МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Харківський національний університет внутрішніх справ

Кафедра інформаційних технологій та кібербезпеки факультету № 4

РОБОЧА 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 2020

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 23.09.2020 № 9

СХВАЛЕНО
Вченою радою
факультету № 4
Протокол від 16.09.2020 № 5

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 18.09.2020 № 5

Розглянуто на засіданні кафедри інформаційних технологій та кібербезпеки факультету № 4 (протокол від 15.09.2020 № 16).

Розробники:
Професор кафедри інформаційних технологій та кібербезпеки факультету № 4, кандидат технічних наук, доцент Носов В.В.
Доцент кафедри інформаційних технологій та кібербезпеки факультету № 4, 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 інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ к.т.н., доцент Тулупов В.В.

1. Опис навчальної дисципліни

<table>
<tr><th>Найменування показників</th><th>Шифри та назви галузі знань, код та назва спеціальності, ступінь вищої освіти</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><td>Кількість кредитів ECTS – 4
Загальна кількість годин – 120
Кількість тем – 3</td><td>125 "Кібербезпека";
(Безпека інформаційних та комунікаційних систем),
магістр</td><td>Дисципліна вибіркового блоку.

Навчальний курс 1
Семестр 2

Види підсумкового контролю: - залік</td></tr>
<tr><td colspan="3">Розподіл навчальної дисципліни за видами занять:</td></tr>
<tr><td colspan="2">денна форма навчання

Лекції – 20 ; (години)
Семінарські заняття – 20 ; (години)
Практичні заняття – _____; (години)
Лабораторні заняття – _____; (години)
Самостійна робота – 80 ; (години)

Індивідуальні завдання:

Курсова робота – _____ (кількість; № семестру)
Реферати (тощо) – 1 (кількість; № семестру)</td><td>заочна форма навчання

Лекції – 4 ; (години)
Семінарські заняття – 6 ; (години)
Практичні заняття – _____; (години)
Лабораторні заняття – _____; (години)
Самостійна робота – 110 ; (години)

Індивідуальні завдання:

Курсова робота – _____

(кількість; № семестру)
Реферати – 1 (кількість; № семестру)</td></tr>
</table>

2. Мета та завдання навчальної дисципліни

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.

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.

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.

Очікувані результати навчання: у результаті вивчення навчальної дисципліни здобувач вищої освіти повинен

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.

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

3. Програма 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

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.

4. Структура навчальної дисципліни

4.1.1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни					Вид контролю
	Всього	з них:				
		лекції	Семінарські заняття	Лабораторні заняття	Самостійна робота	
Семестр № 2						
Тема № 1. Теоретичні засади запобігання і протидії проявам кіберзлочинності	24	4	4		16	
Тема № 2. Державне управління у сфері запобігання і протидії кіберзлочинності в Україні	36	6	6		24	
Тема № 3. Державні механізми запобігання і протидії кіберзлочинності	60	10	10		40	
Всього за семестр	**120**	**20**	**20**		**80**	**залік**

4.1.2. Розподіл часу навчальної дисципліни за темами (заочна форма навчання)

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни					Вид контролю
	Всього	з них:				
		лекції	Семінарські заняття	Лабораторні заняття	Самостійна робота	
Семестр № 2						
Тема № 1. Теоретичні засади запобігання і протидії проявам кіберзлочинності	29	1	2		26	
Тема № 2. Державне управління у сфері запобігання і протидії кіберзлочинності в Україні	37	1	2		34	
Тема № 3. Державні механізми запобігання і протидії кіберзлочинності	54	2	2		50	
Всього за семестр	**120**	**4**	**6**		**110**	**залік**

4.1.3. Питання, що виносяться на самостійне опрацювання

Перелік питань до тем навчальної дисципліни	Література
Тема №1. Теоретичні засади запобігання і протидії проявам кіберзлочинності	
Користуючись текстом лекції та рекомендованою літературою до теми, сформувати тези відповідей на контрольні запитання до теми. Скласти порівняльну таблицю зарубіжного досвіду реалізації державних механізмів у галузі запобігання та боротьби з кіберзлочинністю.	2-5, ресурси Internet
Тема №2. Державне управління у сфері запобігання і протидії кіберзлочинності в Україні	
Користуючись текстом лекції та рекомендованою літературою до теми, сформувати тези відповідей на контрольні запитання до теми. Скласти порівняльну таблицю напрямів вирішення проблеми проявів кіберзлочинності.	2-5, ресурси Internet
Тема №3. Державні механізми запобігання і протидії кіберзлочинності	
Користуючись текстом лекції та рекомендованою літературою до теми, сформувати тези відповідей на контрольні запитання до теми. Скласти порівняльну таблицю складових системи запобігання кіберзлочинності в Україні	2-5, ресурси Internet

5. Індивідуальні завдання

5.1.1. Теми рефератів

1. Огляд закордонного нормативно-правового забезпечення державного управління у сфері запобігання і протидії кіберзлочинності.
2. Механізми запобігання і протидії кіберзлочинності США.
3. Механізми запобігання і протидії кіберзлочинності ЄС.

6. Методи навчання

Аудиторні заняття проводяться у формі візуального представлення аналітично-графічного матеріалу дисципліни, на яких слухачі повинні виконувати відповідні розумові, обчислювальні та практичні дії.

Самостійна робота за кожною темою передбачає вивчення теоретичних питань лекційних занять, опрацювання завдань семінарських занять.

Індивідуальна робота передбачає написання рефератів.

7. Перелік питань та завдань, що виносяться на підсумковий контроль

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.

8. Критерії та засоби оцінювання результатів навчання здобувачів

Контрольні заходи включають у себе поточний та підсумковий контроль.

Поточний контроль.

До форм поточного контролю належить оцінювання:

– рівня знань під час практичних і лабораторних занять;

– якості виконання індивідуальної та самостійної роботи.

Поточний контроль здійснюється під час проведення практичних та лабораторних занять і має за мету перевірку засвоєння слухачем знань, умінь і навичок з навчальної дисципліни.

У ході поточного контролю проводиться систематичний вимір приросту знань, їх корекція. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національної системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Оцінки за самостійну та індивідуальну роботи виставляються в журнали обліку роботи академічної групи окремою графою за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Результати цієї роботи враховуються під час виставлення підсумкових оцінок.

При розрахунку успішності здобувачів вищої освіти в Університеті враховуються такі види робіт: навчальні заняття (практичні, лабораторні тощо); самостійна та індивідуальна роботи (виконання домашніх завдань, ведення конспектів першоджерел та робочих зошитів, виконання розрахункових завдань, підготовка рефератів, наукових робіт, публікацій, розроблення спеціальних технічних пристроїв і приладів, моделей, комп'ютерних програм, виступи на наукових конференціях, семінарах та інше); контрольні роботи (виконання тестів, контрольних робіт у вигляді, передбаченому в робочій програмі навчальної дисципліни). Вони оцінюються за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Результат навчальних занять за семестр розраховується як середньоарифметичне значення з усіх виставлених оцінок під час навчальних занять протягом семестру та виставляється викладачем в журналі обліку роботи академічної групи окремою графою.

Результат самостійної роботи за семестр розраховується як середньоарифметичне значення з усіх виставлених оцінок з

самостійної роботи, отриманих протягом семестру та виставляється викладачем в журналі обліку роботи академічної групи окремою графою.

Здобувач, який отримав оцінку «незадовільно» за навчальні заняття або самостійну роботу, зобов'язаний перескласти її.

Загальна кількість балів (оцінка), отримана здобувачем за семестр перед підсумковим контролем, розраховується як середньоарифметичне значення з оцінок за навчальні заняття та самостійну роботу, та для переводу до 100-бальної системи помножується на коефіцієнт **10**.

Загальна кількість балів (перед підсумковим контролем) ***=((Результат навчальних занять за семестр + Результат самостійної роботи за семестр) / 2) *10***

Підсумковий контроль.

Підсумковий контроль проводиться шляхом усного опитування або письмової контрольної роботи з метою оцінки результатів навчання.

Для обліку результатів підсумкового контролю використовується поточно-накопичувальна інформація, яка реєструються в журналах обліку роботи академічної групи. Результати підсумкового контролю з дисциплін відображуються у відомостях обліку успішності, навчальних картках слухачів, залікових книжках. ***Присутність здобувачів на проведенні підсумкового контролю (заліку) обов'язкова.*** Якщо здобувач вищої освіти не з'явився на підсумковий контроль (залік), то науково-педагогічний працівник ставить у відомість обліку успішності відмітку «не з'явився».

Підсумковий контроль (залік) оцінюється за національною шкалою. Для переводу результатів, набраних на підсумковому контролі (заліку), з національної системи оцінювання в 100-бальну вводиться коефіцієнт **10**, таким чином максимальна кількість балів на підсумковому контролі (заліку), які використовуються при розрахунку успішності здобувачів, становить – **50**.

Підсумкові бали з навчальної дисципліни визначаються як сума балів, отриманих здобувачем протягом семестру та балів, набраних на підсумковому контролі (заліку).

Підсумкові = Загальна кількість + Кількість балів

бали навчальної дисципліни ***балів (перед підсумковим контролем)*** ***за підсумковим контролем***

Здобувач вищої освіти, який під час складання підсумкового контролю отримав оцінку «незадовільно», складає підсумковий контроль (залік) повторно. Повторне складання підсумкового контролю (заліку) допускається не більше двох разів з кожної навчальної дисципліни, у тому числі один раз – викладачеві, а другий – комісії, до складу якої входить керівник відповідної кафедри та 2-3 науково-педагогічних працівники.

Незадовільні оцінки виставляються тільки в відомостях обліку успішності. Здобувачам вищої освіти, які отримали не більше як дві незадовільні оцінки (нижче ніж 60 балів) з навчальної дисципліни, можуть бути встановлені різні строки ліквідації академічної заборгованості, але не пізніше як за день до фактичного початку навчальних занять у наступному семестрі.

Робота під час навчальних занять	**Самостійна та індивідуальна робота**	**Підсумковий контроль**
Отримати не менше 3 позитивних оцінок	Підготувати реферат, підготувати конспект за темами самостійної роботи	Отримати за підсумковий контроль не менше 30 балів

9. Шкала оцінювання: національна та ECTS

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
97-100	Відмінно ("зараховано")	A	**"Відмінно"** – теоретичний зміст курсу освоєний **цілком,** необхідні практичні навички роботи з освоєним матеріалом сформовані, **всі** навчальні завдання, які передбачені програмою навчання **виконані** в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
94-96			
90-93			
85 – 89	Добре ("зараховано")	B	**"Дуже добре"** – теоретичний зміст курсу освоєний **цілком,** необхідні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **всі** навчальні завдання, які передбачені програмою навчання **виконані**, якість виконання **більшості** з них оцінено числом балів, близьким до **максимального,** робота з двома – трьома незначними помилками.
80-84			
75 – 79		C	**"Добре"** – теоретичний зміст курсу освоєний **цілком,** практичні навички роботи з освоєним матеріалом **в основному** сформовані, **всі** навчальні завдання, які передбачені програмою навчання **виконані**, якість виконання **жодного** з них **не оцінено мінімальним** числом балів, деякі види завдань виконані **з помилками,** робота з декількома незначними помилками, або з однією – двома значними помилками.
70 –74	Задовільно ("зараховано")	D	**"Задовільно"** – теоретичний зміст курсу освоєний **не повністю**, але **прогалини не носять істотного** характеру, необхідні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **більшість** передбачених програмою навчання навчальних завдань **виконано, деякі** з виконаних завдань, містять **помилки,** робота з трьома значними помилками.
65-69			
60 – 64		E	**"Достатньо"** – теоретичний зміст курсу освоєний **частково, деякі** практичні навички роботи **не сформовані, частина** передбачених програмою навчання навчальних завдань **не виконані,** або якість виконання деяких з них оцінено числом балів, близьким до **мінімального,** робота, що задовольняє мінімуму критеріїв оцінки.
40–59	Незадовільно ("не зараховано")	FX	**"Умовно незадовільно"** – теоретичний зміст курсу освоєний **частково**, необхідні практичні навички роботи **не сформовані, більшість** передбачених програм навчання, навчальних завдань **не виконано**, або якість їхнього

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
21-40			виконання оцінено числом балів, близьким до **мінімального**; при **додатковій самостійній** роботі над матеріалом курсу **можливе підвищення якості** виконання навчальних завдань (**з можливістю повторного складання**), робота, що потребує доробки
1–20		F	**"Безумовно незадовільно"** – теоретичний зміст курсу **не освоєно**, необхідні практичні навички роботи **не сформовані, всі виконані** навчальні завдання містять грубі **помилки, додаткова самостійна** робота над матеріалом курсу **не приведе** до значимого **підвищення якості** виконання навчальних завдань, робота, що потребує повної переробки

10. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

10.1 Основна:

1. 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: 08.09.2020).
2. 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: 08.09.2020).
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: 08.09.2020).
4. Носов В.В. Організація та забезпечення інформаційної безпеки: навчальний посібник / В.В. Носов, О.В. Манжай. – Х.: Вид-во Харк. нац. ун-ту внутр. справ, 2007. – 216 с.

10.2 Допоміжна:

5. 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.
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. 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.

10.3 Інформаційні ресурси в Інтернеті:

8. http://www.niss.gov.ua/articles/454/
9. https://cyberpolice.gov.ua/strategy-2020/