Національний юридичний університет імені Ярослава Мудрого

Кафедра кримінології та кримінально-виконавчого права

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Кіберзлочинність та електронні докази»

Рівень вищої освіти – другий (магістерський) рівень

Ступінь вищої освіти – магістр

Галузь знань – 08 «Право»

Спеціальність – 081 «Право»

Спеціалізація – «Прокуратура та кримінальна юстиція»

Статус навчальної дисципліни – за вибором студента

Рік набору – 2021

Харків – 2021

Робоча програма навчальної дисципліни «Кіберзлочинність та

електронні докази» для здобувачів вищої освіти другого (магістерського) рівня вищої освіти галузі знань 08 «Право» спеціальності 081 «Право» спеціалізації «Прокуратура та кримінальна юстиція» Інституту прокуратури та кримінальної юстиції. Харків: Нац. юрид. ун-т імені Ярослава Мудрого, 2021. 17 с.

Розробник:

Таволжанський Олексій Володимирович – доцент кафедри кримінології та кримінально-виконавчого права, кандидат юридичних наук, Національного юридичного університету імені Ярослава Мудрого, кандидат юридичних наук, доцент

Затверджено на засіданні кафедри кримінології та кримінально-виконавчого права
(протокол № від 20__ р.)

Завідувач кафедри кримінології та кримінально-виконавчого права –

Головкін Богдан Миколайович, доктор юридичних наук, професор

Гарант освітньої програми – завідуюча кафедри кримінального процесу

Капліна Оксана Володимирівна, доктор юридичних наук, професор

Формуляр розроблений робочої групою у складі:

- *проф. Комаров В. – проректор з навчально-методичної роботи;*
- *проф. Клімова Г. – начальник навчально-методичного відділу;*
- *к.ю.н. Яригіна Є. – методист навчально-методичного відділу*

та затверджено на засіданні Науково-методичної ради (протокол №2 від 23.03.2021 р.)

Голова Науково-методичної ради

_____ *Комаров В.*

Зміст

1. Опис навчальної дисципліни……..4

2. Очікувані результати навчання…….… 5

3. Обсяг і структура навчальної дисципліни…….……7

3.1. Для здобувачів вищої освіти денної форми навчання……..7

3.2. для здобувачів вищої освіти заочної форми навчання……..8

4. Форми педагогічного контролю та засоби оцінювання результатів навчання …….…….…….9

5. Критерії оцінювання результатів навчання……9

6. Педагогічний контроль для здобувачів вищої освіти заочної форми навчання……11

7. Навчально-методичне та інформаційне забезпечення навчальної дисципліни……12

1. Опис навчальної дисципліни

Робоча програма навчальної дисципліни «Кіберзлочинність та електронні докази» розроблена відповідно до освітньо-професійної програми «Прокуратура та кримінальна юстиція» другого (магістерського) рівня вищої освіти галузі знань 08 «Право» спеціальності 081 «Право» спеціалізації «Прокуратура та кримінальна юстиція» Інституту прокуратури та кримінальної юстиції. Харків: Нац. юрид. ун-т імені Ярослава Мудрого, 2021. ____ с.

Найменування показників	Галузь знань, спеціальність, рівень освіти	Дидактична структура навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів ЄКТС - 2	Галузь знань – 08 «Право» Спеціальність – 081 «Право» Спеціалізація – «Прокуратура та кримінальна юстиція» Рівень освіти – другий (магістерський)	За вибором студента	За вибором студента
Кількість модулів – 2		Рік підготовки: 1	Рік підготовки: 1
		семестр	семестр
Загальна кількість годин - 60		1	1
Тижневих годин для денної форми навчання: аудиторних – 2-4, самостійної роботи студента - 6-8.		**Лекції**	**Лекції**
		16 год.	год.
		Практичні/ семінарські заняття	**Практичні /семінарські заняття**
		14 год.	год.
		Самостійна робота	**Самостійна робота**
		30 год.	год.
		Види контролю: поточний контроль; підсумковий контроль знань (залік)	Види контролю: поточний контроль; підсумковий контроль знань (залік)

***Мета* навчальної дисципліни** – теоретично і практично озброїти студента знаннями про соціальну сутність і детермінацію кіберзлочинності та її окремих злочинних проявів (кардинг, фішинг, вішинг, онлайн-шахрайство, піратство, кард-шарінг, соціальна інженерія, мальваре, протиправний контент рефайлінг та ін.), основні напрями запобіжної діяльності державних органів, установ і громадських організацій, систему заходів, які ними розробляються і реалізуються відповідно до Конституції України, законів та інших нормативно-правових актів, спрямованих на недопущення вчинення кіберзлочинів, захист прав та законних інтересів громадян, зниження «страху населення» перед кіберзлочинністю.

Завдання:

- вивчення актуальних проблем запобігання кіберзлочинності;

- формування у студентів уявлення про поняття, зміст, види та засоби запобігання кіберзлочинності;

- визначення прикладних доказування у кіберсфері.

***Пререквізити**: «Кримінальне право»; «Кримінально-процесуальне право»; «Адміністративне право; Кримінально-виконавче право».*

***Кореквізити**: «Кримінальне право»; «Кримінально-процесуальне право»; «Адміністративне право; Кримінально-виконавче право».*

***Постреквізити**: "Кримінальне право»; «Кримінально-процесуальне право; криміналістика»; «Правові засади запобігання корупції».*

2. Очікувані результати навчання

У результаті засвоєння навчальної дисципліни здобувач вищої освіти повинен демонструвати такі результати навчання: *

РН-1.	Демонструвати знання і розуміння положень кримінального права, кримінального процесуального права, кримінології, криміналістики та оперативно-розшукової діяльності, із застосуванням окремих норм законодавства при запобіганні та розслідуванні злочинів з урахуванням їх специфіки
РН 2.	Аналізувати причини та умови вчинення економічних злочинів, а також злочинів у складі організованих злочинних груп і злочинних організацій
РН-3.	Застосовувати теоретичні, нормативні і методологічні засади боротьби з організованою злочинністю при здійсненні оперативно-розшукових заходів, запобіганні та розслідуванні злочинів, припиненні діяльності організованих злочинних угруповань
РН-4.	Охарактеризувати механізм координації діяльності у сфері боротьби з організованою та економічною злочинністю з урахуванням практики країн - членів ЄС, а також міжвідомчої взаємодії і міжнародної співпраці у цій сфері;
РН-5.	Розробляти комплексні плани протидії економічній та організованій злочинності на стратегічному і тактичному рівнях, а також застосовувати заходи із виявлення, ліквідації кримінальних мереж; виявлення і припинення джерел фінансування доходів, отриманих організованими злочинними угрупованнями; відстеження грошових потоків і поверненні активів, одержаних від корупційних та економічних злочинів
РН-6.	Здійснювати кваліфікацію тяжких та особливо тяжких злочинів, що вчиняються у складі організованих злочинних груп і злочинних організацій
РН-7.	Самостійно планувати, організовувати, підготовлювати та здійснювати слідчі

	(розшукові) та негласні слідчі (розшукові) дії, з подальшим аналізом отриманих результатів; самостійно організовувати роботу слідчої чи слідчо-оперативної групи в процесі виявлення, запобігання та розслідування злочинів

Викладання навчальної дисципліни забезпечує формування у здобувача вищої освіти загальних і спеціальних компетентностей та досягнення результатів навчання, визначених стандартом вищої освіти відповідної спеціальності та освітньо-професійною програмою «Прокуратура та кримінальна юстиція», а саме:

ЗК-1 Здатність до абстрактного мислення, аналізу та синтезу знань, набутих у процесі навчання та/або професійної діяльності на рівні новітніх досягнень, які є основою для оригінального мислення та інноваційної діяльності

ЗК-2 Уміння застосовувати отримані знання у практичних ситуаціях в умовах розв'язання складних непередбачуваних задач і проблем у професійній діяльності судді, слідчого, прокурора

ЗК-4 Уміння розв'язувати складні задачі і проблеми у професійній діяльності або у процесі навчання, що передбачає проведення наукових досліджень та впровадження інновацій

ЗК-6 Уміння самостійно здобувати знання, використовуючи різні джерела інформації; здатність до подальшого навчання і професійного самоудосконалення

ЗК-10 Здатність формулювати особисту думку та доказово її представляти

Спеціальних компетентностей:

СК-1. Здатність застосовувати принципи верховенства права для розв'язання складних задач і проблем, у тому числі, у ситуаціях правової невизначеності.

СК-4. Здатність оцінювати взаємодію міжнародного права та міжнародних правових систем з правовою системою України.

СК-5. Здатність використовувати сучасні правові доктрини та принципи у правотворчості та в процесі застосовування інститутів кримінальної юстиції.

СК-6. Здатність обґрунтовувати та мотивувати правові рішення, давати розгорнуту юридичну аргументацію.

СК-9. Здатність застосовувати міждисциплінарний підхід в оцінці правових явищ та правозастосовній діяльності.

СК-10. Здатність ухвалювати рішення у ситуаціях, що вимагають системного, логічного та функціонального тлумачення норм права, а також розуміння особливостей практики їх застосування.

СК-12. Здатність розвивати та утверджувати етичні стандарти правничої діяльності, стандарти професійної незалежності та відповідальності правника.

СК-13. Здатність доносити до фахівців і нефахівців у сфері права

інформацію, ідеї, зміст проблем та характер оптимальних рішень з належною аргументацією.

СК-15. Здатність самостійно готувати проекти актів правозастосування, враховуючи вимоги щодо їх законності, обґрунтованості та вмотивованості.

Програмних результатів навчання:

Демонструвати знання та розуміння різних концепцій, а також положень міжнародних стандартів щодо поняття, сутності та провів кіберзлочинності; ознак конвенційних злочинів, що охоплюються цими поняттями.

Класифікувати види кіберзлочинності за різними критеріями; охарактеризувати особливості здійснення транснаціональної організованої злочинної діяльності, а також типові способи вчинення тяжких та особливо тяжких злочинів у складі організованих злочинних груп і злочинних організацій.

Узагальнювати результати слідчої, оперативно-розшукової та судової практики..

Застосовувати знання положень Конвенцій ООН, міжнародних договорів, норм національного законодавства, практики ЄСПЛ у сфері боротьби кіберзлочинністю, а також поняття вказаних видів злочинності, причини та умов вчинення таких злочинів.

Розв’язувати проблемні ситуації, що виникають при виявленні, запобіганні, припиненні та розслідуванні злочинів, що вчиняються у кіберсфері.

3. Обсяг і структура навчальної дисципліни

3.1. Для здобувачів вищої освіти денної форми навчання

№ п/п	Дата проведення (згідно розкладу)	Тематика навчального курсу	Обсяг у годинах			
			Усього	У тому числі		
				Лекції	Практичні заняття, семінарські заняття, колоквіуми тощо	Самостійна робота
		Модуль 1. Кіберзлочинність: поняття, види та запобігання.				
		Тема 1. Поняття кіберзлочинності та її місце в загальній структурі злочинності. Види кіберзлочинів.	12	2	2	8
		Тема 2. Поняття	12	2	2	8

		та кримінологічна характеристика кіберзлочинності. Особистість кіберзлочинця. Причини та умови вчинення кіберзлочинів. Запобігання кіберзлочинності.				
		Тема 3. Європейський конвенційний механізм запобігання кіберзлочинності: поняття та система.	*12*	*2*	*2*	*8*
		Тема 4. Детермінанти та основні напрямки запобігання кіберзлочинності	*12*	*2*	*2*	*8*
12	2	**Модуль 2. Кримінально-правове забезпечення боротьби з кіберзлочинністю.**	8			
		Тема 1. Сучасний стан кримінально-правового забезпечення боротьби з кіберзлочинністю.	12	4	4	4
		Тема 2. Система та загальна характеристика кіберзлочинів.	12	4	4	4
		Тема 3. Реалізація форм кримінальної відповідальності за кіберзлочини.	12	4	2	6

		Тема 4. Особливості методики розслідування кіберзлочинів.	12	2	2	6
		Тема 5. Поняття електронних доказів у кримінальному провадженні Види електронних доказів	12	2	2	8
		Тема 6. Способи збирання електронних доказів**.** Використання електронних доказів під час судового розгляду	12	2	2	8
		Разом	*36*	*12*	*10*	*14*
		Усього годин / кредитів ECTS	**60/2**	**16/0,5**	**14/05**	**30/1**

3.2. Для здобувачів вищої освіти заочної форми навчання

№ п/п	**Дата проведення (згідно розкладу)**	**Тематика навчального курсу**	**Обсяг у годинах**			
			Усього	**У тому числі**		
				Лекції	**Практичні заняття, семінарські заняття, колоквіуми тощо**	**Самостійна робота**
		Модуль 1. Кіберзлочинність: поняття, види та запобігання.				
		Тема 1. Поняття кіберзлочинності та її місце в загальній структурі злочинності. Види кіберзлочинів.	12	2	2	8
		Тема 2. Поняття	12	2	2	8

		та кримінологічна характеристика кіберзлочинності. Особистість кіберзлочинця. Причини та умови вчинення кіберзлочинів. Запобігання кіберзлочинності.				
		Тема 3. Європейський конвенційний механізм запобігання кіберзлочинності: поняття та система.	*12*	*2*	*2*	*8*
		Тема 4. Детермінанти та основні напрямки запобігання кіберзлочинності	*12*	*2*	*2*	*8*
12	2	2	8	*4*	*4*	*16*
12	2	**Модуль 2. Кримінально-правове забезпечення боротьби з кіберзлочинністю.**	8			
		Тема 1. Сучасний стан кримінально-правового забезпечення боротьби з кіберзлочинністю.	12	4	4	4
		Тема 2. Система та загальна характеристика кіберзлочинів.	12	4	4	4
		Тема 3. Реалізація форм кримінальної відповідальності за	12	4	2	6

		кіберзлочини.				
		Тема 4. Особливості методики розслідування кіберзлочинів.	12	2	2	6
		Тема 5. Поняття електронних доказів у кримінальному провадженні Види електронних доказів	12	2	2	8
		Тема 6. Способи збирання електронних доказів**.** Використання електронних доказів під час судового розгляду	12	2	2	8
		Разом	*36*	*12*	*10*	*14*
		Усього годин / кредитів ECTS	**60/2**	**16/0,5**	**14/05**	**30/1**

4. Форми педагогічного контролю та засоби оцінювання результатів навчання

Оцінювання результатів засвоєння навчальної дисципліни «назва навчальної дисципліни» передбачає проведення поточного та підсумкового контролю і здійснюється на основі накопичувальної бально-рейтингової системи.

Поточний контроль знань включає:

- контроль якості засвоєння студентами програмного матеріалу навчальної дисципліни на *практичних заняттях* із застосуванням таких засобів: усне, письмове або експрес-опитування, виконання текстових завдань, вирішення практичних завдань або задач, участь у розробці кейсу, підготовка і захист есе або реферату за ініціативи студента;
- контроль якості засвоєння студентами програмного матеріалу навчальної дисципліни, що проводяться наприкінці модулів (колоквіуми, контрольні роботи тощо).

Протягом семестру студенти виконують завдання для *самостійної роботи* (підготовка презентації, есе, реферату тощо). Максимальна кількість

балів за самостійну роботу – 10.

Формою *підсумкового контролю* знань здобувачів вищої освіти з навчальної дисципліни є залік.

5. Критерії оцінювання результатів навчання

Розподіл балів між формами організації освітнього процесу і видами контрольних заходів навчальної дисципліни «Етика судді, прокурора, слідчого» для здобувачів вищої освіти денної форми навчання при підсумковому контролі у формі заліку:

Поточний контроль		Самостійна робота студентів	Підсумкова оцінка знань (залік)
Практичні заняття			
Модуль № 1	Модуль № 2		
max 20	Max 30	Max 10	max 100

Вид контролю	Кількість балів	Критерії (за кожною з оцінок)
Поточний контроль на практичному/ семінарському занятті	Max 4	Відмінне засвоєння навчального матеріалу з теми, можливі окремі несуттєві недоліки.
	3	Добре засвоєння матеріалу з теми, але є окремі помилки
	2	Задовільний рівень засвоєння матеріалу, значна кількість помилок
	1	Мінімальні результати, достатні для отримання позитивної оцінки
	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 й творчо мислити, знаходити, узагальнювати, аналізувати матеріал, робити самостійні теоретичні та практичні висновки.
	8	В роботі розкрито основні положення теми, але є деякі неточності у викладанні матеріалу, теоретичні поняття недостатньо підкріплено фактичними даними
	6	Основні положення теми розкрито, але деякі питання висвітлено неповно. Студент добре володіє матеріалом, але відсутня творчість та самостійність у дослідженні
	4	Основні теоретичні питання висвітлено поверхнево, немає висновків або висновки не мають самостійного характеру; студент слабко володіє матеріалом
	2	Основні положення теми висвітлено поверхнево, теоретичні положення не підкріплені фактичним матеріалом; немає висновків; студент слабко володіє матеріалом роботи.

	Min 0	Основні положення теми висвітлено поверхнево, з великою кількістю помилок; немає висновків; студент не володіє матеріалом роботи.
ЗАЛІК	Max 60	1. Всебічне, систематичне і глибоке знання матеріалу, передбаченого програмою навчальної дисципліни, у тому числі орієнтація в основних наукових доктринах та концепціях дисципліни. 2. Засвоєння основної та додаткової літератури, рекомендованої кафедрою. 3. Здатність до самостійного поповнення знань з дисципліни та використання отриманих знань у практичній роботі.
	55	1. Повне знання матеріалу, передбаченого програмою навчальної дисципліни. 2. Засвоєння основної літератури та знайомство з додатковою літературою, рекомендованою кафедрою. 3. Здатність до самостійного поповнення знань з дисципліни, розуміння їх значення для практичної роботи.
	50	1. Достатньо повне знання матеріалу, передбаченого програмою навчальної дисципліни, за відсутності у відповіді суттєвих неточностей. 2. Засвоєння основної літератури, рекомендованої кафедрою. 3. Здатність до самостійного поповнення знань з дисципліни, розуміння їх значення для практичної роботи.
	45	1. Знання основного матеріалу, передбаченого програмою навчальної дисципліни, в обсязі, достатньому для подальшого навчання і майбутньої роботи за професією. 2. Засвоєння основної літератури, рекомендованої кафедрою. 3. Помилки та суттєві неточності у відповіді на іспиті за наявності знань для їх самостійного усунення або за допомогою викладача.
	40	1. Знання основного матеріалу, передбаченого програмою навчальної дисципліни, в обсязі, достатньому для подальшого навчання і майбутньої роботи за професією. 2. Ознайомлення з основною літературою, рекомендованою кафедрою. 3. Помилки у відповіді на іспиті за наявності знань для усунення найсуттєвіших помилок за допомогою викладача.
	35	1. Прогалини в знаннях з певних частин основного матеріалу, передбаченого програмою навчальної дисципліни.

		2. Наявність помилок у відповіді на іспиті.
	Min 0	1. Відсутність знань значної частини основного матеріалу, передбаченого програмою навчальної дисципліни. 2. Неможливість продовжити навчання або здійснювати професійну діяльність без проходження повторного курсу з цієї дисципліни.

6. Педагогічний контроль для здобувачів вищої освіти заочної форми навчання

Шкала підсумкового педагогічного контролю (залік)

Оцінка за шкалою ECTS	Визначення	Оцінка за національною шкалою для заліку	Оцінка за 100- бальною шкалою, що використовується в НЮУ
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 перескладати	не зараховано	35 – 59
F	**Незадовільно** – необхідна серйозна подальша робота, обов'язковий повторний курс		0 – 34

7. Навчально-методичне та інформаційне забезпечення навчальної дисципліни

Нормативно-правові акти

1. Конституція України від 28.06.1996 № 254к/96-ВР (в редакції від 30.09.2016) URL: http://zakon4.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

2. Закон України «Про основні засади забезпечення кібербезпеки України» ?Електрон. ресурс[. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2163-19

3. Рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України".]Електрон. ресурс[. – Режим доступу: http://zakon.rada.gov.ua/laws/show/96/2016

4. Конвенція про кіберзлочинність,

chttp://zakon.rada.gov.ua/laws/show/994_575

5. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»]Електрон. ресурс[. – Режим доступу: http://zakon.rada.gov.ua/laws/show/537-16

6. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»]Електрон. ресурс[. – Режим доступу: http://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

7. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»,]Електрон. ресурс[. – Режим доступу: http://zakon.rada.gov.ua/laws/show/3475-15

8. Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації"]Електрон. ресурс[. – Режим доступу: http://zakon.rada.gov.ua/laws/show/32/2017

9. Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32]Електрон. ресурс[. – Режим доступу: http://zakon.rada.gov.ua/laws/show/n0006525-17

10. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах]Електрон. ресурс[. – Режим доступу: http://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF

11. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави]Електрон. ресурс[. – Режим доступу: https://www.kmu.gov.ua/ua/npas/249267402

Література:

1. Стратегічні комунікації: [словник] / Т. В. Попова, В. А. Ліпкан ; за заг. ред. доктора юридичних наук В. А. Ліпкана. — К. : ФОП Ліпкан О.С., 2016. — 416 с.

2. Тихомиров О.О. Кіберзлочин: теоретико-правові проблеми / О.О.Тихомиров //Зб. матеріалів наук.-практ. конф. “Інформаційна безпека: виклики і загрози сучасності”; 5 квітня 2013 р.—К. : Наук.-вид. центр НА СБ України.—2013.—С. 179-182

3. Пфо, О. М. Основні поняття і класифікація кіберзлочинності / О. М. Пфо // Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23-25 листоп. 2016 р. — Кропивницький : КНТУ, 2016. — С. 33-34.

4. Погорецький М. Кіберзлочини: до визначення поняття / М. Погорецький, В. Шеломенцев // Вісник прокуратури. — 2012. — № 8. — С. 89-96.

5. Міщук Н. Кіберзлочинність як загроза інформаційному суспільству /

Н. Мыщук // Вісник Львівського університету. Серія економічна. — 2014. — Випуск 51. — С. 173-179

6. Марків С. І. Кіберзлочинність. Нова кримінальна загроза / С. І. Марків // [Електронний ресурс]. — Режим доступу : http://gurt.org.ua/articles/34602/

7. Бельський Ю. Щодо визначення поняття кіберзлочину/ Ю. Бельський //Юридичний вісник. — 2014. — № 6. — С. 414-418

8. Кіберзлочинність: проблеми боротьби і прогнози [Електронний ресурс]. — Режим доступу : http://anticyber.com.ua/article_detail.php?id=140

9. Поняття та сутність кібернетичної злочинності [Електронний ресурс]. — Режим доступу : http://legalactivity.com.ua/index.php?option=com_content&view=article&id=1425%3A091216-07&catid=170%3A5-1216&Itemid=211&lang=en

10. Словник термінів з кібербезпеки / за заг. ред. О. Копана, Є. Скулиша. — К. : ВБ «Аванпост-Прим», 2012. — 214 с.

11. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування : Аналітична записка [Електронний ресурс]. — Режим доступу : http:// www.niss.gov.ua/articles/454

12. Стратегія забезпечення кібернетичної безпеки України (Проект) [Електронний ресурс]. — Режим доступу : www.niss.gov.ua/public/File/2013_nauk…/kiberstrateg.pdf

13. Голіна В.В., Головкін Б.М. Кримінологія: Загальна та Особлива частини Навчальний посібник. — Х.: Право, 2014. — 513 с.

14. Конвенція про кіберзлочинність від 23.11.2001 р. // Офіційний вісник України від 10.09.2007 — 2007 р., — № 65. — стор. 107. — стаття 2535.

15. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28.01.2003 р. // Офіційний вісник України. — 2010 р., № 56, / № 31, 2006, ст. 2202 /, — стор. 73, — стаття 1920.

16. Бутузов В. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : [монографія] / В. Бутузов. – К. : КИТ, 2010. – 148 с.

17. Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора // UNODC/CCPCJ/EG.4/2013/2.

18. Преступления в сфере информационных технологий [Электронный ресурс]. –Режим доступа:http://www.ru.wikipedia.org/wiki.

19. Невидин С.Хейг: ущерб от киберпреступлений превышает $1 трлн [Электронный ресурс]. – Режим доступа: http://www.newsland.ru/news/detail/id/807021.

20. Интерпол: киберпреступления являются самой опасной криминальной угрозой [Электронный ресурс]. –Режим доступа: http://www.virusovnet.org/main/309.

21. Конвенция о борьбе с киберпреступностью [Электронный ресурс].– Режим доступа: http://194.8.63.186/portals.

22. АзаровД.С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.08 / Д.С.Азаров. –К.: Ін-т держави і права НАН України, 2003. –18с.

23. Плугатир М.В. Імплементація Україною міжнародно-правових зобов'язань щодо відповідальності за злочини у сфері комп'ютерної інформації: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.08 / М.В.Плугатир. –К.: Держ. наук.-дослід. ін-т МВС України, 2010.– 16с.

Інтернет-ресурси

Сайт Офісу Генерального прокурора - URL: http://www.gp.gov.ua/
Сайт Верховної Ради України - URL: http://rada.gov.ua
Офіційний веб-портал судової влади - http://court.gov.ua/ .
Сайт Національної поліції України - https://www.npu.gov.ua/