Проєкт

ПРОГРАМА ЄДИНОГО ДЕРЖАВНОГО КВАЛІФІКАЦІЙНОГО ІСПИТУ ЗІ СПЕЦІАЛЬНОСТІ 125 «КІБЕРБЕЗПЕКА» ДЛЯ ПЕРШОГО (БАКАЛАВРСЬКОГО) РІВНЯ ВИЩОЇ ОСВІТИ

Когнітивні рівні охоплення:
Рівень А. Необхідний кваліфікаційний рівень «Знання».
Рівень В. Необхідний кваліфікаційний рівень «Знання», «Розуміння».
Рівень С. Необхідний кваліфікаційний рівень «Знання», «Розуміння», «Застосування».
Рівень D. Необхідний кваліфікаційний рівень «Знання», «Розуміння», «Застосування» та «Аналіз»/»Синтез»/»Оцінка».

№, з/п	Тема та її зміст	Питома вага, %	Рівень
1.	**ЗАКОНОДАВЧА ТА НОРМАТИВНО-ПРАВОВА БАЗА, ДЕРЖАВНІ ТА МІЖНАРОДНІ ВИМОГИ, ПРАКТИКИ І СТАНДАРТИ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ ТА/АБО КІБЕРБЕЗПЕКИ**	**8**	
1.1.	**Законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки.**	**6**	
1.1.1.	ЗУ про інформацію, про науково-технічну інформацію.	1	В
1.1.2.	ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах».	1	В
1.1.3.	ЗУ «Про доступ до публічної інформації».	1	В
1.1.4.	ЗУ «Про державну таємницю».	1	В
1.1.5.	ЗУ «Про основні засади забезпечення кібербезпеки України».	1	В
1.1.6.	Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури».	1	В
1.2.	**Міжнародні стандарти в галузі інформаційної та /або кібербезпеки.**	**2**	
1.2.1.	Регламенти ЄС в галузі кібербезпеки.	1	В
1.2.2.	ДСТУ ISO 27001.	1	В

2.	**ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНІЙ ТА/АБО КІБЕРБЕЗПЕЦІ**	**16**	
2.1.	**Інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці.**	**3**	
2.1.1	Мережева модель OSI. Основні протоколи стеку TCP/IP.	1	B
2.1.2.	Віртуалізація (принципи, гіпервізори).	1	B
2.1.3.	Архітектура комп'ютерів.	1	B
2.2.	**Методи і засоби обробки інформації.**	**5**	
2.2.1.	Алгоритмізація та програмування (без прив'язки до конкретної мови програмування).	1	B
2.2.2.	Основи об'єктно-орієнтованого програмування (Класи, Методи, Перевантаження, Наслідування, Делегати, Узагальнення).	1	B
2.2.3.	Методи сортування та пошуку даних.	1	B
2.2.4.	Кількісна міра інформації.	1	B
2.2.5.	Завадостійкі коди.	1	B
2.3.	**Операційні системи.**	**5**	
2.3.1.	Архітектура операційних систем.	1	B
2.3.2.	Процеси і потоки в операційних системах.	1	B
2.3.3.	Керування пам'яттю в операційних системах.	1	B
2.3.4.	Файлові системи.	1	B
2.3.5.	Захисні механізми операційних систем.	1	B
2.4.	**Моделі безпеки в інформаційній та/або кібербезпеці.**	**3**	
2.4.1.	Модель порушника.	1	C
2.4.2.	Модель загроз.	1	C

2.4.3.	Модель вразливостей.	1	С
3.	**БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ**	**20**	
3.1.	**Захист інформації, що обробляється та зберігається в ІКС.**	**2**	
3.1.1.	Процедури ідентифікації, автентифікації, авторизації користувачів.	1	В
3.1.2.	Резервування інформації та компонентів ІКС.	1	В
3.2.	**Програмні та програмно-апаратні комплекси ЗЗІ.**	**6**	
3.2.1.	Антивіруси, міжмережеві екрани.	2	В
3.2.2.	IPS, IDS.	2	В
3.2.3.	Системи контролю та управління доступом.	2	В
3.3.	**Відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.**	**3**	
3.3.1.	Організаційно-технічні заходи відновлення функціонування ІКС.	1	В
3.3.2.	Журнал аудиту подій.	1	В
3.3.3.	Політики резервного копіювання даних.	1	В
3.4.	**Моніторинг процесів функціонування ІКС.**	**4**	
3.4.1.	Джерела інформації про події та типи подій, що аналізуються в системах моніторінгу.	1	В
3.4.2.	Система візуалізації та управління подіями (SIEM).	2	В
3.4.3.	Аналіз подій.	1	В
3.5.	**Механізми безпеки комп'ютерних мереж.**	**5**	
3.5.1.	Віртуальні приватні мережі (VPN).	2	В
3.5.2.	Протоколи автентифікації RADIUS.	1	В
3.5.3.	Протоколи SSL/TLS.	2	В

4.	**КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ**	**9**	
4.1.	**Проєктування, створення, супровід КСЗІ.**	**2**	
4.1.1.	Проведення аудиту інформаційної безпеки та визначення на основі звіту з аудиту ризиків ІБ.	1	B
4.1.2.	Вибір методів та засобів забезпечення необхідного рівня ІБ.	1	B
4.2.	**Моделі загроз та моделі порушника.**	**5**	
4.2.1.	Загрози цілісності.	1	B
4.2.2.	Загрози доступності.	1	B
4.2.3.	Загрози конфіденційності.	1	B
4.2.4.	Загрози через технічні канали.	1	B
4.2.5.	Загрози через соціальну інженерію.	1	B
4.3.	**Оцінка захищеності інформації в ІКС.**	**2**	
4.3.1.	Концептуальна схема оцінки безпеки інформації.	1	B
4.3.2.	Кількісна та якісна оцінки безпеки інформації.	1	A
5.	**УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА / АБО КІБЕРБЕЗПЕКОЮ**	**20**	
5.1.	**Управління кіберінцидентами.**	**4**	
5.1.1.	Поняття кіберінцидента / кібератаки.	2	A
5.1.2.	Розслідування кіберінцидентів / кібератак.	2	B
5.2.	**Управління ризиками в інформаційній та / або кібербезпеці.**	**4**	
5.2.1.	Ризики інформаційної безпеки.	2	A
5.2.2.	Аналіз та оцінка ризику. Прийняття ризику. Зменшення ризику. Страхування (перекладання) ризику.	2	C
5.3.	**Аудит інформаційної та/або кібербезпеки.**	**8**	

5.3.1.	Етапи проведення аудиту.	2	A
5.3.2.	Аудит на основі аналізу ризиків.	2	B
5.3.3.	Аудит на основі стандартів ІБ.	2	B
5.3.4.	Аудит на основі експериментальних досліджень ІС.	2	B
5.4.	**Забезпечення безперервності бізнес-процесів.**	**4**	
5.4.1.	Поняття бізнес-процесу.	2	B
5.4.2.	Модель бізнес-процесу.	2	B
6.	**КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ**	**13**	
6.1.	**Математичні основи криптографії та стеганографії.**	**2**	
6.1.1.	Модулярні обчислення.		C
6.1.2.	Елементи теорії чисел. Алгоритм Евкліда. Теорема Ейлера. Теореми Ферма. Обчислення у скінченних полях.		C
6.1.3.	Умови стійкості шифрів.		B
6.1.4.	Однонаправлені функції, функції гешування.		B
6.1.5.	Псевдовипадкові послідовності в криптосистемах.		B
6.1.6.	Обчислення в системі чисел з плаваючою точкою.		B
6.2.	**Симетричні криптосистеми.**	**3**	
6.2.1.	Модель симетричної криптосистеми.		B
6.2.2.	Класичні методи шифрування. Шифр Цезаря, Вернама. Квадрат Полібія. Шифр гамування.		C
6.2.3.	Блокові шифри. DES, AES, ГОСТ 28147, DSTU7624.		B
6.2.3.1.	DES		
6.2.3.2.	AES		

6.2.3.3.	ДСТУ ГОСТ 28147-2009		
6.2.3.4.	ДСТУ 7624:2014 (режими роботи, довжина ключів, довжина блоку вхідного тексту, кількість раундів, крипостійкість).		
6.2.4.	Потокові шифри. RC4, STRUMOK.		A
6.2.4.1.	RC4		
6.2.4.2.	ДСТУ 8845:2019 (довжина ключів, крипостійкість).		
6.3.	**Асиметричні криптосистеми.**	**3**	
6.3.1.	Модель асиметричної криптосистеми.		B
6.3.2.	Шифри RSA, EG.		B
6.3.3.	Генерація спільних секретів DH.		C
6.3.4.	Електронний цифровий підпис DSA.		B
6.4.	**Криптографічні протоколи.**	**3**	
6.4.1.	Протоколи захисту мережевого трафіку IPSec.		B
6.4.2.	Протоколи безпечної передачі даних прикладного рівня: https.		B
6.5.	**Цифрова стеганографія.**	**2**	
6.5.1.	Поняття цифрової стеганографії.		B
6.5.2.	Модель стеганосистеми. Основні вимоги до стеганосистеми.		B
6.5.3.	Відкриті, напівзакриті, закриті стеганосистеми.		B
6.5.4.	Поняття ЦВЗ, класифікація.		A
6.5.5.	Метод модифікації найменшого значущого біта.		C
6.5.6.	Атаки на стеганосистеми.		B

7.	**ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ**	**14**	
7.1.	**Технічні канали витоку інформації.**	**10**	
7.1.1.	Акустичний (мовний) канал витоку інформації.	2	В
7.1.2.	Електричний канал витоку інформації.	2	В
7.1.3.	Електромагнітний канал витоку інформації.	2	В
7.1.4.	Оптичний та оптоелектронний канал витоку інформації.	2	В
7.1.5.	Параметричний канал витоку інформації.	2	В
7.2.	**Методи та засоби технічного захисту інформації.**	**4**	
7.2.1.	Пасивні та активні методи і засоби захисту інформації від витоку технічними каналами.	2	В
7.2.2.	Системи відеоспостереження.	2	В