МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО
Приймальна комісія ДПУ,
від 27.05.2026, протокол № 2
Голова Приймальної комісії
Державного податкового університету
_____ Дмитро СЕРЕБРЯНСЬКИЙ

ПРОГРАМА
ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

при вступі на навчання для здобуття ступеня магістра
на основі здобутого баклавра, магістра (ОКР спеціаліста)
галузі знань К Безпека та оборона
спеціальності К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)

Ірпінь 2026

Розробник:

_____ Альона ГАРБІНСЬКА-РУДЕНКО, к.ю.н., доцент, доцент кафедри фінансового та податкового права

Гарант : _____ Альона ГАРБІНСЬКА-РУДЕНКО, к.ю.н., доцент, доцент кафедри фінансового та податкового права

Розглянуто та схвалено
на засіданні кафедри фінансового та податкового права

протокол № 9/1 від «14» 04 2026 р.

Завідувач кафедри _____ Марина ГЛУХ
(підпис) (П.І.Б.)

ПОЯСНЮВАЛЬНА ЗАПИСКА

Програма фахового вступного випробування при вступі на навчання для здобуття ступеня магістра галузі знань К Безпека та оборона спеціальності К3 Національна безпека (за окремими сферами забезпечення і видами діяльності) розроблена відповідно до Порядку прийому на навчання для здобуття вищої освіти в 2026 році, Правил прийому на навчання для здобуття вищої освіти до Державного податкового університету в 2026 році.

Програма фахового вступного випробування включає матеріал навчальної дисципліни «Правове регулювання національної безпеки». Мета фахового вступного випробування для вступу на здобуття освітнього ступеня магістра: з'ясувати рівень теоретичних знань та практичних навичок вступників, яких вони набули під час навчання за освітньо-кваліфікаційним рівнем бакалавра з метою формування рейтингового списку та конкурсного відбору вступників на навчання за освітньо-кваліфікаційним рівнем магістр. Завдання фахового вступного випробування полягає у тому, щоб оцінити знання та вміння учасників з питань національної безпеки.

Вимоги до здібностей і підготовленості вступників. До участі у фаховому вступному випробуванні допускаються особи, які завершили навчання та здобули диплом бакалавра. Фахове вступне випробування проводиться у формі тестування.

Програма фахового вступного випробування складається з пояснювальної записки, змісту фахового вступного випробування, критеріїв оцінювання результатів фахового вступного випробування, списку рекомендованих джерел.

ЗМІСТ ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

ТЕМА 1. ТЕОРЕТИЧНІ ОСНОВИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ.

1.Сутність понять «безпека» та «національна безпека».
2. Національна безпека як системна характеристика розвитку людини (особи), суспільства, держави.
3. Об'єкти та суб'єкти національної безпеки.
4. Види та складові національної безпеки.
5. Основні принципи національної безпеки.
6. Основні напрями забезпечення національної безпеки держави.
7. Основні завдання забезпечення національної безпеки.
8. Поняття національних інтересів та цінностей, основні характеристики та місце в державній політиці.

ТЕМА 2. СИСТЕМА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

1. Поняття та призначення системи забезпечення національної безпеки.
2. Мета, завдання і функції системи забезпечення національної безпеки.
3. Структура системи забезпечення національної безпеки
4. Основні чинники, що визначають стан національної безпеки.
5.Принципи системи забезпечення національної безпеки та їх характеристика.
6. Нормативно-правова база як основа для функціонування системи національної безпеки.

ТЕМА 3. СИСТЕМА УПРАВЛІННЯ ТА ДЕРЖАВНА ПОЛІТИКА ЩОДО НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

1. Поняття системи управління національною безпекою.
2. Основні ознаки системи управління національною безпекою.
3. Характерні риси системи управління національною безпекою.
4. Структура системи управління національною безпекою України.
5. Сили забезпечення національної безпеки України.
6. Правові основи та принципи державної політики національної безпеки України.

ТЕМА 4. НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

1. Поняття та зміст нормативно-правового забезпечення національної безпеки.
2. Завдання нормативно-правового регулювання національної безпеки.
3. Принципи формування нормативно-правового забезпечення національної безпеки.
4. Основні засоби забезпечення законотворчої діяльності у сфері забезпечення національної безпеки.
5. Недоліки законотворчої діяльності у сфері забезпечення національної безпеки.

ТЕМА 5. КОНЦЕПЦІЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ ТА ОСНОВНІ НОРМАТИВНО-ПРАВОВІ ДОКУМЕНТИ ЗАБЕЗПЕЧЕННЯ РЕГУЛЮВАННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ: ХАРАКТЕРИСТИКА ОСНОВНИХ ПОЛОЖЕНЬ

1. Історичні корені формування Концепції національної безпеки України.
2. Поняття та зміст Концепції національної безпеки України.
3. Класифікація Концепцій національної безпеки.
4. Основні підходи до формування доктрин національної безпеки.
5. Основні нормативно-правові документи забезпечення регулювання національної безпеки України та характеристика їх основних положень.

ТЕМА 6. ДЕМОКРАТИЧНИЙ ЦИВІЛЬНИЙ КОНТРОЛЬ ЗА СЕКТОРОМ БЕЗПЕКИ

1. Суть, суб’єкти, об’єкти, принципи та механізми демократичного цивільного контролю за сектором безпеки.
2. Предмет демократичного цивільного контролю над сектором безпеки і оборони.
3. Система цивільного контролю над Воєнною організацією і правоохоронними органами держави.
4. Демократичний цивільний контроль за сектором безпеки крізь призму європейського досвіду.
5. Державна політика щодо подолання корупції:
5. 1. Поняття «корупція» та чинники, які здійснюють вплив на ефективність протидії корупцію в Україні.
5.2. Правові засади, суб’єкти та механізми протидії корупції в Україні.

ТЕМА 7. ПЛАНУВАННЯ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

1. Мета, принципи і види планування у сфері національної безпеки.
2. Стратегія національної безпеки України.
3. Інші стратегічні документи у сфері національної безпеки та оборони України:
3.1. Стратегія воєнної безпеки України.
3.2. Стратегія громадської безпеки та цивільного захисту України.
3.3. Стратегія розвитку оборонно-промислового комплексу України.
3.4. Стратегія кібербезпеки України.
3.5. Національна розвідувальна програма.
3.6. Державні програми у сферах національної безпеки і оборони.

ТЕМА 8. ВОЄННА БЕЗПЕКА УКРАЇНИ

1. Поняття воєнної безпеки України.
2. Цілі, стратегічна мета, принципи та напрями забезпечення воєнної безпеки України.
3. Формування і забезпечення реалізації державної політики в сфері воєнної

безпеки України.
4. Загрози воєнній безпеці України.
5. Система забезпечення воєнної безпеки України.
6. Глобальні, регіональні та національні аспекти у контексті воєнної безпеки.

ТЕМА 9. ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ

1. Поняття інформаційної безпеки як складової національної безпеки. Об'єкти інформаційної безпеки.
2. Суб'єкти забезпечення інформаційної безпеки України та їх компетенція в цій сфері.
3. Методи забезпечення інформаційної безпеки.
4. Принципи забезпечення інформаційної безпеки.
5. Загрози інформаційній безпеці.
6. Забезпечення національної безпеки в інформаційній сфері.

ТЕМА 10. ОСНОВНІ ЗАСАДИ КІБЕРБЕЗПЕКИ УКРАЇНИ

1. Поняття та основні елементи кібербезпеки. Принципи забезпечення кібербезпеки.
2. Виклики та кіберзагрози у національному кіберпросторі.
3. Пріоритети забезпечення кібербезпеки України та стратегічні цілі.
4. Стратегічні завдання кібербезпеки.
5. Національна система кібербезпеки: засади розбудови.
6. Об'єкти кібербезпеки та кіберзахисту. Основні завдання суб'єктів забезпечення кібербезпеки України.

ТЕМА 11. КРИМІНАЛОГІЧНА БЕЗПЕКА ЯК ОДИН ІЗ БІЛЬШ ВАЖЛИВИХ ВИДІВ, А ТАКОЖ САМОСТІЙНИХ КОМПОНЕНТІВ (СКЛАДОВИХ) НАЦІОНАЛЬНОЇ БЕЗПЕКИ. ЗЛОЧИНИ ПРОТИ ОСНОВ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

1. Поняття, види та мета кримінологічної безпеки.
2. Класифікація рівнів кримінологічної безпеки.
3. Поняття та загальна характеристика злочинів проти основ національної безпеки України
4. Злочини проти основ національної безпеки, їх кваліфікуючі ознаки.
5. Юридичний аналіз окремих складів злочинів проти основ національної безпеки.

ТЕМА 12. ТЕРОРИЗМ ЯК ГЛОБАЛЬНА ЗАГРОЗА МІЖНАРОДНІЙ І НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

1. Тероризм як соціальне явище: поняття та ознаки. Приклади тероризму.
2. Основні принципи боротьби з тероризмом.
3. Види терористичної діяльності.
3. Особливості сучасного тероризму та фактори, які можуть сприяти його розповсюдженню в Україні.
4. Причини виникнення тероризму. Суб'єкти та правові основи боротьби з

тероризмом в Україні.
5. Держава або організація-спонсор тероризму: поняття та приклади.
6. Кримінальна відповідальність за вчинення терористичного акту та за вчинення інших злочинів, що сприяють тероризму.

КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

Фахове вступне випробування проводиться у строки та згідно з Правилами прийому на навчання для здобуття вищої освіти до Державного податкового університету в 2026 році.

Форма проведення – тестова.

Кількість тестових завдань в екзаменаційному білеті –50.

Кожне завдання передбачає чотири варіанти відповіді один із яких правильний.

Тривалість тестування –2 астрономічні години.

Складеним вважається фахове вступне випробування за результатами якого вступник набрав не менше 50% від загальної кількості балів.

Максимальна кількість балів, яку може набрати вступник за результатами фахового вступного випробування, становить 200 балів, правильна відповідь на один тест – 4 бали.

Шкала переведення кількості правильних відповідей у кількість балів, отриманих за результатами фахового вступного випробування за 200 бальною та 2-бальною шкалою

Кількість вірно виконаних тестових завдань	Кількість балів, отриманих за результатами вступного випробування	Еквівалент оцінки за 2-х бальною шкалою
50	200	складено
49	196	
48	192	
47	188	
46	184	
45	180	
44	176	
43	172	
42	168	
41	164	
40	160	
39	156	
38	152	
37	148	
36	144	
35	140	
34	136	
33	132	
32	128	
31	124	
30	120	
29	116	
28	112	
27	108	
26	104	
25	100	

1-24	96	Не складено

ЗРАЗОК ЗАВДАННЯ ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

Міністерство фінансів України
Державний податковий університет

ТЕСТОВІ ЗАВДАННЯ
для проведення фахових вступних випробувань
при вступі на навчання для здобуття ступеня магістра
на основі здобутого магістра (ОКР спеціаліста)
галузі знань К Безпека та оборона
спеціальності К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)

На виконання завдань тесту Вам дається *2 години.*
На кожне завдання пропонується 4 варіанти відповіді. Тільки один варіант відповіді є правильним.
Ніяких виправлень у даних відповідях не допускається.
Вступне тестове завдання з 1 до 50 оцінюється 4-ма балами.

Варіант №____

1) У якому році було підготовлено Перший неофіційний проект Концепції національної безпеки України?

а) до 16 вересня 1991 р.;
б) 19 жовтня 1993 р.;
в) 24 травня 1996 р.;
г) 16 січня 1997 р.

2) Підготовка офіційного проекту Концепції національної безпеки України почалася відповідно до Указу Президента України № 41 від 15 січня 1992 р. групою із …… вчених.

а) п’яти;
б) шести;
в) семи;
г) десяти.

3) На підготовку і затвердження Концепції національної безпеки України було затрачено рівно ….. років?

а) п’ять;
б) шість;
в) сім;
г) девять.

4) Остаточне затвердження Концепції національної безпеки України відбулося:

а) 11 жовтня 1991 р.;

б) 19 жовтня 1993 р.;

в) 24 травня 1996 р.;

г) 16 січня 1997 р.

5) Першим директором Національного інституту стратегічних досліджень, було призначено доктора економічних наук, професора:

а) В.М. Селіванова;

б) О.В. Богомолова;

в) С.І. Пиріжкова;

г) О.Ф. Бєлова.

6) **Захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від воєнних загроз – це:**

а) громадська безпека і порядок;

б) державна безпека;

в) національна безпека України;

г) воєнна безпека.

7) Воєнна безпека – це:

а) захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенційних загроз невоєнного характеру;

б) захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від воєнних загроз;

в) захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз;

г) захищеність життєво важливих для суспільства та особи інтересів, прав і свобод людини і громадянина, забезпечення яких є пріоритетним завданням діяльності сил безпеки, інших державних органів, органів місцевого самоврядування, їх посадових осіб та громадськості, які здійснюють узгоджені заходи щодо реалізації і захисту національних інтересів від впливу загроз.

8) Виділяють два основні концептуальні різні типи воєнної безпеки:

а) оборонний та наступальний;

б) стратегічний та оборонний;

в) оборонний та забезпечувальний;

г) наступальний та захисний.

9) Документ, у якому викладається система поглядів на причини виникнення, сутність і характер сучасних воєнних конфліктів, принципи і шляхи запобігання їх виникненню, підготовку держави до можливого воєнного конфлікту, а також на застосування воєнної сили для захисту державного суверенітету, територіальної цілісності, інших життєво важливих національних інтересів – це:

а) Стратегія громадської безпеки та цивільного захисту України;

б) Воєнна доктрина України;

в) Стратегія воєнної безпеки України;

г) Стратегія національної безпеки України.

10) Стратегія воєнної безпеки України є документом довгострокового планування та її термін дії розрахований на період понад …. років.

а) 5;

б) 10;

в) 15;

г) 25.

11) Інформаційна безпека України – це:

а) стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі;

б) здатність людини, суспільства і держави запобігати та протидіяти цілеспрямованим негативним впливам і несанкціонованому управлінню інформаційними ресурсами із застосуванням телекомунікаційних та інформаційно-комунікаційних систем і мереж;

в) певний стан системи, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах;

г) складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об’єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформацій з обмеженим доступом.

12) Інформаційна безпека – це:

а) складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об’єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформацій з обмеженим доступом;

б) здатність людини, суспільства і держави запобігати та протидіяти цілеспрямованим негативним впливам і несанкціонованому управлінню інформаційними ресурсами із застосуванням телекомунікаційних та

інформаційно-комунікаційних систем і мереж;

в) стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність та недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій;

г) захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

13) Забезпечення інформаційної безпеки – це:

а) здатність людини, суспільства і держави запобігати та протидіяти цілеспрямованим негативним впливам і несанкціонованому управлінню інформаційними ресурсами із застосуванням телекомунікаційних та інформаційно-комунікаційних систем і мереж;

б) сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

в) діяльність, спрямована на запобігання, своєчасне виявлення, припинення чи нейтралізацію реальних і потенційних загроз інформаційній безпеці України;

г) процес застосування заходів безпеки з метою забезпечення конфіденційності, цілісності та доступності комп’ютерних даних.

14) Загрози інформаційній безпеці – це:

а) наявні та потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави в інформаційній сфері;

б) протиправні суспільно небезпечні діяння, які здійснюються з використанням комп’ютерних і телекомунікаційних технологій шляхом порушення конфіденційності, цілісності та доступності комп’ютерних даних і систем, умисного перехоплення комп’ютерних даних технічними засобами, пошкодження, знищення, погіршення, зміни або приховування комп’ютерної інформації, перешкоджання функціонуванню комп’ютерних і телекомунікаційних систем і технологій;

в) навмисна мотивована атака на інформацію, що обробляється комп’ютером, комп’ютерну систему або мережу, яка пов’язана з небезпекою для життя і здоров’я людей або настанням інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування військового конфлікту;

г) протиправні суспільно небезпечні діяння, які здійснюються з використанням комп'ютерних і телекомунікаційних систем і технологій шляхом свідомих та цілеспрямованих посягань на інформаційні ресурси та інформаційну інфраструктуру, що безпосередньо чи опосередковано створюють або створили небезпеку надзвичайних ситуацій, загрози для персоналу, населення і довкілля, передумови для аварій і катастроф техногенного характеру, провокування громадських та військових конфліктів або погрози вчинення таких дій з метою досягнення злочинних цілей.

15) Інформаційна загроза – це:

а) навмисна мотивована атака на інформацію, що обробляється комп'ютером, комп'ютерну систему або мережу, яка пов'язана з небезпекою для життя і здоров'я людей або настанням інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування військового конфлікту;

б) наявні та потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави в інформаційній сфері;

в) протиправні суспільно небезпечні діяння, які здійснюються з використанням комп'ютерних і телекомунікаційних технологій шляхом порушення конфіденційності, цілісності та доступності комп'ютерних даних і систем, умисного перехоплення комп'ютерних даних технічними засобами, пошкодження, знищення, погіршення, зміни або приховування комп'ютерної інформації, перешкоджання функціонуванню комп'ютерних і телекомунікаційних систем і технологій;

г) потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні.

16) Захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі – це:

а) кібероборона;

б) кіберзахист;

в) інформаційна безпека;

г) кібербезпека.

17) Здатність людини, суспільства і держави запобігати та протидіяти цілеспрямованим негативним впливам і несанкціонованому управлінню інформаційними ресурсами із застосуванням телекомунікаційних та інформаційно-комунікаційних систем і мереж – це:

а) кібербезпека;

б) забезпечення інформаційної безпеки;

в) кіберзахист;

г) кібероборона.

18) Кібербезпека – це:

а) сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;

б) дії, спрямовані на підвищення рівня кіберзахисту шляхом нейтралізації кібератак держави-агресора, його систем і мереж, а також джерел походження кіберзагроз та кібератак, які використовуються для завдання шкоди національній безпеці України;

в) захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

г) сукупність організаційних, правових, наукових та технічних заходів, спрямованих на підвищення рівня кіберзахисту держави шляхом здійснення впливу на інформаційні (автоматизовані), електронно-комунікаційні, інформаційно-комунікаційні системи держави-агресора, джерела походження кіберзагроз та кібератак.

19) Кіберзлочинність (комп’ютерна злочинність) – це:

а) протиправні суспільно небезпечні діяння, які здійснюються з використанням комп’ютерних і телекомунікаційних систем і технологій шляхом свідомих та цілеспрямованих посягань на інформаційні ресурси та інформаційну інфраструктуру, що безпосередньо чи опосередковано створюють або створили небезпеку надзвичайних ситуацій, загрози для персоналу, населення і довкілля, передумови для аварій і катастроф техногенного характеру, провокування громадських та військових конфліктів або погрози вчинення таких дій з метою досягнення злочинних цілей;

б) використання комп`ютерних мережевих інструментів для припинення функціонування критичних об’єктів національної інфраструктури (зокрема, енергетичних, транспортних, урядових), або для примусу або залякування уряду або цивільного населення;

в) протиправні суспільно небезпечні діяння, які здійснюються з використанням комп’ютерних і телекомунікаційних технологій шляхом порушення конфіденційності, цілісності та доступності комп’ютерних даних і систем, умисного перехоплення комп’ютерних даних технічними засобами, пошкодження, знищення, погіршення, зміни або приховування комп’ютерної інформації, перешкоджання функціонуванню комп’ютерних і телекомунікаційних систем і технологій;

г) навмисна мотивована атака на інформацію, що обробляється комп'ютером, комп'ютерну систему або мережу, яка пов'язана з небезпекою для життя і здоров'я людей або настанням інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування військового конфлікту.

20) Кібертероризм – це:

а) протиправні суспільно небезпечні діяння, які здійснюються з використанням комп'ютерних і телекомунікаційних технологій шляхом порушення конфіденційності, цілісності та доступності комп'ютерних даних і систем, умисного перехоплення комп'ютерних даних технічними засобами, пошкодження, знищення, погіршення, зміни або приховування комп'ютерної інформації, перешкоджання функціонуванню комп'ютерних і телекомунікаційних систем і технологій;

б) злочини, що вчиняються з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

в) злочинність, пов'язана як з використанням комп'ютерів, так і з використанням інформаційних технологій і глобальних мереж;

г) протиправні суспільно небезпечні діяння, які здійснюються з використанням комп'ютерних і телекомунікаційних систем і технологій шляхом свідомих та цілеспрямованих посягань на інформаційні ресурси та інформаційну інфраструктуру, що безпосередньо чи опосередковано створюють або створили небезпеку надзвичайних ситуацій, загрози для персоналу, населення і довкілля, передумови для аварій і катастроф техногенного характеру, провокування громадських та військових конфліктів або погрози вчинення таких дій з метою досягнення злочинних цілей.

21) Добровільне зайняття громадянином України посади в незаконних судових або правоохоронних органах, створених на тимчасово окупованій території, а також добровільна участь громадянина України в незаконних збройних чи воєнізованих формуваннях, створених на тимчасово окупованій території, та/або в збройних формуваннях держави-агресора чи надання таким формуванням допомоги у веденні бойових дій проти Збройних Сил України та інших військових формувань, утворених відповідно до законів України, добровольчих формувань, що були утворені або самоорганізовувалися для захисту незалежності, суверенітету та територіальної цілісності України – це:

а) пособництво державі-агресору;

б) державна зрада;

в) дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади;

г) колабораційна діяльність.

22) Діяння, умисно вчинене громадянином України на шкоду суверенітетові, територіальній цілісності та недоторканності, обороноздатності, державній, економічній чи інформаційній безпеці України: перехід на бік ворога в період збройного конфлікту, шпигунство,

надання іноземній державі, іноземній організації або їх представникам допомоги в проведенні підривної діяльності проти України – це:

а) колабораційна діяльність;

б) пособництво державі-агресору;

в) державна зрада;

г) диверсія.

23) Публічне заперечення громадянином України здійснення збройної агресії проти України, встановлення та утвердження тимчасової окупації частини території України або публічні заклики громадянином України до підтримки рішень та/або дій держави-агресора, збройних формувань та/або окупаційної адміністрації держави-агресора, до співпраці з державою-агресором, збройними формуваннями та/або окупаційною адміністрацією держави-агресора, до невизнання поширення державного суверенітету України на тимчасово окуповані території України – це:

а) колабораційна діяльність;

б) державна зрада;

в) дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади;

г) пособництво державі-агресору.

24) Передача або збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю, якщо ці дії вчинені іноземцем або особою без громадянства – це:

а) колабораційна діяльність;

б) пособництво державі-агресору;

в) шпигунство;

г) державна зрада.

25) Державна зрада– це:

а) несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану;

б) діяння, умисно вчинене громадянином України на шкоду суверенітетові, територіальній цілісності та недоторканності, обороноздатності, державній, економічній чи інформаційній безпеці України: перехід на бік ворога в період збройного конфлікту, шпигунство, надання іноземній державі, іноземній організації або їх представникам допомоги в проведенні підривної діяльності проти України;

в) передача або збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю, якщо ці дії вчинені іноземцем або особою без громадянства;

г) передача матеріальних ресурсів незаконним збройним чи воєнізованим формуванням, створеним на тимчасово окупованій території,

та/або збройним чи воєнізованим формуванням держави-агресора, та/або провадження господарської діяльності у взаємодії з державою-агресором, незаконними органами влади, створеними на тимчасово окупованій території, у тому числі окупаційною адміністрацією держави-агресора.

26) **Захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від воєнних загроз – це:**

а) громадська безпека і порядок;

б) державна безпека;

в) національна безпека України;

г) воєнна безпека.

27) Воєнна безпека – це:

а) захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенційних загроз невоєнного характеру;

б) захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від воєнних загроз;

в) захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз;

г) захищеність життєво важливих для суспільства та особи інтересів, прав і свобод людини і громадянина, забезпечення яких є пріоритетним завданням діяльності сил безпеки, інших державних органів, органів місцевого самоврядування, їх посадових осіб та громадськості, які здійснюють узгоджені заходи щодо реалізації і захисту національних інтересів від впливу загроз.

28) Виділяють два основні концептуальні різні типи воєнної безпеки:

а) оборонний та наступальний;

б) стратегічний та оборонний;

в) оборонний та забезпечувальний;

г) наступальний та захисний.

29) Документ, у якому викладається система поглядів на причини виникнення, сутність і характер сучасних воєнних конфліктів, принципи і шляхи запобігання їх виникненню, підготовку держави до можливого воєнного конфлікту, а також на застосування воєнної сили для захисту державного суверенітету, територіальної цілісності, інших життєво важливих національних інтересів – це:

а) Стратегія громадської безпеки та цивільного захисту України;

б) Воєнна доктрина України;

в) Стратегія воєнної безпеки України;

г) Стратегія національної безпеки України.

30) Стратегія воєнної безпеки України є документом довгострокового планування та її термін дії розрахований на період понад

…. років.

а) 5;

б) 10;

в) 15;

г) 25.

31) Інформаційна безпека України – це:

а) стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі;

б) здатність людини, суспільства і держави запобігати та протидіяти цілеспрямованим негативним впливам і несанкціонованому управлінню інформаційними ресурсами із застосуванням телекомунікаційних та інформаційно-комунікаційних систем і мереж;

в) певний стан системи, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах;

г) складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об’єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформацій з обмеженим доступом.

32) Суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров’я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей – це:

а) терористичний акт;

б) пособництво державі-агресору;

в) тероризм;

г) колабораційна діяльність.

33) Стійке об’єднання трьох і більше осіб, яке створене з метою здійснення терористичної діяльності, у межах якого здійснено розподіл функцій, встановлено певні правила поведінки, обов’язкові для цих осіб під час підготовки і вчинення терористичних актів.

а) терористична організація;

б) організація-спонсор тероризму;

в) злочинна організація;

г) терористична група.

34) Захищеність об’єктів можливих терористичних посягань від

терористичних загроз – це:

а) антитерористичне забезпечення об’єктів можливих терористичних посягань;

б) антитерористична операція;

в) боротьба з тероризмом;

г) антитерористична безпека держави.

35) Кримінальні правопорушення, що вчиняються з терористичною метою із застосуванням ядерної, хімічної, бактеріологічної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров’я людей речовин, засобів електромагнітної дії, комп’ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об’єктів, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру – це:

а) кібертероризм;

б) терористичний злочин;

в) терористична діяльність;

г) технологічний тероризм.

36) Застосування зброї, вчинення вибуху, підпалу чи інших дій, які створювали небезпеку для життя чи здоров’я людини або заподіяння значної майнової шкоди чи настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об’єднаннями громадян, юридичними особами, міжнародними організаціями, або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста), а також погроза вчинення зазначених дій з тією самою метою – це:

а) пособництво державі-агресору;

б) колабораційна діяльність;

в) тероризм;

г) терористичний акт.

37) У якому році було підготовлено Перший неофіційний проект Концепції національної безпеки України?

а) до 16 вересня 1991 р.;

б) 19 жовтня 1993 р.;

в) 24 травня 1996 р.;

г) 16 січня 1997 р.

38) Підготовка офіційного проекту Концепції національної безпеки України почалася відповідно до Указу Президента України № 41 від 15 січня 1992 р. групою із …… вчених.

а) п’яти;

б) шести;

в) семи;

г) десяти.

39) На підготовку і затвердження Концепції національної безпеки України було затрачено рівно ….. років?

а) п’ять;

б) шість;

в) сім;

г) девять.

40) Остаточне затвердження Концепції національної безпеки України відбулося:

а) 11 жовтня 1991 р.;

б) 19 жовтня 1993 р.;

в) 24 травня 1996 р.;

г) 16 січня 1997 р.

41) Першим директором Національного інституту стратегічних досліджень, було призначено доктора економічних наук, професора:

а) В.М. Селіванова;

б) О.В. Богомолова;

в) С.І. Пиріжкова;

г) О.Ф. Бєлова.

42) Забезпечення інформаційної безпеки – це:

а) здатність людини, суспільства і держави запобігати та протидіяти цілеспрямованим негативним впливам і несанкціонованому управлінню інформаційними ресурсами із застосуванням телекомунікаційних та інформаційно-комунікаційних систем і мереж;

б) сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

в) діяльність, спрямована на запобігання, своєчасне виявлення, припинення чи нейтралізацію реальних і потенційних загроз інформаційній безпеці України;

г) процес застосування заходів безпеки з метою забезпечення конфіденційності, цілісності та доступності комп’ютерних даних.

43) Загрози інформаційній безпеці – це:

а) наявні та потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави в інформаційній сфері;

б) протиправні суспільно небезпечні діяння, які здійснюються з використанням комп’ютерних і телекомунікаційних технологій шляхом порушення конфіденційності, цілісності та доступності комп’ютерних даних і систем, умисного перехоплення комп’ютерних даних технічними засобами,

пошкодження, знищення, погіршення, зміни або приховування комп'ютерної інформації, перешкоджання функціонуванню комп'ютерних і телекомунікаційних систем і технологій;

в) навмисна мотивована атака на інформацію, що обробляється комп'ютером, комп'ютерну систему або мережу, яка пов'язана з небезпекою для життя і здоров'я людей або настанням інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування військового конфлікту;

г) протиправні суспільно небезпечні діяння, які здійснюються з використанням комп'ютерних і телекомунікаційних систем і технологій шляхом свідомих та цілеспрямованих посягань на інформаційні ресурси та інформаційну інфраструктуру, що безпосередньо чи опосередковано створюють або створили небезпеку надзвичайних ситуацій, загрози для персоналу, населення і довкілля, передумови для аварій і катастроф техногенного характеру, провокування громадських та військових конфліктів або погрози вчинення таких дій з метою досягнення злочинних цілей.

44) Інформаційна загроза – це:

а) навмисна мотивована атака на інформацію, що обробляється комп'ютером, комп'ютерну систему або мережу, яка пов'язана з небезпекою для життя і здоров'я людей або настанням інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування військового конфлікту;

б) наявні та потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави в інформаційній сфері;

в) протиправні суспільно небезпечні діяння, які здійснюються з використанням комп'ютерних і телекомунікаційних технологій шляхом порушення конфіденційності, цілісності та доступності комп'ютерних даних і систем, умисного перехоплення комп'ютерних даних технічними засобами, пошкодження, знищення, погіршення, зміни або приховування комп'ютерної інформації, перешкоджання функціонуванню комп'ютерних і телекомунікаційних систем і технологій;

г) потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні.

45) Захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі – це:

а) кібероборона;

б) кіберзахист;

в) інформаційна безпека;

г) кібербезпека.

46) Здатність людини, суспільства і держави запобігати та протидіяти цілеспрямованим негативним впливам і несанкціонованому управлінню інформаційними ресурсами із застосуванням телекомунікаційних та інформаційно-комунікаційних систем і мереж – це:

а) кібербезпека;

б) забезпечення інформаційної безпеки;

в) кіберзахист;

г) кібероборона.

47) Суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей – це:

а) терористичний акт;

б) пособництво державі-агресору;

в) тероризм;

г) колабораційна діяльність.

48) Стійке об'єднання трьох і більше осіб, яке створене з метою здійснення терористичної діяльності, у межах якого здійснено розподіл функцій, встановлено певні правила поведінки, обов'язкові для цих осіб під час підготовки і вчинення терористичних актів.

а) терористична організація;

б) організація-спонсор тероризму;

в) злочинна організація;

г) терористична група.

49) Захищеність об'єктів можливих терористичних посягань від терористичних загроз – це:

а) антитерористичне забезпечення об'єктів можливих терористичних посягань;

б) антитерористична операція;

в) боротьба з тероризмом;

г) антитерористична безпека держави.

50) Кримінальні правопорушення, що вчиняються з терористичною метою із застосуванням ядерної, хімічної, бактеріологічної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров'я людей речовин, засобів електромагнітної дії, комп'ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об'єктів, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для

персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру – це:

а) кібертероризм;
б) терористичний злочин;
в) терористична діяльність;
г) технологічний тероризм.

Голова фахової атестаційної комісії **Альона ГАРБІНСЬКА-РУДЕНКО**

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19
2. Про правовий режим воєнного стану : Закон України від 12 трав. 2015 р. № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19
3. Про санкції : Закон України від 14 серп. 2014 р. № 1644-VII. URL: https://zakon.rada.gov.ua/laws/show/1644-18
4. Стратегія національної безпеки України : Указ Президента України від 14 верес. 2020 р. № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037
5. Про рішення Ради національної безпеки і оборони України від 11 черв. 2023 р.: Указ Президента України № 321/2023. URL: https://www.president.gov.ua/documents/3212023
6. Боднарчук О. Г., Боднарчук О. І., Глух М. В., Гарбінська-Руденко А. В. Правове регулювання національної безпеки : навч. посіб. Ірпінь: Державний податковий університет, 2024. 202 с.
7. Ситник Г. П. Організаційно-правові засади забезпечення воєнної безпеки України : курс лекцій. Київ : САК Лтд., 2023. 112 с.
8. Литвиненко О. В. Національна безпека України: навч. посіб. Київ: Юрінком Інтер, 2023. 320 с.
9. Теліпко В. М. Державна політика у сфері національної безпеки: навч. посіб. Київ : Центр учбової літератури, 2024. 256 с.
10. Коваль М. В. Публічне управління у сфері національної безпеки: навч. посіб. Львів : ЛьвДУВС, 2023. 280 с.
11. Гаврилюк Р. О. Правове забезпечення національної безпеки України: монографія. Київ : Юрінком Інтер, 2023. 356 с.
12. Бандурка О. М. Національна безпека в умовах воєнного стану: монографія. Харків : Право, 2024. 300 с.
13. Голосніченко І. П. Інституційні засади забезпечення національної безпеки : монографія. Київ : НАВС, 2023. 280 с.
14. Ківалов С. В. Правові механізми протидії загрозам національній безпеці: монографія. Одеса : Фенікс, 2025. 340 с.
15. Бесчастний В. М., Львова О. Тлумачення конституційних положень як чинник забезпечення національної безпеки в умовах війни в Україні: монографія. Київ : Конституційний Суд України, 2024. 180 с.
16. Філіппова В. Д. Стратегічний механізм забезпечення національної безпеки. *Вісник Херсонського національного технічного університету*. 2024. № 2 (89). С. 45–52. URL: https://journals.kntu.kherson.ua/index.php/visnyk_kntu/article/view/828
17. Степановський В. С. Спільна безпекова політика та національна безпека в країнах ЄС. *Аналітично-порівняльне правознавство*. 2025. № 1. С. 112–118. URL: https://journal-app.uzhnu.edu.ua/article/view/327665
18. Шестопалов Р. М. Національна безпека як об’єкт кримінально-правової

охорони держави. *Вісник асоціації кримінального права України*. 2025. № 1 (15). С. 23–31. URL: https://vakp.nlu.edu.ua/article/view/339578

19. Шевчук М. О. Особливості правового забезпечення інформаційної безпеки в Україні. *Правовий часопис Донбасу*. 2024. № 1 (78). С. 67–73. URL: https://ljd.dnuvs.ukr.education/index.php/ljd/article/view/28

20. Каменський Д. В., Вознюк А. А. Національна та економічна безпека: співвідношення концепцій. *Національна безпека: право та економіка*. 2024. № 2. С. 14–21. URL: https://security-journal.nasbu.edu.ua/index.php/nbpe/article/view/8

21. Ромців О. І. Забезпечення національної безпеки України в умовах геополітичних викликів. *Аналітично-порівняльне правознавство*. 2025. № 2. С. 95–101. URL: https://journal-app.uzhnu.edu.ua/article/view/337856

22. Леоненко Н. А., Сухачов М. Р. Державна політика забезпечення безпекового середовища функціонування критичної інфраструктури в Україні. *Вісник Національного університету цивільного захисту України. Серія: Державне управління*. 2023. № 2 (18). С. 162–170. URL: https://repositsc.nuczu.edu.ua/bitstream/123456789/19347/1/LeonenkoSukhachov.pdf

23. Помаза-Пономаренко А. Л., Тарадуда Д. В., Леоненко Н. А., Порока С. Г., Сухачов М. Р. Ensuring the safety of citizens in times of war: aspects of civil defense organization. *AD ALTA: Journal of Interdisciplinary Research*. 2024. Vol. 14, Issue 1. P. 216–220. URL: https://www.magnanimitas.cz/ADALTA/140139/papers/K_10.pdf