**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**

**Харківський національний**
**університет внутрішніх справ**

**Факультет № 6**

**Кафедра кібербезпеки та DATA-технологій**

# ПРОГРАМА

навчальної дисципліни
**«Державне управління у сфері кібербезпеки»**
**вибіркових компонент освітньої програми**
**другого (магістерського) рівня вищої освіти**

**125 «Кібербезпека» (Безпека інформаційних та комунікаційних систем)**

Харків 2022

**ЗАТВЕРДЖЕНО**
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 28.11.2022 № 11

**СХВАЛЕНО**
Вченою радою
факультету № 6
Протокол від 23.11.2022 № 9

**ПОГОДЖЕНО**
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 25.11.2022 № 11

Розглянуто на засіданні кафедри кібербезпеки та DATA-технологій факультету № 6 (протокол від 18.11.2022 № 12).

**Розробники:**
Доцент кафедри кібербезпеки та DATA-технологій факультету № 6, кандидат наук з державного управління, доцент Онищенко Ю.М.

**Рецензенти:**
завідувач кафедри інформаційних управляючих систем Харківського національного університету радіоелектроніки, доктор технічних наук, професор Петров К.Е.
доцент кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ к.т.н., доцент Світличний В.А.

## ПОЯСНЮВАЛЬНА ЗАПИСКА

Програма вибіркової навчальної дисципліни складена відповідно до освітньої програми другого (магістерського) рівня вищої освіти 125 «Кібербезпека» (Безпека інформаційних та комунікаційних систем).

**Предметом** вивчення навчальної дисципліни є державні механізми запобігання і протидії кіберзлочинності в умовах глобалізації.

**Міждисциплінарні зв'язки.** Навчальна дисципліна спирається на дисципліни: «Інформаційні технології», «Кібербезпека», «Управління та організація в сфері інформаційної безпеки» та формує фахові компетентності в галузі кібербезпеки.

Програма навчальної дисципліни складається з таких тем:

1. Теоретичні засади запобігання і протидії проявам кіберзлочинності.
2. Державне управління у сфері запобігання і протидії кіберзлочинності в Україні.
3. Державні механізми запобігання і протидії кіберзлочинності.

### 1. Мета та завдання навчальної дисципліни

1.1. Метою викладання навчальної дисципліни «Державне управління у сфері кібербезпеки» є формування знань щодо державних механізмів запобігання і протидії кіберзлочинності в Україні в умовах глобалізації світового інформаційного простору.

1.2. Основними завданнями вивчення дисципліни є:

- ознайомлення із сучасними підходами забезпечення ефективного державного управління та структурою державного механізму взаємодії у сфері боротьби з кіберзлочинністю в Україні;
- формування навичок аналізу державних механізмів запобігання і протидії кіберзлочинності в умовах глобалізації.

1.3. Згідно з освітньою програмою здобувачі вищої освіти повинні:

**знати:** теоретичні засади запобігання і протидії проявам кіберзлочинності; сучасний стан державного управління у сфері запобігання і протидії кіберзлочинності в Україні; шляхи удосконалення державних механізмів запобігання і

протидії кіберзлочинності.

**вміти:** аналізувати державні механізми запобігання і протидії кіберзлочинності в умовах глобалізації.

1.4. Форма підсумкового контролю залік.

На вивчення навчальної дисципліни відводиться 120 годин / 4 кредити ECTS.

1.5 Програмні компетентності:

| **Програмні компетентності, які формуються при вивченні навчальної дисципліни:** | | |
|---|---|---|
| **Інтегральна компетентність** | Здатність самостійно досліджувати і розроблювати комплексні системи забезпечення кібербезпеки викладати і здійснювати аналітичну діяльність в області кібербезпеки | |
| **Загальні компетентності (ЗК)** | ЗК 1 | Здатність до абстрактного, логічного, критичного мислення та встановлення взаємозв'язків між явищами та процесами |
| **Фахові компетентності спеціальності (ФК)** | ФК 1 | Здатність використовувати актуальні підходи та технології забезпечення кібербезпеки у поєднанні із потрібними програмними інструментами аналізу кіберзагроз |

## 2. Короткий опис змісту навчальної дисципліни

### Тема № 1. Теоретичні засади запобігання і протидії проявам кіберзлочинності

Понятійно-категоріальний апарат: співвідношення основних понять у сфері боротьби з кіберзлочинністю. Взаємозв'язок злочинності та інформаційних технологій. Запобігання та протидія кіберзлочинності як об'єкт державного управління в умовах глобалізації. Зарубіжний досвід реалізації державних механізмів у галузі запобігання та боротьби з кіберзлочинністю.

### Тема № 2. Державне управління у сфері запобігання і протидії кіберзлочинності в Україні

Особливості організаційних та нормативно-правових засад боротьби з кіберзлочинністю. Проблеми державного управління у сфері запобігання проявам кіберзлочинності. Напрями вирішення проблеми проявів кіберзлочинності.

**Тема № 3. Державні механізми запобігання і протидії кіберзлочинності в умовах воєнного стану**

Підходи і моделі реформування державних механізмів боротьби з кіберзлочинністю. Напрями впорядкування правового підґрунтя діяльності та взаємовідносин в організаційно-функціональній структурі суб'єктів протидії кіберзлочинності. Система запобігання кіберзлочинності в Україні.

## 3. Рекомендована література (основна, допоміжна), інформаційні ресурси в інтернеті

### 3.1 Основна:


1. Про основні засади забезпечення кібербезпеки України: закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України»/Верховна Рада України. URL:http://zakon3.rada.gov.ua/laws/show/2163-19 (дата звернення: 26.10.2022).
2. Про кіберзлочинність: конвенція Ради Європи від 07.09.2005 ратифікована Верховною Радою України 07.09.2005 URL:http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 26.10.2022).
3. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 р. № 96/2016. – URL:http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 26.10.2022).
4. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.2021 № 447/2021. – URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 26.10.2022).
5. Онищенко Ю.М. Державні механізми запобігання і протидії кіберзлочинності в умовах глобалізації. дис. канд. наук з держ. управ: 25.00.02. Харків, 2015. 200 с.
6. Кравцова М.О. Запобігання кіберзлочинності в Україні: монографія / М.О. Кравцова, О.М. Литвинов / [За загальною редакцією д-ра юрид. наук, проф. О.М. Литвинова]. – Харків: Панов, 2016. – 212 с.

7. Орлов О.В. Совершенствование механизмов реализации государственной политики в сфере борьбы с киберпреступностью в Украине / О.В. Орлов, Ю.М. Онищенко // Публичное управление: научный журнал Академии государственного управления Республіки Армения. – 2014. – № 1-2/2014. – 42 с.
8. Гуцалюк М. Сучасні тенденції організованої кіберзлочинності. Інформація і право. № 1(28)/2019. С. 118-128.

**3.2 Додаткова:**

9. Про національну безпеку України: Закон України від 21.06.2018 № 2469. Відомості Верховної Ради. 2018. № 31. Ст. 241.
10. Про рішення Ради національної безпеки і оборони України від 16 травня 2019 року "Про організацію планування в секторі безпеки і оборони України": Указ Президента України від 16.05.2019 № 225/2019. URL: https://zakon.rada.gov.ua/laws/show/225/2019#n2 (дата звернення: 26.10.2022).
11. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України": Указ Президента України від 14.09.2020 №392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 26.10.2022).
12. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом: Постанова Кабінету Міністрів України від 11.11.2020 № 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-п#Text (дата звернення: 26.10.2022).
13. Положення про Департамент кіберполіції Національної поліції України, затверджене наказом Національної поліції України № 85: від 10.11.2015. К.: Національна поліція України, 2015. 9 с.
14. Про ратифікацію Угоди між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво: Закон України від 12.07.2017 № 2129. URL: https://zakon.rada.gov.ua/laws/show/2129-19#n2 (дата звернення: 26.10.2022).
15. Internet Organised Crime Threat Assessment (IOCTA). URL: https://www.europol.europa.eu/ activities-services/main-reports/internet-organised-crime-threat-assessment (дата звернення: 26.10.2022).

**3.3 Інформаційні ресурси в інтернеті:**

16. http://www.niss.gov.ua/
17. https://cyberpolice.gov.ua/
18. https://cip.gov.ua/ua
19. https://cert.gov.ua/
20. https://ssu.gov.ua/
21. https://www.president.gov.ua/

## 4. Засоби оцінювання здобувачів вищої освіти

З метою діагностики успішності навчання використовуються:

- поточне письмове опитування на семінарських заняттях по тематиці лекцій, що були прослухані;
- тематичні письмові самостійні роботи у формі рефератів;
- контроль за тестовими завданнями;
- підсумкове тестування з усієї дисципліни – залік.

### Питання, або тестові завдання, які виносяться на складання підсумкового контролю (залік)

1. Аспекти взаємозв'язку злочинності та інформаційних технологій.
2. Співвідношення глобалізації інформаційних процесів та кіберзлочинності.
3. Позитивні та негативні наслідки поширення комп'ютерних технологій.
4. Темпи розвитку всесвітньої мережі Інтернет.
5. Превентивні можливості глобальних інформаційних мереж.
6. Транснаціональна злочинність: визначення, причини виникнення, тенденції.
7. Що належить до комп'ютерних злочинів згідно з міжнародними класифікаторами
8. Напрями використання кібертерористами глобальної мережі Інтернет.
9. Соціально-психологічний аспект глобальної мережі Інтернет.
10. Незаконний контент у глобальній мережі Інтернет: види, способи розповсюдження.
11. Напрями використання інформаційних технологій органами державної влади.
12. Напрями використання інформаційних технологій правоохоронними органами США.

13. Напрями використання інформаційних технологій правоохоронними органами України.
14. Наведіть характеристику дефініції кіберпростір.
15. Ознаки кіберпростору.
16. Шляхи вирішення питання щодо регулювання мережі Інтернет і, відповідно, визначення повноважень держави в цій сфері.
17. Співвідношення понять “кіберзлочинність” і “комп'ютерні злочини”.
18. Як Конвенція Ради Європи «Про кіберзлочинність» визначає види комп'ютерних злочинів “у чистому вигляді”?
19. Як Конвенція Ради Європи «Про кіберзлочинність» визначає скоювані за допомогою комп'ютера (computer-facilitated) злочини?
20. Характеристика дефініції кіберзлочинність.
21. Наведіть визначення поняття кіберпростір.
22. Наведіть визначення поняття кіберзлочин.
23. Що складає правову основу забезпечення кібербезпеки України?
24. Який Закон України визначає засади забезпечення кібербезпеки України?
25. Наведіть визначення поняття кібербезпеки.
26. Що належить до об’єктів кібербезпеки?
27. Наведіть визначення поняття кіберзахисту.
28. Що належить до об’єктів кіберзахисту?
29. Визначення терміну об’єкт критичної інформаційної інфраструктури.
30. Визначення терміну система управління технологічними процесами.
31. Які об’єкти можуть бути віднесені до критичної інфраструктури?
32. Надайте визначення та характеристику поняття кіберпростір.
33. Надайте визначення та характеристику поняття інцидент кібербезпеки (кіберінцидент).
34. Надайте визначення та характеристику поняття кібератака.
35. Надайте визначення та характеристику поняття кіберзагроза.
36. Надайте визначення та характеристику поняття кібероборона.
37. Надайте визначення та характеристику поняття кіберзагроз.
38. Визначення терміну кіберрозвідка.
39. Визначення терміну кібершпигунство.

40. Визначення терміну кібертероризм.
41. Хто здійснює координацію діяльності у сфері кібербезпеки в Україні?
42. Хто забезпечує формування та реалізацію державної політики у сфері кібербезпеки в Україні?
43. Суб'єкти забезпечення кібербезпеки.
44. Завдання суб'єктів національної системи кібербезпеки.
45. Надайте визначення та характеристику поняття Національна телекомунікаційна мережа.
46. Надайте визначення та характеристику поняття Національні електронні інформаційні ресурси.
47. Надайте визначення та характеристику поняття системи електронних комунікацій.
48. Наведіть основні завдання Департаменту кіберполіції.
49. Наведіть основні функції Департаменту кіберполіції.
50. Надайте визначення та характеристику поняття національна система кібербезпеки.
51. Наведіть основні завдання у сфері забезпечення кібербезпеки Державної служби спеціального зв'язку та захисту інформації України.
52. Наведіть основні завдання у сфері забезпечення кібербезпеки Національної поліції України.
53. Наведіть основні завдання у сфері забезпечення кібербезпеки Служби безпеки України.
54. Наведіть основні завдання у сфері забезпечення кібербезпеки Міністерства оборони України, Генерального штабу Збройних Сил України.
55. Наведіть основні завдання у сфері забезпечення кібербезпеки розвідувальних органів України.
56. Наведіть основні завдання у сфері забезпечення кібербезпеки Національного банку України.
57. Проведенням яких заходів забезпечується функціонування національної системи кібербезпеки?
58. У чому полягають застереження, з якими Україна ратифікувала Конвенцію «Про кіберзлочинність»?
59. Наведіть юрисдикцію щодо кіберзлочинів згідно Конвенції «Про кіберзлочинність».

60. Яким чином у Конвенції «Про кіберзлочинність» висвітлено принципи міжнародного співробітництва країн-учасниць у сфері протидії кіберзлочинності?
61. У чому полягає процедура екстрадиції?
62. Наведіть визначення OSINT та ставлення Конвенції «Про кіберзлочинність» до даного методу збору інформації.
63. Наведіть основні умови для забезпечення функціонування вільної та безпечної глобальної мережі Інтернет.
64. Наведіть основні пропозиції вирішення проблеми національної кібербезпеки.
65. Наведіть першочергові кроки України на шляху забезпечення кібербезпеки.
66. Наведіть основні складові кібербезпеки та надайте їх характеристику.
67. Що має визначати типова політика кібербезпеки держави?
68. Наведіть основні вимоги до національної політики кібербезпеки держави.
69. Які положення має містити стратегія кібербезпеки держави?
70. Значення CERT у забезпеченні кібербезпеки держави?
71. Завдання CERT-UA.
72. Державно-приватне партнерство у сфері забезпечення кібербезпеки держави: визначення, принципи, першочергові завдання.
73. Співпраця між органами державної влади, які опікуються питаннями кібербезпеки держави: визначення, принципи, першочергові завдання.
74. Що вимагає створення національного потенціалу держави для усунення кіберінцидентів?
75. У чому полягає реалізація механізму координації в системі державного управління?
76. У чому полягає реалізація практики обміну інформацією у сфері забезпечення кібербезпеки між приватним сектором і урядовими органами?
77. Принципи застосування законодавства у сфері кібербезпеки.
78. Принципи забезпечення кібербезпеки.
79. Міжнародне співробітництво у сфері кібербезпеки.
80. Контроль за законністю заходів із забезпечення кібербезпеки України.

81. Запобігання та протидія кіберзлочинності як об’єкт державного управління в умовах глобалізації.
82. Зарубіжний досвід щодо реалізації державних механізмів у галузі запобігання та боротьби з кіберзлочинністю.
83. Особливості організаційних та нормативно-правових засад боротьби з кіберзлочинністю.
84. Проблеми державного управління у сфері запобігання проявам кіберзлочинності.
85. Напрями розв'язання проблеми проявів кіберзлочинності.
86. Моделі державних механізмів боротьби з кіберзлочинністю.
87. Напрями впорядкування правового підґрунтя діяльності та взаємовідносин в організаційно-функціональній структурі суб’єктів протидії кіберзлочинності.
88. Система запобігання кіберзлочинності в Україні.