МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ФАХОВИЙ КОЛЕДЖ ІНЖЕНЕРІЇ, УПРАВЛІННЯ ТА ЗЕМЛЕВПОРЯДКУВАННЯ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

ЗАТВЕРДЖУЮ

Заступник директора з навчально-методичної роботи

_____ **Альона ХЕБДА**

«23» 04 2025 р.

ПРОГРАМА
кваліфікаційного екзамену

Галузь знань: 12 Інформаційні технології
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма: Кібербезпека
Освітньо-професійний ступінь: фаховий молодший бакалавр

Обговорено та схвалено на засіданні циклової комісії:
кібербезпеки, інженерії програмного забезпечення та комп'ютерного дизайну
протокол № 15(7) від «18» квітня 2025 р.
Голова циклової комісії:
_____/ Ганна КРАЛІНА /

2024-2025
навчальний рік

Програму кваліфікаційного екзамену розробили:

Ганна КРАЛІНА
Викладач вищої категорії, голова ЦК кібербезпеки,
інженерії програмного забезпечення та комп'ютерного дизайну

Андрій ПОНОМАРЕНКО
Викладач вищої категорії ЦК кібербезпеки,
інженерії програмного забезпечення та комп'ютерного дизайну

Наталія РЯБЧУК
Викладач-методист вищої категорії, завідувач відділення
Інженерії програмного забезпечення

Програма кваліфікаційного екзамену обговорена та схвалена на засіданні випускової циклової комісії Кібербезпеки, інженерії програмного забезпечення та комп'ютерного дизайну, протокол №15(7) від «18» квітня 2025р.

Голова циклової комісії _____ / Ганна КРАЛІНА/

Програма атестаційного (кваліфікаційного) екзамену обговорена та схвалена на засіданні Науково-методичної ради КІУтЗ КАІ
протокол № 9 від «23» 04 2025р.

Голова НМР _____ / Альона ХЕБДА/

ЗМІСТ

Пояснювальна записка
до кваліфікаційного екзамену

Програма кваліфікаційного екзамену (далі – Програма) розроблена на основі освітньо-професійної програми «Кібербезпека» та відповідного навчального плану підготовки здобувачів фахової передвищої освіти освітньо-професійного ступеня «Фаховий молодший бакалавр» спеціальності 125 «Кібербезпека та захист інформації».

Кваліфікаційний екзамен проводиться за такими принципами:

- академічна доброчесність;
- об'єктивність;
- прозорість і публічність;
- нетерпимість до корупційних та пов'язаних з корупцією діянь.

Метою кваліфікаційного екзамену є вимірювання та оцінювання результатів навчання, досягнутих здобувачем фахової передвищої освіти за підсумками опанування освітньо-професійної програми «Кібербезпека» спеціальності 125 «Кібербезпека та захист інформації», галузі знань 12 «Інформаційні технології».

Для успішного складання кваліфікаційного екзамену майбутній фахівець з кібербезпеки має здобути компетентності, які формуються під час вивчення комплексу усіх обов'язкових освітніх компонент упродовж всього нормативного терміну у закладі фахової передвищої 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. (**більш детально перелік компетентностей здобувачів фахової передвищої освіти та результати навчання викладені в ОПП «Кібербезпека»*)

Програма кваліфікаційного екзамену 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.

Перелік дисциплін, що виносяться на кваліфікаційний екзамен, охоплює усі фахові освітні компоненти обов'язкового типу навчального плану ОПП «Кібербезпека».

Складання екзамену відбувається шляхом письмової відповіді на екзаменаційний білет, кожний з яких містить 3 теоретичні питання (перше питання базового рівня складності, а решта підвищеного рівня) та виконання практичного завдання/задачі, яке складається з двох підзавдань, поєднаних однією спільною темою. Загалом екзамен розрахований на 180 хвилин. З них для письмової відповіді на теоретичні питання відводиться 60 хвилин, а решту часу на виконання практичного завдання.

Кваліфікаційний екзамен містить завдання різного типу та рівня складності, що відповідають програмі та 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.

Кваліфікаційний екзамен є обов'язковим компонентом індивідуального навчального плану здобувача фахової передвищої освіти. Здобувач освіти допускається до складання кваліфікаційного екзамену за умови відсутності в нього академічної заборгованості.

У разі неуспішного складання кваліфікаційного екзамену здобувач освіти вважається таким, що не виконав індивідуальний навчальний план та відраховується із закладу вищої освіти відповідно до пункту 4 частини першої статті 46 Закону України «Про вищу освіту». Таку особу може бути поновлено на навчання за такою самою спеціальністю для однократного повторного складання кваліфікаційного екзамену. Строк, до якого здобувачі освіти можуть повторно скласти кваліфікаційний екзамен встановлено 1 рік.

У разі повторного неуспішного складання кваліфікаційного екзамену особа може бути поновлена на навчання за такою самою спеціальністю для повторного навчання протягом не менше як двох семестрів. Рішення про зарахування, результатів контрольних заходів під час повторного навчання та надання допуску до складання кваліфікаційного екзамену ухвалюється адміністрацією коледжу.

Повторне навчання та складання кваліфікаційного екзамену здійснюється виключно за рахунок коштів фізичних та/або юридичних осіб.

Повторне складання кваліфікаційного екзамену проводиться за програмою та відповідно до умов проведення, що діють на дату його складання.

Для проведення атестації лише у формі кваліфікаційного екзамену створюється ЕК, яка на підставі результатів кваліфікаційного екзамену приймає рішення про присудження кваліфікації «Фаховий молодший бакалавр з кібербезпеки» та видачі відповідного диплома встановленого зразка.

Екзаменаційні матеріали для кваліфікаційного екзамену заслухані та обговорені на засіданні циклової комісії Кібербезпеки, інженерії програмного забезпечення та комп'ютерного дизайну, схвалені на засіданні Науково-методичної ради КІУтЗ КАІ та рекомендовані до використання в якості підсумкової атестації здобувачів фахової передвищої освіти.

Узагальнена структура кваліфікаційного екзамену

зі спеціальності 125 «Кібербезпека та захист інформації»

для освітньо-професійного ступеня фаховий молодший бакалавр

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

кваліфікаційного екзамену
зі спеціальності 125 «Кібербезпека та захист інформації »
ОПП «Кібербезпека» для освітньо-професійного ступеню фаховий молодший бакалавр

Код	Найменування розділу/ підрозділу/ теми	Питома вага, %	Когнітив - ний 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		В
2.2.2.	Основи об'єктно-орієнтованого програмування (класи, об’єкти, методи, перевантаження, наслідування, інкапсуляція)		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 моніторингу		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 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.	Елементи теорії чисел. Алгоритм Евкліда. Теорема Ейлера. Теореми Ферма.		C
6.1.2.	Умови стійкості шифрів		C
6.1.3.	Однонаправлені функції, функції хешування		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

Зразки питань екзаменаційних білетів згідно вище наведеної програми

Законодавча та нормативно-правова база України в галузі інформаційної та/або кібербезпеки:

- Які основні положення Закону України "Про основні засади забезпечення кібербезпеки України"? Наведіть приклади конкретних заходів, які він регулює.

Міжнародні стандарти в галузі інформаційної та/або кібербезпеки:

-Охарактеризуйте стандарт ISO/IEC 27001. Які основні вимоги він висуває до систем управління інформаційною безпекою?

Інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці:

-Які основні функції та можливості надає інструмент Metasploit для проведення тестування на проникнення? Як він використовується в практиці?

*Методи і засоби обробки інформації:

-Які методи забезпечення цілісності даних існують, і як контрольні суми використовуються для виявлення змін у даних?

Операційні системи:

-Які механізми забезпечення контролю доступу реалізовані в операційній системі Linux? Поясніть концепцію списків контролю доступу (ACL) в цій системі.

Захист інформації, що обробляється та зберігається в ІКС:

-Опишіть методи шифрування даних на рівні диска та їх роль у захисті інформації. Наведіть приклади програмного забезпечення, що реалізує такі методи.

Програмні та програмно-апаратні комплекси захисту:

-Як функціонують системи запобігання витокам даних (DLP-системи)? Які основні компоненти і функції включають такі системи?

Відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження:

-Які етапи включає процес відновлення після кібератаки? Розгляньте конкретний приклад плану реагування на інцидент.

Моніторинг процесів функціонування інформаційних комп'ютерних систем:

-Які технології та інструменти використовуються для моніторингу мережевої активності? Розгляньте можливості та особливості системи Splunk.

Механізми безпеки комп'ютерних мереж:

-Які функції виконують міжмережеві екрани (фаєрволи)? Поясніть різницю між статичними і динамічними фаєрволами, надаючи конкретні приклади їх застосування.

Проєктування, створення, супровід комплексних систем захисту інформації:

-Які етапи проєктування комплексної системи захисту інформації (КСЗІ) існують? Поясніть, як здійснюється аналіз загроз та ризиків на початковому етапі.

Оцінка захищеності інформації в інформаційних комп'ютерних системах:

-Як проводиться аудит інформаційної безпеки? Опишіть основні етапи та методи проведення аудиту, надаючи приклади використання інструментів.

Управління кіберінцидентами:

-Які етапи включає процес управління кіберінцидентами? Опишіть, як здійснюється документування інцидентів та які заходи застосовуються для їх аналізу.

Управління ризиками в інформаційній та/або кібербезпеці:

-Які методи кількісної та якісної оцінки ризиків використовуються в інформаційній безпеці? Поясніть концепцію аналізу впливу бізнесу (BIA) і її значення.

Політика інформаційної безпеки:

-Які ключові компоненти повинні бути включені в політику інформаційної безпеки організації? Наведіть приклади конкретних розділів та їх змісту.

Математичні основи криптографії та стеганографії:

-Що таке криптографічні хеш-функції? Поясніть їхні основні властивості та наведіть приклади використання в сучасних інформаційних системах.

Симетричні криптосистеми:

-Опишіть алгоритм AES (Advanced Encryption Standard). Які основні етапи шифрування і розшифрування інформації він включає?

Асиметричні криптосистеми:

-Як працює алгоритм RSA? Опишіть процес генерації ключів, шифрування та розшифрування даних за допомогою RSA.

Цифрова стеганографія:

-Які методи цифрової стеганографії використовуються для приховування інформації в зображеннях? Розгляньте алгоритм LSB (Least Significant Bit) детально.

Технічні канали витоку інформації:

-Які існують технічні канали витоку інформації через електромагнітне випромінювання? Поясніть методи їх виявлення та запобігання.

Методи та засоби технічного захисту інформації:

-Які засоби технічного захисту інформації використовуються для захисту від акустичних атак? Опишіть конкретні методи та обладнання для захисту.

Приклад екзаменаційного білету:

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Фаховий коледж інженерії, управління та землевпорядкування
Державного некомерційного підприємства
«Державний університет «Київський авіаційний інститут»

Галузь знань: 12 Інформаційні технології
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма: Кібербезпека
Освітньо-професійний ступінь: фаховий молодший бакалавр
ЦК Кібербезпеки, інженерії програмного забезпечення та комп'ютерного дизайну

ЕКЗАМЕНАЦІЙНИЙ БІЛЕТ №1

1. **Проаналізуйте методи та засоби захисту інформації від витоку по технічним каналах. Які є шляхи утворення технічних каналів витоку інформації, що обробляється основними технічними засобами та системами?** *(Деталізація запитання: Наведіть класифікацію методів та засобів інформації від витоку по технічним каналах. Наведіть основні різновиди та сутність технічних каналів витоку інформації. Розгляньте діючі нормативні документи, в яких зазначено порядок створення комплексів технічного захисту інформації.)*

2. **Охарактеризуйте основні види атак на стегосистему. Опишіть атаку на основі відомої математичної моделі контейнера або відомої його частини.**
(Деталізація запитання: Опишіть види атак на стегосистему та наведіть основний захист від них. Розгляньте групи атак та коротко опишіть кожну з них. Наведіть приклад використання блокового детектора)

3. **Охарактеризуйте процес авторизації користувачів у системах управління доступом. Як різні моделі авторизації впливають на безпеку системи?**
(Деталізація запитання: У відповіді слід зазначити основні етапи процесу авторизації: перевірка прав доступу, прийняття рішень про надання або обмеження доступу. Моделі авторизації: RBAC (Role-Based Access Control), ABAC (Attribute-Based Access Control), DAC (Discretionary Access Control), MAC (Mandatory Access Control). Вплив різних моделей на безпеку системи: гнучкість і масштабованість RBAC, детальна налаштовуваність ABAC, жорсткість і контроль у MAC. Переваги та обмеження кожної моделі: ефективність управління доступом в великих організаціях (RBAC), складність і витрати на впровадження (ABAC), високий рівень безпеки, але обмежена гнучкість (MAC).)

Практичне завдання/задача:
Дослідження стану кібербезпеки на уявному підприємстві/установі

1. Оцініть потенційні уразливості (за вірогідністю та рівнем небезпеки, враховуючи специфіку установи/підприємства) та обґрунтуйте метод аналізу, який буде використовуватися, наприклад, сканування вразливостей, тестування проникнення, аналіз коду тощо. Задокументуйте вразливості, включаючи: опис вразливості, рівень серйозності, вірогідність, можливі наслідки. Результат надайте у вигляді схеми.
2. Надайте план підготовки до кібератак та реагування на них.

Обговорено та схвалено на засіданні циклової комісії Кібербезпеки, інженерії програмного забезпечення та комп'ютерного дизайну, протокол №___ від «___» _____ 2025 р.

Голова циклової комісії: _____/ Ганна КРАЛІНА /

Рейтингова система оцінювання виконання завдань кваліфікаційного екзамену

Підсумкова рейтингова оцінка з кваліфікаційного екзамену є еквівалентом підсумкової семестрової рейтингової оцінки. Вона визначається, виходячи із 100-бальної шкали, з наступним переведенням до оцінки за національною шкалою та шкалою ECTS (табл.1).

Таблиця 1 Шкала оцінювання підсумків виконання завдань кваліфікаційного екзамену

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS
90 – 100	Відмінно	A
82 – 89	Добре	B
75 – 81		C
67 – 74	Задовільно	D
60 – 66		E
35 – 59	Незадовільно	FX
1 – 34		F

Підсумкова рейтингова оцінка за складання кваліфікаційного екзамену визначається як сума оцінок за виконання завдань теоретичної та практичної частин. Рейтингові оцінки за виконання кожного завдання екзаменаційного білету виставляються в балах з урахуванням відповідних критеріїв (табл. 2,3).

Рейтингова оцінка за виконання теоретичної частини екзаменаційного білету складається з суми балів за виконання її трьох завдань. Рейтингова оцінка за виконання практичної частини екзаменаційного білету складається з суми балів за виконання її двох завдань.

Оцінки за виконання кожної частини екзаменаційного білету визначаються в балах та за національною шкалою відповідно до табл. 4.

Рейтингові оцінки за виконання кожної частини екзаменаційного білету, а також підсумкова рейтингова оцінка, заносяться до Протоколу засідання екзаменаційної комісії. До індивідуального навчального плану здобувача освіти заноситься тільки підсумкова рейтингова оцінка, наприклад, 90/Відм./А.

У випадку відсутності здобувача освіти на кваліфікаційному екзамені з будь-яких причин, або отримання за його підсумками оцінки "Незадовільно" (за національною шкалою), питання подальшого навчання здобувача освіти вирішується в установленому порядку.

Таблиця 2

Оцінювання виконання окремих завдань екзаменаційного білету

Вид навчальної роботи	Max кількість балів	Критерії оцінювання підсумків виконання окремих завдань	Зміст критеріїв оцінювання підсумків виконання окремих завдань	Оцінка в балах
Теоретична частина		Відповідність підсумків виконання суті запропонованого завдання	- відповідає повністю - неповністю відповідає - недостатньо відповідає суті завдання	**4** **3** **1-2**
Виконання завдання №1	**20**			
Виконання завдання №2	**20**	Повнота та ступіть обґрунтованих рішень, обсяг та рівень використаних знань і умінь	- повно та обґрунтовано - недостатньо повно та обґрунтовано - неповно та необгрунтовано	**4** **3** **1-2**
Виконання завдання №3	**20**			
Усього за теоретичну частину	**60**	Наявність елементів творчого, продуктивного мислення, оригінальність способів вирішення професійних та соціально-виробничих завдань	- наявні елементи творчості, оригінальність підходу до вирішення завдання - типове (стандартне) вирішення завдання - відсутність творчості та оригінальності	**4** **3** **1-2**
Практична частина				
Виконання завдання №1	**20**	Вміння аналізувати і оцінювати факти, події, застосовувати певні правила, методи, принципи, закони в конкретних ситуаціях та прогнозувати очікувані результати	- високий рівень - середній рівень - низький рівень	**4** **3** **1-2**
Виконання завдання №2	**20**			
Усього за практичну частину	**40**	Вміння викладати матеріал професійно, логічно, послідовно, з дотриманням вимог ДСТУ	- матеріал викладено достатньо послідовно та логічно - матеріал викладено недостатньо послідовно та логічно - матеріал викладено непослідовно та нелогічно	**4** **3** **1-2**
Усього	**100**			

Таблиця 3 Відповідність рейтингових оцінок за виконання окремих завдань екзаменаційного білету у балах оцінкам за національною шкалою

Оцінка в балах	Оцінка за національною шкалою	Пояснення
18 – 20	Відмінно	Відмінне виконання лише з незначною кількістю помилок
16 – 17	Добре	Виконання вище середнього рівня з кількома помилками
15		У загальному вірне виконання з певною кількістю суттєвих помилок
13 – 14	Задовільно	Непогане виконання, але зі значною кількістю недоліків
12		Виконання задовольняє мінімальним критеріям
менше 12	Незадовільно	Виконання не задовольняє мінімальним критеріям

Таблиця 4 Відповідність рейтингових оцінок за виконання завдань екзаменаційного білету у балах оцінкам за національною шкалою

Теоретична частина	Практична частина	Оцінка за національною шкалою
54 – 60	36 – 40	Відмінно
45 – 53	30 – 35	Добре
36 – 44	24 – 29	Задовільно
менше 36	менше 24	Незадовільно

Таблиця 5 Приклад заповнення протоколу засідання екзаменаційної комісії з проведення кваліфікаційного екзамену

№ пор.	ПІБ. студента	Варіант завдання	Оцінка		
			Частина 1	Частина 2	Підсумкова
			55/Відм.	36/Відм.	91/Відм./A
			36/Задов.	35/Добре	71/Задов./D
			60/Відм.	24/Задов.	84/Добре/B
			44/Задов.	36/Відм.	80/Добре/C

Список рекомендованої літератури*

1. Основи інформаційної безпеки - М.І. Згуровський, О.А. Кузьмін, Видавничий дім "Академперіодика", 2016, 256 с.
2. Кібербезпека: Навчальний посібник - В.М. Горохов, Львівський національний університет імені Івана Франка, 2018, 180 с.
3. Кібербезпека та захист інформації - А. О. Кравчук, В. В. Лук'яненко, Видавничий дім "Кондор", 2019, 320 с.
4. Інформаційна безпека: навчальний посібник - А.Ю. Залуський, С.В. Кривуля, О.І. Волошин, Видавництво Харківського національного університету імені В.Н. Каразіна, 2015, 240 с.
5. Безпека інформаційних систем і технологій: Навчальний посібник - А.О. Баранов, В.А. Ткачук, С.В. Кривуля, Вид-во Харківського національного університету імені В.Н. Каразіна, 2017, 220 с.
6. Security+ Guide to Network Security Fundamentals by Mark Ciampa. Cengage Learning, 2018, 608p.
7. Hacking: The Art of Exploitation by Jon Erickson No Starch Press, 2008, 488
8. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws by Dafydd Stuttard and Marcus Pinto: Wiley, 2011, 560p.
9. Network Security Essentials: Applications and Standards by William Stallings, Pearson, 2016, 480p.
10. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig, No Starch Press, 2012, 800
11. Gray Hat Hacking: The Ethical Hacker's Handbook by Allen Harper, Daniel Regalado, et al. McGraw-Hill Education, 2018, 608p.
12. Computer Security: Principles and Practice by William Stallings and Lawrie Brown, Pearson, 2017, 800p.
13. Cryptography and Network Security: Principles and Practice by William Stallings, Pearson, 2016 (7th edition), 768p.
14. Cryptography: Theory and Practice by Douglas R. Stinson and Maura Paterson, CRC Press, 2018 (4th edition), 598p.
15. Mathematical Cryptography: An Introduction to Provable Security by Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, Springer, 2018, 538p.
16. Computer Security and the Internet: Tools and Jewels by Paul C. van Oorschot, Springer, 2020, 365p.
17. Introduction to Applied Cryptography: Protocols, Algorithms, and Source Code in C by Bruce Schneier and Niels Ferguson, Wiley, 2015, 408p.
18. A Graduate Course in Applied Cryptography by Dan Boneh and Victor Shoup Published online, 2020, 500p.

* *Примітка: Крім зазначеної літератури, рекомендується скористатися усіма переліками основної та додаткової літератури, які рекомендували викладачі по окремих фахових предметах у рамках певної навчальної дисципліни.*

Перелік довідкових джерел інформації, якими дозволяється користуватись під час кваліфікаційного екзамену

1. Законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки

1.1. ЗУ «Про інформацію», «Про науково-технічну інформацію»

1.2. ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України»

1.3. ЗУ «Про державну таємницю». «Про захист персональних даних»

1.4. Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»

1.5. Державні Стандарти України в галузі інформаційної та/або кібербезпеки ДСТУ 3396.0,1,2-97 ДСТУ ISO/IEC 15408-1:2017

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»

2. Міжнародні стандарти в галузі інформаційної та /або кібербезпеки

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»

2.2. ISO 27001, ISO 27002, ISO 27003 ISO/IEC 15408- 2, ISO/IEC 15408-3

3. Г.М. Барабаш, В.М. Кирилич, О.В. Пелюшкевич Збірник-довідник з курсу "Вища математика". Львів: ЛНУ імені Івана Франка, 2019 – 257 с.

Перелік спеціальних програмних засобів, якими дозволяється користуватись під час кваліфікаційного екзамену

1. Антивірусні програми (наприклад Bitdefender, McAfee, Avast)
2. Системи виявлення та запобігання вторгненням (IDS/IPS):
   2.1. Snort: Відкрите програмне забезпечення для виявлення вторгнень.
   2.2. Suricata: Високопродуктивна система IDS/IPS з можливістю аналізу мережевого трафіку.
   2.3. Bro(Zeek): Система моніторингу мережевої безпеки, що дозволяє здійснювати детальний аналіз мережевого трафіку.
3. Платформи для управління інформаційною безпекою (SIEM):
   3.1. Splunk: Платформа для моніторингу, аналізу та візуалізації даних у реальному часі.
   3.2. IBM QRadar: Платформа для моніторингу подій та управління інформаційною безпекою.
   3.3. ArcSight: Платформа від Micro Focus для аналізу безпеки та управління подіями.
4. Інструменти для тестування на проникнення (пентестинг):
   4.1. Metasploit: Популярна платформа для розробки, тестування та експлуатації вразливостей.
   4.2. Nmap: Інструмент для сканування мережевих портів та виявлення мережевих служб.
   4.3. Wireshark: Аналізатор мережевого трафіку, який дозволяє детально досліджувати пакети даних.
   4.4. Burp Suite: Інструмент для тестування безпеки веб-додатків.
5. Інструменти для аналізу вразливостей:
   5.1. Nessus: Відома платформа для сканування вразливостей.
   5.2. OpenVAS: Відкрита платформа для сканування вразливостей та управління.
   5.3. Qualys: Хмарний сервіс для управління вразливостями та перевірки безпеки.
6. Інструменти для моніторингу та аналізу мережевого трафіку:
   6.1. Wireshark: Інструмент для аналізу мережевого трафіку.
   6.2. tcpdump: Командний інструмент для перехоплення і відображення мережевих пакетів.
   6.3. Nagios: Система для моніторингу мережевих пристроїв та сервісів.
7. Інструменти для шифрування та управління ключами:
   7.1. GnuPG: Відкрите програмне забезпечення для шифрування та підписування даних.
   7.2. VeraCrypt: Програма для шифрування дисків та створення захищених томів.
   7.3. OpenSSL: Інструменти та бібліотеки для роботи з криптографією та SSL/TLS.