МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ЮРИДИЧНИЙ УНІВЕРСИТЕТ
імені ЯРОСЛАВА МУДРОГО

Електронне видання

МЕТОДИЧНІ МАТЕРІАЛИ ДО ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ЗАПОБІГАННЯ КІБЕРЗЛОЧИНАМ»

Харків
2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ЮРИДИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЯРОСЛАВА МУДРОГО

Електронне видання

МЕТОДИЧНІ МАТЕРІАЛИ ДО ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ЗАПОБІГАННЯ КІБЕРЗЛОЧИНАМ»

для студентів
першого (бакалаврського) рівня вищої освіти
галузі знань 26 «Цивільна безпека»
спеціальності 262 «Правоохоронна діяльність»

Харків
2021

Методичні матеріали до вивчення навчальної дисципліни «Запобігання кіберзлочинам» (за вибором) для здобувачів вищої для здобувачів вищої освіти бакалаврського (першого) рівня вищої освіти галузі знань 26 «Цивільна безпека» спеціальності 262 «Правоохоронна діяльність». Харків: Нац. юрид. ун-т імені Ярослава Мудрого, 2021. 51 с.

У к л а д а ч : О. В. Таволжанський

В С Т У П

Мета навчальної дисципліни – формування системи наукових знань про правове регулювання запобігання кіберзлочинів, вивчення вітчизняних та зарубіжних підходів до розуміння змісту заходів забезпечення кібербезпеки, вироблення основних умінь і навичок застосування національного законодавства, активізація аналітичної діяльності студентів, проведення науково-дослідницької роботи, а також практичних навичок діяльності правника.

Завдання: формування системи теоретичних знань про інститут кібербезпеки, його змістовне наповнення; опанування інструментарієм інституту запобігання кіберзлочинам, базовими категоріями кібербезпеки; визначення поняття, видів та стану кіберзлочинності: рівня, структури, динаміки та інших показників; аналіз і дослідження прикладних проблем порядку формування та реалізації державної політики в сфері забезпечення кібербезпеки, спрямованих на набуття (підтвердження) суб'єктивних прав та покладення на приватних осіб передбачених законом обов'язків; наведення характеристики, класифікацій та видів кіберзлочинів, аналіз їх структури, визначення стадій та етапів, окреслення повноважень суб'єктів запобігання кіберзлочинам; розвиток навичок і умінь запровадження та застосування заходів запобігання кіберзлочинам.

У результаті вивчення навчальної дисципліни "Запобігання кіберзлочинам" студенти *повинні:*

мати уявлення:

про новітні досягнення науки в сфері запобігання кіберзлочинам;

закономірності виникнення і поширення кіберзлочинності;

знати:

основні принципи забезпечення кібербезпеки;

сукупність ознак структури особи кіберзлочинця;

основні теорії пояснення причин кіберзлочинності;

засадничі положення державної політики забезпечення кіберзахисту та кібербезпеки;

уміти:

досліджувати рівень, структуру, динаміку кіберзлочинності;

характеризувати суспільні явища і процеси, що породжують та зумовлюють кіберзлочинність;

аналізувати законодавство, що визначає систему заходів запобігання різним формам і проявам кіберзлочинності;

надавати кримінологічну характеристику кримінальним правопорушенням у віртуальній сфері та пропонувати заходи запобігання їм;

володіти навичками:

аналізу та оцінювання стану кіберзлочинності в державі;

складання проєктів програм запобігання окремим видам кіберзлочинів.

Оволодіння навчальної дисципліни «Запобігання кіберзлочинам» сприятиме суттєвому підвищенню загального рівня підготовки правників, розвиткові аналітичних здібностей, удосконаленню володіння компетентностями, що забезпечить у подальшому їх належний професійний рівень.

1. ЗАГАЛЬНИЙ РОЗРАХУНОК ГОДИН ЛЕКЦІЙ, ПРАКТИЧНИХ ЗАНЯТЬ, САМОСТІЙНОЇ РОБОТИ

№п/п	Тема	Всього годин	У тому числі		
			лекції	практичні заняття	самостійна робота
ЗМІСТОВИЙ МОДУЛЬ І Формування та реалізація державної політики в сфері кібербезпеки					
1.	Основні цілі, напрями та принципи державної політики у сфері кібербезпеки.	**10**	**2**	**2**	**6**
2.	Стан забезпечення кібербезпеки на сучасному етапі.	**16**	**2**	**4**	**10**
3.	Міжнародний досвід у побудові безпечного кіберпростору.	**18**	**4**	**4**	**10**
Разом		**44**	**8**	**10**	**26**
	ЗМІСТОВИЙ МОДУЛЬ ІІ Базові засади запобігання кіберзлочинам				
4.	Поняття і визначення кіберзлочину.	**12**	**2**	**4**	**6**
5.	Кіберзлочинність та її вимірювання.	**14**	**4**	**4**	**6**
6.	Особа кіберзлочинця.	**12**	**2**	**4**	**6**
7.	Запобігання кіберзлочинності: поняття, зміст, значення.	**14**	**4**	**4**	**6**
Разом		**52**	**12**	**16**	**24**
ЗМІСТОВИЙ МОДУЛЬ ІІІ Теорія окремих видів кіберзлочинів та їх запобігання					
8.	Підходи до класифікації кіберзлочинів. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як	**8**	**2**	**4**	**2**

	незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.				
9.	Характеристика кіберзлочинів пов'язаних з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо)	**8**	**2**	**4**	**2**
10.	Характеристика кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією).	**6**	**2**	**2**	**2**
11.	Характеристика кіберзлочинів, пов'язаних з порушенням авторського права і суміжних прав.	**6**	**2**	**2**	**2**
12.	Поняття та кримінологічна характеристика кіберзлочинів, зафіксованих в окремому протоколі (акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж).	**4**	**-**	**2**	**2**
13.	Кіберзлочинність у сфері економіки.	**4**	**-**	**2**	**2**
14.	Характеристика кіберзлочинів у сфері обігу наркотичних засобів.	**4**	**-**	**2**	**2**
15.	Гібридна війна.	**6**	**2**	**2**	**2**
16.	Корупція у віртуальній сфері.	**4**	**-**	**2**	**2**
17.	Характеристика злочинності неповнолітніх у віртуальній	**4**	**-**	**2**	**2**

	сфері.				
Разом		**56**	**10**	**24**	**20**
Усього (I, II, III змістові модулі)		**150**	**30**	**50**	**70**

ЗАТВЕРДЖЕНО
на засіданні кафедри кримінології
та кримінально-виконавчого права
Національного юридичного
університету
імені Ярослава Мудрого
(протокол № 1 від 03.09.2021р.)

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ЗАПОБІГАННЯ КІБЕРЗЛОЧИНАМ»

I. ФОРМУВАННЯ ТА РЕАЛІЗАЦІЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ КІБЕРБЕЗПЕКИ.

Основні цілі, напрями та принципи державної політики у сфері кібербезпеки.

Правові основи забезпечення кібербезпеки України. Кіберпростір та його визначення. Об'єкти кібербезпеки та кіберзахисту. Суб'єкти забезпечення кібербезпеки. Передумови та чинники кіберзагроз.

Стан забезпечення кібербезпеки на сучасному етапі. Світовий досвід та тенденції у формуванні безпечного віртуального простору.

Передумови та чинники кіберзагроз. Заходи забезпечення кібербезпеки. Концепція розвитку науки щодо запобіганню кіберзлочинності в Україні на початку XXI століття. Методологічні особливості вивчення кіберпростору.

Міжнародний досвід у побудові безпечного кіберпростору.

Базові міжнародні документи щодо запобігання кіберзлочинності. Кіберзлочинність та транснаціональна організована злочинність. Міжнародні акти про захист дітей від сексуальної

експлуатації та сексуального насильства. Міжнародні та іноземні суб'єкти запобігання кіберзлочинності.

ІІ. БАЗОВІ ЗАСАДИ ЗАПОБІГАННЯ КІБЕРЗЛОЧИНАМ

Поняття і визначення кіберзлочину.

Кіберзлочин як соціально-правове явище, особа кіберзлочинця, детермінація кіберзлочинності, запобігання кіберзлочинності. Запобігання кіберзлочинам як міжгалузева дисципліна. Класифікація кіберзлочинів. Запобігання кіберзлочинності на сучасному етапі розвитку України і в перспективі.

Кіберзлочинність та її вимірювання.

Поняття кіберзлочинності та основні науково-практичні підходи щодо її розуміння і визначення. Кількісно-якісне вимірювання кіберзлочинності. Рівень кіберзлочинності. Структура кіберзлочинності. Кримінально-правові ознаки структури кіберзлочинності. Кримінологічні ознаки структури кіберзлочинності. Динаміка кіберзлочинності. Технічні фактори, які впливають на динаміку кіберзлочинності. Соціальні фактори, які впливають на динаміку кіберзлочинності. Правові фактори, які впливають на динаміку кіберзлочинності. Географія кіберзлочинності. Топографія кіберзлочинності. Ціна кіберзлочинності. Латентність кіберзлочинності. Структура латентної кіберзлочинності. Загальна характеристика сучасної кіберзлочинності в Україні, тенденції її розвитку. Детермінанти кіберзлочинності. Умови формування кримінальної мотивації та мотивів. Умови реалізації мотивів і рішення про вчинення кіберзлочину.

Особа кіберзлочинця.

Структура особистості кіберзлочинця. Соціально-демографічні ознаки особистості кіберзлочинця. Морально-психологічні якості і особистісно-рольові властивості особистості кіберзлочинця. Соціальне і біологічне в особистості кіберзлочинця, їх

співвідношення. Типологія кіберзлочинців. Наукове і практичне значення вивчення особистості кіберзлочинця та її типології. Поняття причини кіберзлочину. Умови, що сприяють вчиненню кіберзлочину.

Запобігання кіберзлочинності: поняття, зміст, значення.

Поняття і система запобігання кіберзлочинності, класифікація запобіжних заходів. Загально соціальне, спеціально-кримінологічне та індивідуальне запобігання кіберзлочинності і окремих злочинів. Об'єкти запобігання кіберзлочинності. Суб'єкти запобігання кіберзлочинності та основні напрями їх діяльності. Прогнозування в сфері кіберзахисту. Поточне прогнозування. Короткострокове прогнозування. Середньострокове прогнозування. Перспективне прогнозування. Загальнодержавне планування. Регіональне планування. Відомче та галузеве планування. Головні етапи планування.

ІІІ. ТЕОРІЯ ОКРЕМИХ ВИДІВ КІБЕРЗЛОЧИНІВ ТА ЇХ ЗАПОБІГАННЯ.

Підходи до класифікації кіберзлочинів. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.

Поняття та характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерної інформації. Основні кримінологічні риси особистості кіберзлочинців, які вчиняють злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему. Причини та умови злочинів проти конфіденційності, цілісності та доступності

комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему. Запобігання кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.

Характеристика кіберзлочинів пов'язаних з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо) .

Поняття та характеристика кіберзлочинів пов'язаних з використанням комп'ютера як засобу скоєння злочинів. Особистість кібершахрая, основні риси. Причини і умови кіберзлочинів, пов'язаних з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо). Запобігання кіберзлочинам, пов'язаним з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо).

Характеристика кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією).

Характеристика кіберзлочинів, пов'язаних з контентом. Особистість кіберзлочинця, основні риси. Причини і умови кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією). Запобігання кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією).

Характеристика кіберзлочинів, пов'язаних з порушенням авторського права і суміжних прав.

Поняття та характеристика кіберзлочинів, пов’язаних з порушенням авторського права і суміжних прав. Причини та умови кіберзлочинів пов’язаних з порушенням авторського права і суміжних прав. Запобігання кіберзлочинам пов’язаних з порушенням авторського права і суміжних прав.

Характеристика кіберзлочинів, зафіксованих в окремому протоколі (акти расизму та ксенофобії, вчинені за допомогою комп’ютерних мереж).

Поняття та характеристика кіберзлочинів, зафіксованих в окремому протоколі (акти расизму та ксенофобії, вчинені за допомогою комп’ютерних мереж). Хуліганство у віртуальній сфері. Запобігання кіберзлочинам проти громадського порядку та моральності.

Кіберзлочинність у сфері економіки.

Поняття та характеристика кіберзлочинів у сфері економіки. Особистість кіберзлочинця у сфері економіки, основні риси. Захист об’єктів критичної інфраструктури. Причини та умови кіберзлочинів у сфері економіки. Запобігання кіберзлочинам у сфері економіки.

Характеристика кіберзлочинів у сфері обігу наркотичних засобів.

Поняття та характеристика кіберзлочинів у сфері обігу наркотичних засобів. Причини та умови кіберзлочинів у сфері обігу наркотичних засобів. Запобігання кіберзлочинам у сфері обігу наркотичних засобів. Поняття та взаємозв'язок організованої злочинності та кіберзлочинності. Характеристика організованої кіберзлочинності. Причини та умови організованої злочинності. Запобігання організованій злочинності. Міжнародне співробітництво у сфері запобігання організованій злочинності.

Гібридна війна.

Характеристика кіберзлочинів у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації. Причини та умови кіберзлочинів у сфері

охорони державної таємниці, недоторканності державних кордонів, забезпечення. Поняття військових кіберзлочинів та їх характеристика. призову та мобілізації. Запобігання кіберзлочинам у сфері охорони державної таємниці, недоторканості державних кордонів, забезпечення призову та мобілізації.

Корупція у віртуальній сфері.

Визначення корупції як соціального явища та зв'язок з новітніми технологіями, види корупційних кіберпроявів. Характеристика корупційної кіберзлочинності. Причини та умови корупційної кіберзлочинності. Запобігання корупційній кіберзлочинності.

Характеристика злочинності неповнолітніх у віртуальній сфері.

Поняття та характеристика злочинності неповнолітніх у віртуальній сфері. Особистість неповнолітнього кіберзлочинця, основні риси. Причини та умови кіберзлочинності неповнолітніх. Запобігання кіберзлочинності неповнолітніх.

3. ЗАВДАННЯ ДО ПРАКТИЧНИХ ЗАНЯТЬ ТА САМОСТІЙНОЇ РОБОТИ

Тема 1. ОСНОВНІ ЦІЛІ, НАПРЯМИ ТА ПРИНЦИПИ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ КІБЕРБЕЗПЕКИ.

Питання для обговорення

1. Правові основи забезпечення кібербезпеки України. Визначення кіберпростору.
2. Об'єкти кібербезпеки та кіберзахисту.
3. Суб'єкти забезпечення кібербезпеки.
4. Передумови та чинники кіберзагроз.

Завдання

1. Розкрийте та порівняйте за обсягом та змістом наступні визначення: кіберзлочин, кіберзагроза, кібератака, кіберінцендент. Назвіть об'єкт та розкрийте предмет кіберзахисту.

2. Проаналізуйте мету, задачі та функції запобігання кіберзлочинам на рівні держави та міжнародному рівні.

3. Перелічте законодавчі та підзаконні акти якими врегульовано сферу боротьби з кіберзлочинами.

4. Проаналізуйте основні ідеї і положення Конвенції про кіберзлочинність.

5. Назвіть ідеї і положення міжнародних практик запобігання кіберзлочинам, що знайшли своє втілення в національному законодавстві та практичній діяльності у сфері боротьби з кіберзлочинністю.

Література до теми 1

1. Кримінологія : підручник / Б. М. Головкін, В. В. Голіна, О. В. Лисодєд та ін.; за заг. ред. Б. М. Головкіна. Харків : Право, 2020. 384 с.
2. Захист прав, приватності та безпеки людини в інформаційну епоху / Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін. : монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. Київ-Одеса : Фенікс, 2020. 260 с.
3. Гавловський В.Д. Аналіз стану кіберзлочинності в Україні. Інформація і право. № 1(28)/2019. С. 108-117.
4. V. V. Tsypko, K. I. Alieksieieva, I. A. Venger, O. V. Tavolzhanskyi, N. I. Galunets, A. V. Klyuchnik. Information policy of the enterprise as the basis for the reproduction of human potential in the structure of public social interaction () // Journal of Advanced Research in Law and Economics (Журнал перспективных исследований в области права и экономики). - 2019. Румыния. - Vol. 10 Issue 6.- P.1664-1672. (Scopus) https://www.scopus.com/record/display.uri?eid=2-s2.0-85087468504&origin=resultslist
5. Головкін Б. М. Теперішнє і майбутнє кримінології. Проблеми законності. 2020. Вип. 149. С. 168–184.

Т е м а 2. **СТАН ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ НА СУЧАСНОМУ ЕТАПІ.**

Питання для обговорення

1. Стратегія, законодавство, напрямки сучасної політики у сфері кібербезпеки в Україні та зарубіжних країнах.
2. Концепція розвитку науки щодо запобіганню кіберзлочинності в Україні на початку XXI століття.
3. Сучасні тенденції у формуванні безпечного віртуального простору.

Література до теми 2

1. Кримінологія : підручник / Б. М. Головкін, В. В. Голіна, О. В. Лисодєд та ін.; за заг. ред. Б. М. Головкіна. Харків : Право, 2020. 384 с.
2. Захист прав, приватності та безпеки людини в інформаційну епоху / Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін. : монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. Київ-Одеса : Фенікс, 2020. 260 с.
3. Гавловський В.Д. Аналіз стану кіберзлочинності в Україні. Інформація і право. № 1(28)/2019. С. 108-117.
4. Головкін Б. М. Теперішнє і майбутнє кримінології. Проблеми законності. 2020. Вип. 149. С. 168–184.

Т е м а 3. **МІЖНАРОДНИЙ ДОСВІД У ПОБУДОВІ БЕЗПЕЧНОГО ВІРТУАЛЬНОГО ПРОСТОРУ.**

Питання для обговорення

1. Базові міжнародні документи щодо запобігання кіберзлочинності.
2. Кіберзлочинність та транснаціональна організована злочинність.
3. Міжнародні акти про захист дітей від сексуальної експлуатації та сексуального насильства.
4. Міжнародні та іноземні суб'єкти запобігання кіберзлочинності.

Література до теми 3

1. Конвенція про кіберзлочинність (Конвенцію ратифіковано із застереженнями і заявами Законом N 2824-IV (2824-15) від 07.09.2005 [Електронний ресурс] // ВВР, 2006, N 5-6, ст.71) — Режим доступу: http://zakon5.rada.gov.ua/laws/show/994_575
2. Конвенція Ради Європи про запобігання тероризму { Конвенцію ратифіковано з заявами і застереженнями Законом N 54-V (54-16) від 31.07.2006 [Електронний ресурс] //

ВВР, 2006, N 39, ст.340 } — Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_712

3. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності. Прийнята резолюцією 55/25 Генеральної Асамблеї від 15 листопада 2000 року [Електронний ресурс], — Режим доступу: http://zakon0.rada.gov.ua/laws/show/995_789

4. Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства {Конвенцію ратифіковано з заявами Законом № 4988-VI від 20.06.2012} [Електронний ресурс], — Режим доступу: http://zakon5.rada.gov.ua/laws/show/994_927

5. Конвенція Ради Європи про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом, та про фінансування тероризму. {Конвенцію ратифіковано з заявами і застереженнями Законом N 2698-VI (2698-17) від 17.11.2010} [Електронний ресурс], — Режим доступу: http://zakon3.rada.gov.ua/laws/show/994_948

Тема 4. **ПОНЯТТЯ І ВИЗНАЧЕННЯ КІБЕРЗЛОЧИНУ.**

Питання для обговорення

1. Поняття і визначення кіберзлочину.
2. Кіберзлочин як соціально-правове явище, особа кіберзлочинця, детермінація кіберзлочинності, запобігання кіберзлочинності.
3. Запобігання кіберзлочинам як міжгалузева дисципліна.
4. Класифікації кіберзлочинів. Найбільш розповсюджені підходи до групування кіберзлочинів.
5. Загальні положення щодо запобігання кіберзлочинності на сучасному етапі розвитку України і в перспективі.

Завдання

6. Надайте легальне визначення кіберзлочину. Порівняйте з визначеннями наданими в науці.

7. Охарактеризуйте основні ознаки кіберзлочинності.

8. Назвіть, які кримінально карані діяння у віртуальному просторі відображаються у офіційній статистиці України.

Література до теми 4

1. Кримінологія : підручник / Б. М. Головкін, В. В. Голіна, О. В. Лисодєд та ін. ; за заг. ред. Б. М. Головкіна. Харків : Право, 2020. 384 с.
2. Тимошенко В. І., Шакун В. І. Теоретичні основи кримінології: монографія. Київ: Юрінком Інтер, 2021. 240 с.
3. Гавловський В.Д. Аналіз стану кіберзлочинності в Україні. Інформація і право. № 1(28)/2019. С. 108-117.
4. V. V. Tsypko, K. I. Alieksieieva, I. A. Venger, O. V. Tavolzhanskyi, N. I. Galunets, A. V. Klyuchnik. Information policy of the enterprise as the basis for the reproduction of human potential in the structure of public social interaction // Journal of Advanced Research in Law and Economics (Журнал перспективных исследований в области права и экономики). - 2019. Румыния. - Vol. 10 Issue 6.- P.1664-1672. (Scopus) https://www.scopus.com/record/display.uri?eid=2-s2.0-85087468504&origin=resultslist
5. Головкін Б. М. Теперішнє і майбутнє кримінології. Проблеми законності. 2020. Вип. 149. С. 168–184.

Т е м а 5. **КІБЕРЗЛОЧИННІСТЬ ТА ЇЇ ВИМІРЮВАННЯ. ДЕТЕРМІНАНТИ КІБЕРЗЛОЧИННОСТІ.**

Питання для обговорення

1. Поняття кіберзлочинності та основні науково-практичні підходи щодо її розуміння і визначення.

2. Кількісно-якісне вимірювання кіберзлочинності.

3. Рівень кіберзлочинності.

4. Структура кіберзлочинності.

5. Кримінально-правові ознаки структури кіберзлочинності. Кримінологічні ознаки структури кіберзлочинності.

6. Динаміка кіберзлочинності. Технічні фактори, які впливають на динаміку кіберзлочинності. Соціальні фактори, які впливають на динаміку кіберзлочинності. Правові фактори, які впливають на динаміку кіберзлочинності.

7. Географія кіберзлочинності. Топографія кіберзлочинності. Ціна кіберзлочинності. Латентність кіберзлочинності. Структура латентної кіберзлочинності.

8. Детермінанти кіберзлочинності. Умови формування кримінальної мотивації та мотивів. Умови реалізації мотивів і рішення про вчинення кіберзлочину.

Завдання

9. Розкрийте основні проблеми, що виникають у пізнанні природи кіберзлочинності, аргументовано доведіть свою точку зору.

10. На основі аналізу статистичної інформації Офісу Генерального прокурора «Єдиний звіт про кримінальні правопорушення» (https://www.gp.gov.ua/ua/1stat) та статистичної інформації Держкомстату України (http://www.ukrstat.gov.ua/) «Про чисельність населення, станом на 1 січня за певний період»:

1) обчисліть коефіцієнт злочинної інтенсивності в сфері вчинення кіберзлочинів в цілому по Україні у розрахунку на 10 тис. населення за останній звітній період (один рік);

2) здійсніть рейтингування областей України за кількістю облікованих кіберзлочинів, а також за коефіцієнтом злочинної інтенсивності та поясність одержані результати.

11. Проаналізувавши дані статистичної інформації Офісу Генерального прокурора «Єдиний звіт про кримінальні правопорушення» (https://www.gp.gov.ua/ua/1stat),

– побудуйте секторальну діаграму, що відображає структуру кіберзлочинності в Україні за видами кеберзлочинів за останній звітній період (один рік);

– створіть графічне зображення динаміки кіберзлочинності в Україні за останні 5 років та поясність, які чинники можуть впливати на зростання або зниження рівня злочинності.

Література до теми 5

1. Кримінологія : підручник / Б. М. Головкін, В. В. Голіна, О. В. Лисодєд та ін.; за заг. ред. Б. М. Головкіна. Харків: Право, 2020. 384 с.
2. Сметаніна Н. В. Наукові підходи до теорії злочинності у сучасній українській кримінології: монографія. Харків: Право, 2016. 192 с.
3. V. V. Tsypko, K. I. Alieksieieva, I. A. Venger, O. V. Tavolzhanskyi, N. I. Galunets, A. V. Klyuchnik. Information policy of the enterprise as the basis for the reproduction of human potential in the structure of public social interaction // Journal of Advanced Research in Law and Economics (Журнал перспективных исследований в области права и экономики). - 2019. Румыния. - Vol. 10 Issue 6.- P.1664-1672. (Scopus) https://www.scopus.com/record/display.uri?eid=2-s2.0-85087468504&origin=resultslist
4. Головкін Б. М. Теперішнє і майбутнє кримінології. Проблеми законності. 2020. Вип. 149. С. 168–184.

Т е м а 6. **ОСОБА КІБЕРЗЛОЧИНЦЯ.**

Питання для обговорення

1. Поняття особи кіберзлочинця.

2. Структура особистості кіберзлочинця. Соціально-демографічні ознаки особистості кіберзлочинця. Морально-психологічні якості і особистісно-рольові властивості особистості кіберзлочинця.

3. Типологія кіберзлочинців.

4. Наукове і практичне значення вивчення особистості кіберзлочинця та її типології.

Завдання

12. Розкрийте поняття «особа кіберзлочинця». Аргументуйте свою відповідь.

13. Які типології кіберзлочинців Ви знаєте? За якими критеріями проводяться типології кіберзлочинців? Яке практичне значення має типологія кіберзлочинців?

Література до теми 6

1. Кримінологія : підручник / Б. М. Головкін, В. В. Голіна, О. В. Лисодєд та ін. ; за заг. ред. Б. М. Головкіна. Харків : Право, 2020. 384 с.

2. Тимошенко В. І., Шакун В. І. Теоретичні основи кримінології: монографія. Київ: Юрінком Інтер, 2021. 240 с.

3. Гавловський В.Д. Аналіз стану кіберзлочинності в Україні. Інформація і право. № 1(28)/2019. С. 108-117.

4. V. V. Tsypko, K. I. Alieksieieva, I. A. Venger, O. V. Tavolzhanskyi, N. I. Galunets, A. V. Klyuchnik. Information policy of the enterprise as the basis for the reproduction of human potential in the structure of public social interaction // Journal of Advanced Research in Law and Economics (Журнал перспективных исследований в области права и экономики). - 2019. Румыния. - Vol. 10 Issue 6.- P.1664-1672. (Scopus) https://www.scopus.com/record/display.uri?eid=2-s2.0-85087468504&origin=resultslist

5. Головкін Б. М. Теперішнє і майбутнє кримінології. Проблеми законності. 2020. Вип. 149. С. 168–184.

Т е м а **7. ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ: ПОНЯТТЯ, ЗМІСТ, ЗНАЧЕННЯ.**

Питання для обговорення

1. Запобігання кіберзлочинності: поняття, зміст, значення.
2. Поняття і система запобігання кіберзлочинності, класифікація запобіжних заходів.
3. Загально соціальне, спеціально-кримінологічне та індивідуальне запобігання кіберзлочинності і окремих злочинів.
4. Об'єкти запобігання кіберзлочинності.
5. Суб'єкти запобігання кіберзлочинності та основні напрями їх діяльності.

Література до теми 7

1. Про участь громадян в охороні громадського порядку і державного кордону: Закон України від 22.06.2000 № 1835-III URL: https://zakon.rada.gov.ua/laws/show/1835-14#Text
2. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон України від 06.12.2019 № 361-IX URL: https://zakon.rada.gov.ua/laws/show/361-20#Text
3. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
4. Про участь громадян в охороні громадського порядку і державного кордону: Закон України від 22.06.2000 № 1835-III URL: https://zakon.rada.gov.ua/laws/show/1835-14#Text

5. Кримінологія: підручник /Б. М. Головкін, В. В. Голіна, О. В. Лисодєд та ін.; за заг. ред. Б. М. Головкіна. Харків: Право, 2020. 384 с.

6. Велика українська юридична енциклопедія: у 20 т. Т. 18: Кримінологія. Кримінально-виконавче право / редкол.: В. І. Шакун, В. І. Тимошенко. Харків : Нац. акад. прав. наук України; Ін-т держави та права ім. В. М. Корецького НАН України; Нац. юрид. ун-т ім. Ярослава Мудрого. 2019. 544 с.

Тема **8. ПІДХОДИ ДО КЛАСИФІКАЦІЇ КІБЕРЗЛОЧИНІВ. ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИННОСТІ ПРОТИ КОНФІДЕНЦІЙНОСТІ, ЦІЛІСНОСТІ ТА ДОСТУПНОСТІ КОМП'ЮТЕРНИХ ДАНИХ І СИСТЕМ, ТАКІ ЯК НЕЗАКОННИЙ ДОСТУП, НЕЗАКОННЕ ПЕРЕХОПЛЕННЯ, ВТРУЧАННЯ В ДАНІ, ВТРУЧАННЯ В СИСТЕМУ.**

Питання для обговорення

1. Поняття та характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерної інформації.
2. Основні кримінологічні риси особистості кіберзлочинців, які вчиняють злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.
3. Причини та умови злочинів проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.
4. Запобігання кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.

Література до теми 7:

1. Кримінологія : підручник / Б. М. Головкін, В. В. Голіна, О. В. Лисодєда ін.; за заг. ред. Б. М. Головкіна. Харків : Право, 2020. 384 с. (Розділ 12).

2. Фіскальна безпека України – загрози, ризики, вразливості: стратегічна візія / Користін О. Є., Катамадзе Г. Ш., Некрасов В. А., Мельник В. І. та ін. Херсон: Гельветика, 2021. 64 с.

3. Філіппов С. О. Протидія транскордонній злочинності: глобальний контекст і реалії України: монографія. Одеса: Фенікс, 2019. 452 с.

4. Олійник Д. О. Запобігання корупційним злочинам, що вчиняються при здійсненні митних процедур : монографія/наук. ред. Б. М. Головкін. Харків : Право, 2018. 200 с.

Тема **9. ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИНІВ ПОВ'ЯЗАНИХ З ВИКОРИСТАННЯМ КОМП'ЮТЕРА ЯК ЗАСОБУ СКОЄННЯ ЗЛОЧИНІВ, А САМЕ, ЯК ЗАСІБ МАНІПУЛЯЦІЙ З ІНФОРМАЦІЄЮ (КОМП'ЮТЕРНЕ ШАХРАЙСТВО ТА КОМП'ЮТЕРНЕ ПІДРОБЛЕННЯ ТОЩО).**

Питання для обговорення

1. Характеристика кіберзлочинів пов'язаних з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо).

2. Особистість кібершахрая, його основні риси.

3. Причини і умови кіберзлочинів, пов'язаних з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо).

4. Запобігання кіберзлочинам, пов'язаним з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо).

Література до теми 9:

1. Стратегія боротьби з організованою злочинністю, схвалена розпорядженням Кабінету Міністрів України від 16 вересня 2020 р. № 1126-р. URL: https://zakon.rada.gov.ua/laws/show/1126-2020-%D1%80#Text

2. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності та протоколи, що її доповнюють від 15.11.2000 № 55/25, ратифікована законом від 04.02.2004 № 1433-IV URL: https://zakon.rada.gov.ua/laws/show/1433-15#Text

3. Жаровська Г. П. Транснаціональна організована злочинність в Україні: феномен, детермінація, протидія: монографія. Чернівці: Чернівецький національний університет, 2018. 568 с.

Тема **10. ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИНІВ, ПОВ'ЯЗАНИХ З КОНТЕНТОМ (ЗМІСТОМ ДАНИХ), РОЗМІЩЕНИХ У КОМП'ЮТЕРНИХ МЕРЕЖАХ (ЗОКРЕМА ЗЛОЧИНИ, ПОВ'ЯЗАНІ З ДИТЯЧОЮ ПОРНОГРАФІЄЮ).**

Питання для обговорення

1. Загальна характеристика кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією).
2. Особистість кіберзлочинця, основні риси.
3. Причини і умови кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією).
4. Запобігання кіберзлочинам, пов'язаним з контентом (змістом даних), розміщених у комп'ютерних мережах.

Література до теми 5

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Стратегія кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку України», затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

3. Таволжанський О. В. Питання визначення кіберзлочинності в умовах розбудови інформаційного суспільства. *Журнал східноєвропейського права*. 2017. Вип. 45. С. 97-103.

4. Таволжанський О. В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності**.** *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія: Право*. 2018. Вип. 6. С. 154–163.

Тема **11. ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИНІВ, ПОВ'ЯЗАНИХ З ПОРУШЕННЯМ АВТОРСЬКОГО ПРАВА І СУМІЖНИХ ПРАВ.**

.

Питання для обговорення

1. Поняття та характеристика кіберзлочинів, пов'язаних з порушенням авторського права і суміжних прав.
2. Причини та умови кіберзлочинів пов'язаних з порушенням авторського права і суміжних прав.
3. Запобігання кіберзлочинам пов'язаних з порушенням авторського права і суміжних прав.

Література до теми 11

1. Офіційний сайт Офісу Генерального прокурора. Статистика. URL: https://www.gp.gov.ua/ua/1stat

2. Офіційний сайт Державної судової адміністрації України. URL: https://dsa.court.gov.ua/dsa/

3. Про заходи протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та зловживанню ними: Закон України від 15.02.1995р. № 62/95-ВР URL: https://zakon.rada.gov.ua/laws/show/62/95-%D0%B2%D1%80#Text

Тема **12. ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИНІВ, ЗАФІКСОВАНИХ В ОКРЕМОМУ ПРОТОКОЛІ (АКТИ РАСИЗМУ ТА КСЕНОФОБІЇ, ВЧИНЕНІ ЗА ДОПОМОГОЮ КОМП'ЮТЕРНИХ МЕРЕЖ).**

Питання для обговорення

1. Поняття та характеристика кіберзлочинів, зафіксованих в окремому протоколі (акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж).
2. Хуліганство у віртуальній сфері: причини та умови.
3. Запобігання кіберзлочинам проти громадського порядку та моральності.

Література до теми 12

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Таволжанський О. В. Питання визначення кіберзлочинності в умовах розбудови інформаційного суспільства. *Журнал східноєвропейського права*. 2017. Вип. 45. С. 97-103.

3. Таволжанський О. В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності**.** *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія: Право*. 2018. Вип. 6. С. 154–163.

Т е м а **13. КІБЕРЗЛОЧИННІСТЬ У СФЕРІ ЕКОНОМІКИ**

Питання для обговорення

1. Поняття та характеристика кіберзлочинів у сфері економіки.
2. Кирптовалюта та економічні злочини.
3. Особистість кіберзлочинця у сфері економіки, основні риси. Захист об'єктів критичної інфраструктури.
4. Детермінанти кіберзлочинів у сфері економіки. Запобігання кіберзлочинам у сфері економіки.

Література до теми 13

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
2. Таволжанський О. В. Питання визначення кіберзлочинності в умовах розбудови інформаційного суспільства. *Журнал східноєвропейського права*. 2017. Вип. 45. С. 97-103.
3. Таволжанський О. В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності**.** *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія: Право*. 2018. Вип. 6. С. 154–163.

Т е м а **14. ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИНІВ У СФЕРІ ОБІГУ НАРКОТИЧНИХ ЗАСОБІВ.**

Питання для обговорення

1. Поняття та характеристика кіберзлочинів у сфері обігу наркотичних засобів.
2. Причини та умови кіберзлочинів у сфері обігу наркотичних засобів.

3. Запобігання кіберзлочинам у сфері обігу наркотичних засобів. Поняття та взаємозв'язок організованої злочинності та кіберзлочинності.

.

Література до теми 14

1. Офіційний сайт Офісу Генерального прокурора. Статистика. URL: https://www.gp.gov.ua/ua/1stat

2. Офіційний сайт Державної судової адміністрації України. URL: https://dsa.court.gov.ua/dsa/

3. Про заходи протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та зловживанню ними: Закон України від 15.02.1995р. № 62/95-ВР URL: https://zakon.rada.gov.ua/laws/show/62/95-%D0%B2%D1%80#Text

Тема **15. ГІБРИДНІ ВІЙНИ.**

Питання для обговорення

4. Характеристика кіберзлочинів у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації.

5. Причини та умови кіберзлочинів у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення.

6. Поняття військових кіберзлочинів та їх характеристика. призову та мобілізації.

7. Запобігання кіберзлочинам у сфері охорони державної таємниці, недоторканості державних кордонів, забезпечення призову та мобілізації.

Література до теми 15

4. Офіційний сайт Офісу Генерального прокурора. Статистика. URL: https://www.gp.gov.ua/ua/1stat

5. Офіційний сайт Державної судової адміністрації України. URL: https://dsa.court.gov.ua/dsa/

6. Про наркотичні засоби, психотропні речовини та прекурсори: Закон України від 15.02.1995 р. № 60/95-ВР. URL: https://zakon.rada.gov.ua/laws/show/60/95-%D0%B2%D1%80#Text

7. Про заходи протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та зловживанню ними: Закон України від 15.02.1995р. № 62/95-ВР URL: https://zakon.rada.gov.ua/laws/show/62/95-%D0%B2%D1%80#Text

8. Проєкт розпорядження Кабінету Міністрів України «Про схвалення Стратегії державної політики щодо наркотиків на період до 2030 року». URL: https://www.dls.gov.ua/for_subject/%D0%BC%D0%BE%D0%B7-%D0%BF%D1%80%D0%BE%D0%BF%D0%BE%D0%BD%D1%83%D1%94-%D0%B7%D0%B0%D1%82%D0%B2%D0%B5%D1%80%D0%B4%D0%B8%D1%82%D0%B8-%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%8E-%D0%B4%D0%B5/

Т е м а **16. КОРУПЦІЯ У ВІРТУАЛЬНІЙ СФЕРІ.**

Питання для обговорення

1. Визначення корупції як соціального явища та зв'язок з новітніми технологіями, види корупційних кіберпроявів. Характеристика корупційної кіберзлочинності.
2. Причини та умови корупційної кіберзлочинності.
3. Запобігання корупційній кіберзлочинності.

Література до теми 16

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Таволжанський О. В. Питання визначення кіберзлочинності в умовах розбудови інформаційного суспільства. *Журнал східноєвропейського права*. 2017. Вип. 45. С. 97-103.

3. Таволжанський О. В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності**.** *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія: Право*. 2018. Вип. 6. С. 154–163.

Т е м а **17. ХАРАКТЕРИСТИКА ЗЛОЧИННОСТІ НЕПОВНОЛІТНІХ У ВІРТУАЛЬНІЙ СФЕРІ.**

Питання для обговорення

1. Поняття та характеристика злочинності неповнолітніх у віртуальній сфері.
2. Особистість неповнолітнього кіберзлочинця, основні риси.
3. Причини та умови кіберзлочинності неповнолітніх.
4. Запобігання кіберзлочинності неповнолітніх.

Література до теми 17

1. Про участь громадян в охороні громадського порядку і державного кордону: Закон України від 22.06.2000 № 1835-III URL: https://zakon.rada.gov.ua/laws/show/1835-14#Text

2. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

3. Кримінологія: підручник /Б. М. Головкін, В. В. Голіна, О. В. Лисодєд та ін.; за заг. ред. Б. М. Головкіна. Харків: Право, 2020. 384 с.

4. Велика українська юридична енциклопедія: у 20 т. Т. 18: Кримінологія. Кримінально-виконавче право / редкол.: В. І. Шакун, В. І. Тимошенко. Харків : Нац. акад. прав. наук України;

Ін-т держави та права ім. В. М. Корецького НАН України; Нац. юрид. ун-т ім. Ярослава Мудрого. 2019. 544 с.

САМОСТІЙНА РОБОТА СТУДЕНТІВ

Самостійна робота – вид позааудиторної роботи навчального характеру, яка спрямована на вивчення програмного матеріалу курсу, під час якої студент має самостійно опрацювати конспекти лекцій, рекомендовану літературу, нормативні акти, матеріали емпіричних досліджень до тем, що виносяться на практичні заняття.

Формами її є: індивідуальна письмова робота; доопрацювання матеріалів лекції; робота над кейсами з питань розроблення заходів запобігання кримінальним правопорушенням; робота в інформаційних мережах; наукове повідомлення за вузькоспеціальною проблематикою; підготовка тематичних презентацій; написання та публікація наукових статей, тез тощо; розробка схем, таблиць за темами навчальної дисципліни; анотування наукових статей і монографій; здійснення аналізу законопроєктів та змін законодавства.

Самостійна робота студентів полягає в опануванні додаткової навчальної, наукової літератури, ознайомленні із законодавством у сфері запобігання кіберзлочинам у інших країн, вивченні зарубіжного досвіду та кращих практик протидії злочинності; призначена для поглиблення знань за темами, що передбачені навчальною дисципліною, і має на меті формування вмінь самостійно працювати із реєстрами органів правопорядку, міжнародними договорами і документами, законами, іншими нормативними правовими актами та спеціальною літературою. У процесі занять студентам надається методична допомога, а також провадиться контроль за їх самостійною роботою.

5. СЛОВНИК ОСНОВНИХ ТЕРМІНІВ І ПОНЯТЬ ДИСЦИПЛІНИ «ЗАПОБІГАННЯ КІБЕРЗЛОЧИНАМ»

індикатори кіберзагроз - показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;

інформація про інцидент кібербезпеки - відомості про обставини кіберінциденту, зокрема про те, які об'єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;

інцидент кібербезпеки (далі - кіберінцидент) - подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

кібератака - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються

(передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

кібербезпека - 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;

кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;

кіберзахист - 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;

кіберзлочин (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом

України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

кіберзлочинність - сукупність кіберзлочинів;

кібероборона - 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;

кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;

кіберрозвідка - діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням;

кібертероризм - терористична діяльність, що здійснюється у кіберпросторі або з його використанням;

кібершпигунство - шпигунство, що здійснюється у кіберпросторі або з його використанням;

критична інформаційна інфраструктура - сукупність об'єктів критичної інформаційної інфраструктури;

критично важливі об'єкти інфраструктури (далі - об'єкти критичної інфраструктури) - підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей;

Національна телекомунікаційна мережа - сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам;

національні електронні інформаційні ресурси (далі - національні інформаційні ресурси) - систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи

публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів;

об'єкт критичної інформаційної інфраструктури - комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури;

система управління технологічними процесами (далі - технологічна система) - автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних;

системи електронних комунікацій (далі - комунікаційні системи) - системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв'язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації

(передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних.

ПОТОЧНИЙ ТА ПІДСУМКОВИЙ КОНТРОЛЬ ЗНАНЬ СТУДЕНТІВ

Опис предмета курсу

Курс	Рівень вищої освіти, галузь знань, спеціальність	Характеристика (структура) навчального курсу	
		денна форма навчання	заочна форма навчання
Кількість кредитів ЄКТС – 6,0	Бакалавр 08 «Право» 081 «Право»	вибіркова	вибіркова
Кількість модулів – 3		Рік підготовки: 2021–2022	Рік підготовки: 2021–2022
Загальна кількість годин – 180		Семестр: 3–8	Семестр: 3–8
		Лекції: 32 год	Лекції: 16 год
		Практичні/ семінарські заняття: 36 год	Практичні/ семінарські заняття: 8 год
		Самостійна робота: 112 год	Самостійна робота: 156 год
		Види контролю: поточний контроль; підсумковий контроль знань –залік	Види контролю: поточний контроль; підсумковий контроль знань – залік

Організація поточного контролю

Оцінювання знань студентів здійснюється на основі результатів поточного контролю. Завдання ПК – перевірка розуміння та опанування навчального матеріалу змістового модуля, здатності осмислити зміст теми чи розділу, умінь застосовувати отримані кримінологічні знання при вирішенні професійних завдань. Загальним об'єктом оцінювання знань студентів є відповідна частина навчальної програми з навчальної дисципліни "Запобігання кіберзлочинам", засвоєння якої перевіряється під час поточного контролю. Об'єктами поточного контролю знань студентів з дисципліни «Запобігання кіберзлочинам» виступають їх успішність на практичних заняттях, виконання контрольних та індивідуальних завдань. Поточний контроль має на меті перевірку рівня підготовки студента у вивченні поточного матеріалу. У ході практичного заняття студент може отримати оцінку за чотирибальною шкалою (0, 3, 4, 5);

Упродовж семестру студенти виконують завдання для самостійної роботи (підготовка презентації, есе, реферату тощо). Максимальна кількість балів за самостійну роботу – 10.

Оцінювання результатів ПК здійснюється викладачем наприкінці вивчення дисципліни. Критеріями оцінювання ПК є: систематичність, активність та успішність роботи студента на практичних заняттях, а також оцінка за контрольну роботу. Виконання контрольних завдань може проводитися у формі тестування. Підсумковий бал за результатами ПК оформляється під час останнього практичного заняття відповідного семестру.

Формою підсумкового контролю знань здобувачів вищої освіти з навчальної дисципліни є залік. Мінімальна кількість балів для отримання заліку – 60.

Розподіл балів між формами організації освітнього процесу і видами контрольних заходів:

Поточний контроль						Самостійна робота студентів	Підсумкова оцінка знань (залік)
Модуль I		Модуль II		Модуль III			
п/з	коло-квіум	п/з	коло-квіум	п/з	коло-квіум		
Max 15	Max 5	Max 20	Max 5	Max 40	Max 5	Max 10	Max 100

Критерії оцінювання результатів навчання

Вид контролю	Кількість балів	Критерії (за кожною з оцінок)
Поточний контроль на практичному занятті	Max 5	Відмінне засвоєння навчального матеріалу за темою, можливі окремі несуттєві недоліки
	4	Добре засвоєння матеріалу за темою, але є окремі помилки
	3	Задовільний рівень засвоєння матеріалу, значна кількість помилок
	Min 0	Незадовільний рівень засвоєння матеріалу
Колоквіум	Max 5	Результати опрацювання матеріалу високі, можлива незначна кількість несуттєвих помилок
	4	Добре засвоєння матеріалу за

		темою, але є окремі помилки
	3	Задовільний рівень засвоєння матеріалу, значна кількість несуттєвих помилок
	2	Задовільний рівень засвоєння матеріалу, значна кількість суттєвих помилок
	1	Прогалини в знаннях, студент слабко володіє матеріалом
	Min 0	Незадовільний рівень засвоєння матеріалу
Оцінка самостійної роботи студента	Max 10	Глибоке знання проблем, пов'язаних із темою дослідження. Вільне володіння матеріалом, вміння самостійно і творчо мислити, знаходити, узагальнювати, аналізувати матеріал, робити самостійні теоретичні і практичні висновки
	5	Основні питання висвітлено поверхово, висновки не мають самостійного характеру
	Min 0	Основні положення теми висвітлено поверхово, з великою кількістю помилок, немає висновків, курсант/ студент слабко володіє матеріалом
Залік	Min 60	Достатнє засвоєння матеріалу із дисципліни
	Max 100	Відмінне оволодіння матеріалом із дисципліни

Шкала підсумкового педагогічного контролю

Оцінка за шкалою ECTS	Визначення	Оцінка за національною шкалою	Оцінка за 100-бальною шкалою, що використовується в НЮУ імені Ярослава Мудрого
A	**Відмінно** – відмінне виконання, лише з незначною кількістю помилок	зараховано	90 – 100
B	**Дуже добре** – вище середнього рівня з кількома помилками		80 – 89
C	**Добре** – у цілому правильна робота з певною кількістю незначних помилок		75 – 79
D	**Задовільно** – непогано, але зі значною кількістю недоліків		70 – 74
E	**Достатньо** – виконання задовольняє мінімальні критерії		60 – 69
FX	**Незадовільно** – потрібно попрацювати перед тим, як перескласти	не зараховано	35 – 59
F	**Незадовільно** – необхідна серйозна подальша робота, обов'язковий повторний курс		0 – 34

ПРОГРАМНІ ПИТАННЯ

1. Основні ціла, напрями та принципи державної політики у сфері кібербезпеки.
2. Правові основи забезпечення кібербезпеки України.
3. Об’єкти кібербезпеки та кіберзахисту.
4. Суб’єкти забезпечення кібербезпеки.
5. Стратегія, законодавство, напрямки сучасної політики у сфері кібербезпеки в Україні та зарубіжних країнах.
6. Концепція розвитку науки щодо запобігання кіберзлочинності в Україні на початку XXI століття.
7. Поняття і визначення кіберзлочину.
8. Кіберзлочин як соціально-правове явище, особа кіберзлочинця, детермінація кіберзлочинності, запобігання кіберзлочинності.
9. Запобігання кіберзлочинам як міжгалузева дисципліна.
10. Класифікація кіберзлочинів.
11. Запобігання кіберзлочинності на сучасному етапі розвитку України і в перспективі.
12. Поняття кіберзлочинності та основні науково-практичні підходи щодо її розуміння і визначення.
13. Кількісно-якісне вимірювання кіберзлочинності.
14. Рівень кіберзлочинності. Структура кіберзлочинності.
15. Кримінально-правові ознаки структури кіберзлочинності.
16. Кримінологічні ознаки структури кіберзлочинності.
17. Динаміка кіберзлочинності. Технічні соціальні правові фактори, які впливають на динаміку кіберзлочинності. фактори, які впливають на динаміку кіберзлочинності.
18. Географія кіберзлочинності та топографія кіберзлочинності. Ціна кіберзлочинності.
19. Латентність кіберзлочинності. Структура латентної кіберзлочинності. Загальна характеристика сучасної кіберзлочинності в Україні, тенденції її розвитку.
20. Зміст поняття кіберзлочинець й основні підходи до його визначення. Структура особистості кіберзлочинця.
21. Соціально-демографічні ознаки особистості кіберзлочинця.

22. Морально-психологічні якості і особистісно-рольові властивості особистості кіберзлочинця.
23. Типологія кіберзлочинців. Наукове і практичне значення вивчення особистості кіберзлочинця та її типології.
24. Поняття причини кіберзлочину.
25. Умови, що сприяють вчиненню кіберзлочину. Умови формування кримінальної мотивації та мотивів. Умови реалізації мотивів і рішення про вчинення кіберзлочину.
26. Політика в сфері запобігання кіберзлочинності: поняття, зміст, значення.
27. Поняття і система запобігання кіберзлочинності, класифікація запобіжних заходів. Загально соціальне, спеціально-кримінологічне та індивідуальне запобігання кіберзлочинності і окремих злочинів.
28. Об'єкти запобігання кіберзлочинності.
29. Суб'єкти запобігання кіберзлочинності та основні напрями їх діяльності.
30. Прогнозування в сфері кіберзахисту. Поточне прогнозування. Короткострокове прогнозування. Середньострокове прогнозування. Перспективне прогнозування. Головні етапи планування.
31. Підходи до класифікації кіберзлочинів.
32. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.
33. Основні кримінологічні риси особистості кіберзлочинців, які вчиняють злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.
34. Причини та умови злочинів проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.

35. Запобігання кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.
36. Характеристика кіберзлочинів пов'язаних з використанням комп'ютера , як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо).
37. Особистість кібершахрая, основні риси.
38. Причини і умови кіберзлочинів, пов'язаних з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо).
39. Запобігання кіберзлочинам, пов'язаним з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо).
40. Характеристика кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією).
41. Особистість кіберзлочинця, основні риси. Причини і умови кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією).
42. Характеристика кіберзлочинів, пов'язаних з порушенням авторського права і суміжних прав.
43. Причини та умови кіберзлочинів пов'язаних з порушенням авторського права і суміжних прав.
44. Запобігання кіберзлочинам пов'язаних з порушенням авторського права і суміжних прав.
45. Поняття та кримінологічна характеристика кіберзлочинів, зафіксованих в окремому протоколі (акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж).
46. Хуліганство у віртуальній сфері.
47. Запобігання кіберзлочинам проти громадського порядку та моральності.

48. Кіберзлочинність у сфері економіки.
49. Характеристика кіберзлочинів у сфері економіки.
50. Особистість кіберзлочинця, основні риси.
51. Причини та умови кіберзлочинів у сфері економіки. Запобігання кіберзлочинам у сфері економіки.
52. Характеристика кіберзлочинів у сфері обігу наркотичних засобів.
53. Причини та умови кіберзлочинів у сфері обігу наркотичних засобів.
54. Запобігання кіберзлочинам у сфері обігу наркотичних засобів.
55. Гібридна війна. Характеристика кіберзлочинів у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації.
56. Причини та умови кіберзлочинів у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення.
57. Поняття та взаємозв'язок організованої злочинності та кіберзлочинності. Характеристика організованої кіберзлочинності.
58. Міжнародне співробітництво у сфері запобігання організованій злочинності.
59. Корупція у віртуальній сфері. Визначення корупції як соціального явища та зв'язок з новітніми технологіями, види корупційних кіберпроявів.
60. Характеристика злочинності неповнолітніх у віртуальній сфері. Запобігання кіберзлочинності неповнолітніх.

З М І С Т

Н а в ч а л ь н е в и д а н н я

Електронне видання

МЕТОДИЧНІ МАТЕРІАЛИ ДО ВИВЧЕННЯ

НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ЗАПОБІГАННЯ КІБЕРЗЛОЧИНАМ»

для студентів
першого (бакалаврського) рівня вищої освіти
галузі знань 26 «Цивільна безпека»
спеціальності 262 «Правоохоронна діяльність»

У к л а д а ч : Таволжанський Олексій Володимирович

Відповідальний за випуск *Б. М. Головкін*

Редактор *Л. М. Рибалко*