

Міністерство освіти і науки України  
Прикарпатський національний університет імені Василя Стефаника  
Навчально-науковий юридичний інститут  
кафедра правоохоронної діяльності

## **ПРОГРАМОВІ ВИМОГИ**

для проведення заліку зі студентами  
денної та заочної форм навчання (ОР «Бакалавр»)

**з навчальної дисципліни «Державна політика в сфері кіберзахисту»**

Галузь знань 26 «Цивільна безпека»  
Спеціальність 262 «Правоохоронна діяльність»

Програмові вимоги для проведення екзамену затверджено  
на засіданні кафедри правоохоронної діяльності

**Протокол № 5 від 21.01.2025 року**

викладач кафедри політики у сфері боротьби зі  
злочинністю та кримінального права, доктор філософії      Максим ЯЦИНА

**Івано-Франківськ-2025**

## Перелік питань, що виносяться для проведення заліку

1. Кіберпростір: поняття та особливості.
2. Поняття та сутність національної безпеки України.
3. Інформаційна безпека у системі національної безпеки.
4. Кібербезпека: поняття та зміст.
5. Поняття «кіберзахисту».
6. Сучасний стан нормативно-правового забезпечення кібербезпеки.
7. Закон України «Про національну безпеку України».
8. Стратегія національної безпеки України.
9. Закон України «Про основні засади забезпечення кібербезпеки України».
10. Стратегія кібербезпеки України.
11. Поняття та види загроз безпеці держави у кіберпросторі.
12. Чинники та передумови формування загроз кібербезпеці.
13. Основні об'єкти кіберзахисту України.
14. Комп'ютерна злочинність (кіберзлочинність): поняття, ознаки та тенденції розвитку.
15. Детермінанти кіберзлочинності.
16. Видова характеристика кіберзлочинності та її структура.
17. Місце кіберзлочинності у структурі системи злочинності, її показники.
18. Способи здійснення комп'ютерних злочинів у кіберпросторі.
19. Кібертероризм: поняття та ознаки.
20. Основні форми кібертероризму.
21. Співвідношення понять «кібертероризм» та «тероризм» (спільне та відмінне).
22. Юридичний склад кібертероризму.
23. Міжнародно-правовий досвід запобігання та протидії кібертероризму.
24. Державна політика кібербезпеки України.
25. Національна система кібербезпеки України.
26. Інтеграція України до міжнародно-правового регулювання кіберпростору.
27. Державні суб'єкти забезпечення кібербезпеки України.
28. Державна служба спеціального зв'язку та захисту інформації України.
29. Національний координаційний центр кібербезпеки при РНБО.
30. Національна поліція України (Департамент кіберполіції).
31. Роль розвідувальних органів у забезпеченні кібербезпеки України.
32. Приватний сектор як суб'єкт забезпечення кібербезпеки України.

33. Поняття, види та особливості юридичної відповідальності за кіберзлочини.
34. Кримінальна відповідальність за кіберзлочини: загальна характеристика та основні положення.
35. Адміністративна відповідальність за правопорушення у сфері кібербезпеки.
36. Цивільно-правова відповідальність за кіберзлочини: механізми відшкодування завданої шкоди.
37. Міжнародно-правове регулювання відповідальності за кіберзлочини.
38. Організаційно-правове регулювання кібербезпеки НАТО.
39. Правові засади забезпечення кібербезпеки ЄС.
40. Конвенція Ради Європи про кіберзлочинність: основні положення.