ЗАТВЕРДЖЕНО
Наказом Міністерства
освіти і науки України
від 04 листопада 2022 р. № 980

Програма єдиного державного кваліфікаційного іспиту зі спеціальності «Кібербезпека» на першому (бакалаврському) рівні вищої освіти

Єдиний державний кваліфікаційний іспит за спеціальністю 125 «Кібербезпека» на першому (бакалаврському) рівні вищої освіти (далі – ЄДКІ) є обов'язковим компонентом атестації здобувачів вищої освіти за спеціальністю 125 «Кібербезпека».

Метою ЄДКІ є вимірювання та оцінювання результатів навчання, досягнутих здобувачем освіти відповідно до вимог стандарту вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти, затвердженого наказом Міністерства освіти і науки України від 04 жовтня 2018 року № 1074.

Для успішного складання ЄДКІ майбутній фахівець з кібербезпеки має здобути компетентності, які формуються під час вивчення комплексу обов'язкових освітніх компонент упродовж всього нормативного терміну у закладі вищої освіти. Екзаменований повинен мати достатній рівень знань, умінь та компетентностей у галузі забезпечення інформаційної безпеки і/або кібербезпеки; мати здатності до застосовування отриманих знань у практичних ситуаціях; знати та розуміти предметну область, розуміти професію; вміти виявляти, ставити та вирішувати проблеми у галузі кібербезпеки.

ЄДКІ містить завдання зі стислим зрозумілим описом, що охоплюють сфери законодавчої та нормативно-правової бази забезпечення інформаційної і/або кібербезпеки, управління інформаційною та/або кібербезпекою, криптографічного та технічного захисту інформації, безпеки інформаційно-комунікаційних систем, комплексних систем захисту інформації.

Програма ЄДКІ складається з розділів щодо законодавчої та нормативно-правової бази, державних та міжнародних вимог, практик і стандартів в галузі інформаційної та/або кібербезпеки; інформаційних технологій в інформаційній та/або кібербезпеці; безпеки інформаційно-комунікаційних систем; комплексних систем захисту інформації; управління інформаційною та/або кібербезпекою; криптографічного захисту інформації; технічного захисту інформації.

ЄДКІ проводять за такими принципами: академічна доброчесність; об'єктивність; прозорість і публічність; нетерпимість до корупційних та пов'язаних з корупцією діянь; інтеграція у міжнародний освітній та науковий простір; єдність методики оцінювання результатів.

ЄДКІ проводять у формі зовнішнього незалежного оцінювання відповідно до програми ЄДКІ, використовуючи різні види завдань.

Завдання кваліфікаційного іспиту розробляють відповідно до програми ЄДКІ.

УЗАГАЛЬНЕНА СТРУКТУРА ЄДИНОГО ДЕРЖАВНОГО КВАЛІФІКАЦІЙНОГО ІСПИТУ ЗІ СПЕЦІАЛЬНОСТІ «КІБЕРБЕЗПЕКА» НА ПЕРШОМУ (БАКАЛАВРСЬКОМУ) РІВНІ ВИЩОЇ ОСВІТИ

Найменування розділу	**Питома вага розділу**
Законодавча та нормативно-правова база, державні та міжнародні вимоги, практики і стандарти в галузі інформаційної та/або кібербезпеки	**8-12%**
Інформаційні технології в інформаційній та/або кібербезпеці	**14-18%**
Безпека інформаційно-комунікаційних систем	**15-25%**
Комплексні системи захисту інформації	**8-10%**
Управління інформаційною та/або кібербезпекою	**16-20%**
Криптографічний захист інформації	**11-15%**
Технічний захист інформації	**12-16%**

Когнітивні рівні, необхідні для відповіді на запитання за темою:
Рівень A. Знання.
Рівень B. Знання, розуміння.
Рівень C. Знання, розуміння, застосування.
Рівень D. Знання, розуміння, застосування та аналіз/синтез/оцінка.

ДЕТАЛІЗОВАНА ПРОГРАМА
ЄДИНОГО ДЕРЖАВНОГО КВАЛІФІКАЦІЙНОГО ІСПИТУ ЗІ СПЕЦІАЛЬНОСТІ «КІБЕРБЕЗПЕКА» НА ПЕРШОМУ (БАКАЛАВРСЬКОМУ) РІВНІ ВИЩОЇ ОСВІТИ

Код	Найменування розділу/ підрозділу/ теми	Питома вага, %	Когнітивний рівень
1	2	3	4
1	**ЗАКОНОДАВЧА ТА НОРМАТИВНО-ПРАВОВА БАЗА, ДЕРЖАВНІ ТА МІЖНАРОДНІ ВИМОГИ, ПРАКТИКИ І СТАНДАРТИ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ ТА/АБО КІБЕРБЕЗПЕКИ**	**8-12**	
1.1.	**Законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки**	**6-8**	
1.1.1.	ЗУ «Про інформацію», «Про науково-технічну інформацію»		В
1.1.2.	ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України»		В
1.1.3.	ЗУ «Про державну таємницю». «Про захист персональних даних»		В
1.1.4.	Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»		В
1.1.5.	Державні Стандарти України в галузі інформаційної та/або кібербезпеки ДСТУ 3396.0,1,2-97 ДСТУ ISO/IEC 15408-1:2017		В
1.1.6.	Нормативні документи з технічного захисту інформації НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»		В
1.2.	**Міжнародні стандарти в галузі інформаційної та /або кібербезпеки**	**2,5-3,5**	
1.2.1.	Регламенти ЄС в галузі кібербезпеки Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій»		В
1.2.2.	ISO 27001, ISO 27002, ISO 27003 ISO/IEC 15408- 2, ISO/IEC 15408-3		В

1	2	3	4
2.	**ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНІЙ ТА/АБО КІБЕРБЕЗПЕЦІ**	**14-18**	
2.1.	**Інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці**	**3,5-4,5**	
2.1.1	Мережева модель OSI. Основні протоколи стеку TCP/IP		В
2.1.2.	Віртуалізація (принципи, гіпервізори)		В
2.1.3.	Архітектура комп'ютерів		В
2.2.	**Методи і засоби обробки інформації**	**5-7**	
2.2.1.	Алгоритмізація та програмування (без прив'язки до конкретної мови програмування)		В
2.2.2.	Основи об'єктно-орієнтованого програмування (Класи, Методи, Перевантаження, Наслідування, Узагальнення)		В
2.2.3.	Методи сортування та пошуку даних		В
2.3.	**Операційні системи**	**5-7**	
2.3.1.	Архітектура операційних систем		В
2.3.2.	Процеси і потоки в операційних системах		В
2.3.3.	Керування пам'яттю в операційних системах		В
2.3.4.	Файлові системи		В
2.3.5.	Захисні механізми операційних систем		В
3.	**БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ**	**15-25**	
3.1.	**Захист інформації, що обробляється та зберігається в ІКС**	**1,5-2,5**	
3.1.1.	Процедури ідентифікації, автентифікації, авторизації користувачів		В
3.1.2.	Резервування інформації та компонентів ІКС		В
3.2.	**Програмні та програмно-апаратні комплекси ЗЗІ**	**5-7**	
3.2.1.	Антивіруси, міжмережеві екрани (призначення, архітектура, функції)		В
3.2.2.	IPS, IDS (призначення, архітектура, функції)		В
3.2.3.	Системи контролю та управління доступом в ІКС (Active Directory, ACL)		В
3.3.	**Відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження**	**2,5-3,5**	
3.3.1.	Організаційно-технічні заходи відновлення функціонування ІКС		В
3.3.2.	Журнал аудиту подій		В

1	2	3	4
3.3.3.	Політики резервного копіювання даних		B
3.4.	**Моніторинг процесів функціонування ІКС**	**2,5-3,5**	
3.4.1.	Джерела інформації про події та типи подій, що аналізуються в системах моніторінгу		B
3.4.2.	Система візуалізації та управління подіями (SIEM)		B
3.4.3.	Аналіз подій		B
3.5.	**Механізми безпеки комп'ютерних мереж**	**5-7**	
3.5.1.	Протоколи безпеки на канальному рівні		B
3.5.2.	Протоколи безпеки на мережному рівні (IPSec)		B
3.5.3.	Протоколи безпеки на транспортному/сеансовому рівні (SSL/TLS)		B
3.5.4.	Протоколи безпеки прикладного рівня (HTTPS)		B
3.5.5.	Протоколи автентифікації прикладного рівня (RADIUS)		B
3.5.6.	Віртуальні приватні мережі (VPN)		B
4.	**КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ**	**8-10**	
4.1.	**Проєктування, створення, супровід КСЗІ**	**1,5-2,5**	
4.1.1.	Дослідження середовищ функціонування ІС – середовища користувачів, обчислювальної системи, фізичного середовища, інформаційного середовища та побудова моделі загроз		B
4.1.2.	Вибір методів та засобів забезпечення необхідного рівня ІБ		B
4.2.	**Моделі загроз та моделі порушника**	**4-6**	
4.2.1.	Загрози цілісності		B
4.2.2.	Загрози доступності		B
4.2.3.	Загрози конфіденційності		B
4.2.4.	Загрози через технічні канали		B
4.2.5	Загрози автентичності		B
4.3.	**Оцінка захищеності інформації в ІКС**	**1,5-2,5**	**B**
5.	**УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА / АБО КІБЕРБЕЗПЕКОЮ**	**16-20**	
5.1.	**Управління кіберінцидентами**	**3-5**	
5.1.1.	Поняття кіберінцидента / кібератаки		A
5.1.2.	Розслідування кіберінцидентів / кібератак		B
5.2.	**Управління ризиками в інформаційній та / або кібербезпеці**	**8-12**	
5.2.1.	Ризики інформаційної безпеки	4-6	A
5.2.2.	Аналіз та оцінка ризику. Прийняття ризику. Зменшення ризику. Страхування (перекладання) ризику	4-6	C

1	2	3	4
5.3	**Політика інформаційної безпеки**	**3-5**	
5.3.1	Розробка політик ІБ під час забезпечення бізнес-процесів		B
5.3.2	Дотримання політик ІБ під час забезпечення бізнес-процесів		B
6.	**КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ**	**11-15**	
6.1.	**Математичні основи криптографії та стеганографії**	**1,5-2,5**	
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**	**4-6**	
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, ДСТУ ГОСТ 28147-2009, ДСТУ 7624:2014 (довжина ключів, довжина блоку вхідного тексту, кількість раундів, крипостійкість, режими роботи згідно з ДСТУ ISO/IEC 10116:2019)		B
6.2.4.	Потокові шифри. RC4, STRUMOK. (довжина ключів, крипостійкість)		A
6.3.	**Асиметричні криптосистеми**	**3-5**	
6.3.1.	Модель асиметричної криптосистеми		B
6.3.2.	Шифри RSA, Ель Гамаля (EG)		B
6.3.3.	Генерація спільних секретних ключів Діффі-Хеллмана (DH)		C
6.3.4.	Електронний цифровий підпис DSA		B
6.4.	**Цифрова стеганографія**	**1,5-2,5**	
6.4.1.	Поняття цифрової стеганографії		B
6.4.2.	Модель стеганосистеми. Основні вимоги до стеганосистеми		B
6.4.3.	Відкриті, напівзакриті, закриті стеганосистеми		A
6.4.4.	Поняття ЦВЗ, класифікація		A
6.4.5.	Метод модифікації найменшого значущого біта		B
7.	**ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ**	**12-16**	
7.1.	**Технічні канали витоку інформації**	**5-7**	
7.1.1.	Вібро-акустичний канал витоку інформації		B

1	2	3	4
7.1.2.	Електричний канал витоку інформації		В
7.1.3.	Електромагнітний канал витоку інформації		В
7.1.4.	Оптичний та оптоелектронний канал витоку інформації		В
7.1.5.	Параметричний канал витоку інформації		В
7.2.	**Методи та засоби технічного захисту інформації**	**7-9**	
7.2.1.	Пасивні методи та засоби захисту інформації від витоку технічними каналами		В
7.2.2.	Активні методи та засоби захисту інформації від витоку технічними каналами		В
7.2.3.	Методи пошуку та блокування засобів негласного отримання інформації		В
7.2.4.	Методи та засоби технічного захисту інформації від витоку вібро-акустичними каналами		В
7.2.5.	Методи та засоби технічного захисту інформації від витоку електромагнітними та електричними каналами		В
7.2.6.	Методи та засоби технічного захисту інформації від витоку оптичними та оптоелектронними каналами		В
7.2.7.	Методи та засоби технічного захисту інформації від витоку параметричними каналами		В
7.2.8.	Системи відеоспостереження, охоронних сигналізацій, контролю доступу		В

Генеральний директор директорату
фахової передвищої, вищої освіти Олег ШАРОВ