захист оброблюваної інформації від певних загроз;

г) всі відповіді вірні.

6. Технічний захист інформації – це:

а) діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації;

б) сукупність заходів та засобів, призначених для реалізації захисту інформації в інформаційній системі або на об'єкті;

в) розроблення, видання нормативно-правових актів з питань захисту інформації.

7. Об’єкт інформаційної діяльності – це:

а) підрозділ-заявник створення комплексу технічного захисту інформації;

б) будівлі, приміщення, транспортні засоби чи інші інженерно-технічні споруди, функціональне призначення яких передбачає обіг інформації з обмеженим доступом;

в) засоби забезпечення захисту інформації у складі комплексу технічного захисту інформації.

8. До Інформації з обмеженим доступом відноситься: а) конфіденційна інформація;

б) інформація, що становить державну;

в) таємна, службова та конфіденційна інформація.

9. За напрямами здійснення всі заходи управління ІБ підприємства поділяють (оберіть невірну відповідь):

а) нормативно-правові;

б) організаційні;

в) програмні-технічні;

г) стратегічні.

10. Відповідно до процесного підходу формування СУІБ підприємства складається з таких етапів (оберіть невірну відповідь):

а) прогнозування та проектування СУІБ;

б) створення СУІБ;

в) реалізація та впровадження відповідних заходів;

г)оцінка ефективності та продуктивності СУІБ;

д) виконання превентивних і коригуючих дій.

5. Критерії оцінювання додаткового вступного випробування

Програму додаткового вступного випробування (іспиту) зі спеціальності складено на підставі програм рівня вищої освіти магістра зі спеціальності «125 – Кібербезпека та захист інформації» у Державному університеті інформаційно-комунікаційних технологій.

Додаткове вступне випробування зі спеціальності проводиться у письмовій формі. Згідно з діючою в університеті системою комплексної діагностики знань результати складання вступних випробувань оцінюються за рейтинговою 100-бальною шкалою, та двобальною, семибальною шкалою A, B, C, D, E (зараховано), FX, F (не зараховано). Підсумкові оцінки виставляються та вносяться до екзаменаційної відомості. Знання та вміння, продемонстровані вступниками до аспірантури на вступних випробуваннях зі спеціальності, оцінюватимуться за 100-бальною шкалою. Вступники, які наберуть менш як 60 балів, позбавлятимуться права участі в конкурсі. В екзаменаційній відомості в національній та європейській системах оцінювання знань і при переведенні оцінки в систему ECTS викладач керується співвідношеннями, поданими нижче у таблиці

Таблиця

Відповідність підсумкових рейтингових оцінок
у балах оцінкам за національною шкалою та шкалою ECTS

Оцінка в балах	**Оцінка за національною шкалою**	**Оцінка за шкалою ECTS**	
		Оцінка	**Пояснення**
90-100	Відмінно	A	Зараховано
83 – 89	Добре	B	
75 – 82		C	
65 – 74	Задовільно	D	
60 – 64		E	
40 – 59	Незадовільно	FX	Не зараховано
0 – 39		F	

Загальні критерії оцінювання знань:

“A” (90-100) – Вступник виявляє особисті творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування й нахили.

“B” (82-89) – Вступник вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв’язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна.

“C” (75-81) – Вступник вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати

її на практиці; контролювати власну діяльність; виправляти помилки, серед яких є суттєві, добирати аргументи для підтвердження думок.

“D” (64-74) – Вступник відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих.

“E” (60-63) – Вступник володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні.

“FX” (35-59) – Вступник володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.

“F” (1-34) – Вступник володіє матеріалом на рівні елементарного розпізнавання і відтворення окремих фактів, елементів, об’єктів.

При оцінюванні знань і вмінь вступника увага звертається передусім на:

уміння визначати найсуттєвіші проблемні питання, що потребують концептуального вирішення;

наявність нестандартних елементів аналізу та діагностики; різноманітність використаних способів зіставлення інформації;

здатність до комбінування та рекомбінування вихідної інформації; глибину опрацювання проблеми;

адекватність запропонованих заходів виявленим проблемам; наявність чітко визначеної позиції вступника;

аргументованість, переконливість обґрунтування запропонованих рішень;

уміння стисло, послідовно і чітко викласти сутність і результати своїх пропозицій;

наявність посилань на джерела, з яких запозичена будь-яка інформація та дотримання етики цитування;

логічність, конкретність і переконливість та повноту відповідей на запитання;

здатність аргументовано захищати свої технічні пропозиції;

вільне володіння технічною термінологією;

загальний рівень підготовки студента.

На вступному випробуванні оцінюванню підлягають:

- володіння ключовими теоретичними знаннями про об’єкт дисципліни;
- здатність творчо мислити та синтезувати знання;
- уміння використовувати знання для розв’язання практичних завдань;
- точність виконання розрахунків, тощо.

Додаткові бали за наукові та навчальні досягнення вступників до аспірантури нараховує екзаменаційна комісія по прийому вступного іспиту зі спеціальності.

ЛІТЕРАТУРА

1. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект / В.Л. Бурячок, В.Б.Толубко, С.В. Дорошенко: – К.: ДУТ, 2015. – 298 с.

2. Гребенніков В. Комплексні системи захисту інформації. Проектування, впровадження, супровід / В. Гребенніков – «Издательские решения», 2018. – 249 с.
3. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації: підручник. – Вінниця: ВНТУ, 2011 р.
4. ДСТУ 33960-96. Захист інформації. Технічний захист інформації. Основні положення. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38911&cat_id=38836
5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
6. Закон України «Про основні засади забезпечення кібербезпеки України». https://zakon.rada.gov.ua/laws/main/2163-19
7. Ластівка Г.І., Шпатар П.М. Технічний захист інформації в інформаційних та телекомунікаційних системах. Навчальний посібник. Чернівці. Чернівецький національний університет, 2018. – С. 252.
8. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі. http://www.dut.edu.ua/uploads/1_1023_75718671.pdf
9. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.
10. НД ТЗІ 2.7-011-12 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки методики виявлення закладних пристроїв. http://www.dstszi.gov.ua/dsszzi/doccatalog/document%3Fid=103253
11. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС. http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46075
12. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074
13. Указ Президента України «Про положення про технічний захист інформації в Україні» від 27.09.1999 № 1229.

ПОРЯДОК ПРОВЕДЕННЯ ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

Склад предметної комісії визначається додатковим наказом ректора Державного університету інформаційно-комунікаційних технологій «Про створення предметних комісій з приймання вступних іспитів до

аспірантури». Робота комісії та порядок проведення вступного випробування регламентується Правилами прийому до аспірантури для здобуття наукового ступеня доктора філософії у Державному університеті інформаційно-комунікаційних технологій на навчальний рік.

Програму обговорено та схвалено на засіданні кафедри Інформаційної та кібернетичної безпеки.

Протокол № 9 від «02» квітня 2024 р.

Гарант освітньої програми
Голова предметної комісії
Директор Навчально-наукового інституту захисту інформації

доктор технічних наук, професор Віталій САВЧЕНКО