МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ ПРАВА, ЕКОНОМІКИ ТА КІБЕРБЕЗПЕКИ

Кафедра кримінального права, процесу та криміналістики

« ЗАТВЕРДЖУЮ »

Ректор, проф.

_____ К.В. Громовенко

«_1_» _березня_ 2021 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«КОМП'ЮТЕРНА КРИМІНАЛІСТИКА»

Галузь **26- Цивільна безпека**

(шифр і назва напряму підготовки)

Спеціальності **262- Правоохоронна діяльність**

(шифр і назва спеціальності)

Назви освітньо-наукових програм: **Правоохоронна діяльність**

Факультет права, економіки та кібербезпеки

(назва інституту, факультету)

Рівень вищої освіти: **перший (бакалаврський)**

ОДЕСА - 2021 рік

Робоча програма навчальної дисципліни **«Комп'ютерна криміналістика»** для здобувачів наукового ступеня бакалавра за спеціальністю 262 – Правоохоронна діяльність. 25 с.

Розробник:

Подобний О. О., доктор юридичних наук, професор, завідувач кафедри кримінального права, процесу та криміналістики Міжнародного гуманітарного університету.

/ Подобний О. О. /
(прізвище та ініціали)

Робоча програма затверджена на засіданні кафедри кримінального права, процесу та криміналістики

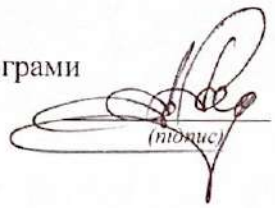
Протокол № 1 від «20» серпня 2021 року

Завідувач кафедри
д.ю.н., професор

/ Подобний О. О./
(прізвище та ініціали)

«20» серпня 2021 р.

Гарант освітньо-професійної програми
д.ю.н., професор.



/ Подобний О. О./
(прізвище та ініціали)

«30» серпня 2021 р.

Схвалено Вченою радою Міжнародного гуманітарного університету
Протокол № 1 від «31» серпня 2021 року

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, напрям підготовки, освітньо-науковий рівень</th><th colspan="2">Характеристика навчальної дисципліни</th></tr>
<tr><th>денна форма навчання</th><th>заочна форма навчання</th></tr>
<tr><td>Кількість кредитів – 9</td><td>Галузь знань
26 - Цивільна безпека
(шифр і назва)</td><td colspan="2">Вибіркова</td></tr>
<tr><td>Модулів – 3</td><td rowspan="4">Спеціальність
262- Правоохоронна діяльність</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 3</td><td>3-й</td><td>3-й</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 270</td><td colspan="2">Семестр</td></tr>
<tr><td>6-й</td><td>6-й</td></tr>
<tr><td rowspan="10">Тижневих годин
- для денної форми навчання:
аудиторних – 1
самостійної роботи –4,3;
- для заочної форми навчання:
аудиторних – 0.3
самостійної роботи –7</td><td rowspan="10">Освітньо-кваліфікаційний рівень:
перший
(бакалаврський)</td><td colspan="2">Лекції</td></tr>
<tr><td>16 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>14 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>60 год.</td><td>82 год.</td></tr>
<tr><td colspan="2">Індивідуальні завдання:</td></tr>
<tr><td colspan="2">Вид контролю: залік</td></tr>
</table>

В навчальній дисципліні «Комп'ютерна криміналістика» розглядається як юридична наука, що забезпечує швидке, повне і об'єктивне кримінальне провадження засобами, пов'язаними із використанням високих інформаційних технологій. У сучасних умовах саме комп'ютерна криміналістика знаходиться на передовій боротьбі зі злочинністю, активно та творчо розвиваючись на тлі науково-технічного прогресу сучасного світу, створюючи, перероблюючи та втілюючи всі досягнення науки в практику розслідування злочинів. Компютерна криміналістика вивчає закономірності діяльності з вчинення кіберзлочинів, механізму їх слідоутворення та досвід слідчої практики з метою розробки ефективних методів, засобів і прийомів у розслідуванні кримінальних правопорушень, що вчинюються із використанням високих інформаційних технологій.

Суб'єктами, які використовують рекомендації комп'ютерної криміналістики, є слідчі, судді, прокурори, працівники оперативних підрозділів, захисники (адвокати), нотаріуси, експерти, охоронні служби та інші службові особи.

Досягнення завдань кримінального судочинства з охорони прав та законних інтересів фізичних та юридичних осіб, які беруть у ньому участь, а також зі швидкого і повного розкриття злочинів та викриття винних осіб

можливе лише за умови кваліфікованого застосування сучасних криміналістичних знань.

Комп'ютерна криміналістика включає в себе теоретичні і методичні положення, криміналістичну техніку, криміналістичну тактику і методику розслідування кіберзлочинів. Криміналістика, взагалі, та комп'ютерна криміналістика, зокрема, має як теоретичне, так і практичне значення для розробки науково обґрунтованої програми боротьби зі злочинністю, а також іншими протиправними проявами у життєдіяльності суспільства і держави. Для досягнення цієї мети криміналістика широко залучає досягнення юридичних, природознавчих, технічних, економічних та інших наук, використовує результати аналізу та узагальнення слідчої і судової практики.

2. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

У процесі реалізації програми дисципліни «Комп'ютерна криміналістика» формуються наступні компетентності із передбачених освітньо-науковою програмою:

Інтегральна компетентність

Здатність вирішувати складні спеціалізовані задачі та практичні проблеми у сфері правоохоронної діяльності або у процесі навчання, що передбачає застосування певних теорій та методів правоохоронної діяльності і характеризується комплексністю та невизначеністю умов.

Загальні компетентності

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК4. Здатність використовувати інформаційні та комунікаційні технології.

ЗК5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК7. Здатність до адаптації та дії в новій ситуації.

ЗК8. Здатність приймати обґрунтовані рішення.

Спеціальні (фахові) компетентності

СК3. Здатність професійно оперувати категоріально-понятійним апаратом права і правоохоронної діяльності.

СК4. Здатність до критичного та системного аналізу правових явищ і застосування набутих знань та навичок у професійній діяльності.

СК5. Здатність самостійно збирати та критично опрацьовувати, аналізувати та узагальнювати правову інформацію з різних джерел.

СК6. Здатність аналізувати та систематизувати одержані результати, формулювати аргументовані висновки та рекомендації.

СК10. Здатність визначати належні та придатні для юридичного аналізу факти.

СК14. Здатність до використання технічних приладів та спеціальних засобів, інформаційно-пошукових систем та баз даних.

СК15. Здатність до застосування спеціальної техніки, спеціальних, оперативних та оперативно-технічних засобів, здійснення оперативно-розшукової діяльності.

СК18. Здатність забезпечувати кібербезпеку, економічну та інформаційну безпеку держави, об'єктів критичної інфраструктури.

СК19. Здатність забезпечувати охорону державної таємниці та працювати з носіями інформації з обмеженим доступом.

Навчальна дисципліна «Комп'ютерна криміналістика» забезпечує досягнення програмних результатів навчання (РН), передбачених освітньою програмою:

РН3. Збирати необхідну інформацію з різних джерел, аналізувати і оцінювати її.

РН4. Формулювати і перевіряти гіпотези, аргументувати висновки.

РН8. Здійснювати пошук інформації у доступних джерелах для повного та всебічного встановлення необхідних обставин.

РН9. Користуватись державною системою урядового зв'язку, Національною системою конфіденційного зв'язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку.

РН10. Виокремлювати юридично значущі факти і формувати обґрунтовані правові висновки.

РН12. Адаптуватися і ефективно діяти за звичних умов правоохоронної діяльності та за умов ускладнення оперативної обстановки.

РН14. Здійснювати пошук та аналіз новітньої інформації у сфері правоохоронної діяльності, мати навички саморозвитку та самоосвіти протягом життя, підвищення професійної майстерності, вивчення та використання передового досвіду у сфері правоохоронної діяльності.

РН17. Використовувати основні методи та засоби забезпечення правопорядку в державі, дотримуватись прав і свобод людини і громадянина, попередження та припинення нелегальної (незаконної) міграції та інших загроз національної безпеки держави (кібербезпеку, економічну та інформаційну безпеку, тощо).

РН18. Застосовувати штатне озброєння підрозділу (вогнепальну зброю, спеціальні засоби, засоби фізичної сили); інформаційні системи, інформаційні технології, технології захисту даних, методи обробки, накопичення та оцінювання інформації, інформаційно-аналітичної роботи, бази даних (в тому числі міжвідомчі та міжнародні), оперативні та оперативно-технічні засоби, здійснення оперативно-розшукової діяльності.

РН21. Організовувати заходи щодо режиму секретності та захисту інформації.

Очікувані результати навчання (компетентності освітньої складової)

Мета навчальної дисципліни «Комп'ютерна криміналістика»: засвоєння студентами теоретичних положень щодо закономірностей виникнення, збирання, дослідження, оцінювання і використання криміналістичної інформації та отримання ними знань, навичок, вмінь для успішного використання у практичній діяльності з розслідування, розкриття і попередження злочинів.

Завданням навчальної дисципліни «Комп'ютерна криміналістика» є систематизоване засвоєння її наукознавчих основ та методології, положень криміналістичної техніки, криміналістичної тактики, криміналістичної методики та набуття вміння застосовувати отримані знання під час розслідування окремих видів кіберзлочинів.

Вимоги до знань та вмінь студентів

Знати:

- історію криміналістики та комп'ютерної криміналістики; предмет комп'ютерної криміналістики, її систему, категорії; завдання, принципи, методи; особливості застосування теорій криміналістичної ідентифікації та групофікації в розслідуванні крмп'ютерних злочинів; теорію криміналістичної діагностики;
- загальні положення компютеро-криміналістичної техніки; електронне слідознавство; інформаційно-довідкове забезпечення розслідування та його автоматизацію;
- загальні положення компютеро-криміналістичної тактики; організацію і планування розслідування; тактику проведення у розслідуванні комп'ютерних злочинів таких процесуальних дій як огляд, обшук, слідчий експеримент, використання спеціальних знань, негласних слідчих (розшукових) дій;
- загальні положення криміналістичної методики під час розслідування комп'ютерних злочинів.

Вміти:

- вільно орієнтуватися в криміналістичних знаннях з метою використання їх у розслідуванні кіберзлочинів;

– оцінювати первинну інформацію про кіберзлочин та визначати слідчу ситуацію, обирати програми розслідування, розробляти відповідні плани; проводити розслідування злочину, керуючись висунутими версіями і планами;

– визначати необхідність застосування в конкретній слідчій ситуації та використовувати належні техніко-криміналістичні засоби, прийоми і методи, призначені для виявлення, фіксації, вилучення, забезпечення схоронності доказів у електронній формі в інтересах розкриття і розслідування кіберзлочинів;

– визначати необхідність і можливість призначення в конкретній слідчій ситуації криміналістичної експертизи, формулювати питання, які належить вирішити експертові, готувати матеріали, що надсилаються на експертизу з урахуванням вимог, які ставляться до них та їх оформлення;

- розробляти з використанням криміналістичних рекомендацій план підготовки і проведення слідчої дії, тактичної операції, використання спеціальних знань, проводити відповідну слідчу дію, призначати судову експертизу, організовувати взаємодію слідчого з працівниками оперативних підрозділів й іншими суб'єктами під час розслідування кіберзлочинів з використанням рекомендованих криміналістикою тактичних прийомів.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ТЕМА 1
ЗАГАЛЬНІ ПОЛОЖЕННЯ КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ

1. Особливості кіберпростору як об'єкта криміналістичного дослідження
2. Правові основи боротьби зі злочинами, що вчиняються в кіберпросторі
3. Криміналістична класифікація кіберзлочинів

ТЕМА 2
ТЕХНІЧНІ ЗАСАДИ КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ

1. Спеціальні технічні засоби: апаратні; експертні програми; набори хешей; архівування; криміналістичні інформаційні системи; програмні засоби розслідування комп'ютерних злочинів; апаратно-програмні засоби шифрування мобільного зв'язку; захищені модульні системи зберігання даних.

2. Технічні канали витоку інформації та способи її несанкціонованого зняття.

3. Методи та засоби блокування технічних каналів витоку інформації (захист інформації від витоку акустичним, віброакустичним, оптоелектронним каналами та від закладних пристроїв).

ТЕМА 3
ТАКТИЧНІ ЗАСАДИ КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ

1. Специфіка тактики проведення слідчих (розшукових) дій у розслідуванні кіберзлочинів: огляд комп'ютера; вилучення лог-файлів та їх доказове значення; тактика обшуку; пошук інформації на диску.

2. Тактичні прийоми негласних слідчих (розшукових) дій у розслідуванні кіберзлочинів: перехоплення та дослідження трафіку; дослідження статистики трафіку; інші дані про трафік (аналіз назв пакетів, поштова скринька, достовірність, посвідчення); кефлогери; інтернет-моніторинг (пошук).

3. Методи компютерно-технічної експертизи (дослідження файлових систем, копіювання носіїв, хеж-функції для встановлення тотожності, дослідження файлів; зашифровані данні).

ТЕМА 4
КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИНІВ

1. Структура криміналістичної характеристики кіберзлочинів
2. Характеристика типових предметів посягання та їх зв'язок з мотивами вчинення кіберзлочинів
3. Характеристика та взаємозв'язок типової особи злочинця й типових слідів кіберзлочинів
4. Характеристика типових способів/технологій вчинення кіберзлочинів

ТЕМА 5
ВІДКРИТТЯ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ ТА ВЗАЄМОДІЯ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

1. Виявлення кіберзлочинів як напрямок правоохоронної діяльності. Джерела інформації про кіберзлочин.
2. Організаційні форми початку кримінального провадження щодо кіберзлочинів та джерела обставин, що можуть свідчити про вчинення певного виду кіберзлочинів.
3. Особливості перевірки інформації про кіберзлочини, що вчинені або готуються.
4. Особливості відкриття кримінального провадження за заявою та повідомленням особи про кіберзлочин.

ТЕМА 6
ОРГАНІЗАЦІЯ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У КІБЕРПРОСТОРІ

1. Періодизація розслідування кіберзлочинів
2. Типові слідчі ситуації у розслідуванні кіберзлочинів, тактичні завдання та засоби їх розв'язання
3. Тактичні операції розслідування кіберзлочинів

ТЕМА 7
ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ У РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

1. Спеціальні знання та специфіка залучення спеціаліста під час розслідування кіберзлочинів.
2. Залучення експерта для проведення судової комп'ютерно-технічної експертизи під час розслідування кіберзлочинів.
3. Залучення експерта для проведення інших судових експертиз підчас розслідування кіберзлочинів: експертиза у сфері інтелектуальної власності;

експертиза телекомунікаційних систем (обладнання) та засобів; комплексні експертизи (КТЕ та експертизи відео звукозапису; КТЕ і ТЕД).

ТЕМА 8
ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ ОКРЕМИХ ВИДІВ КІБЕРЗЛОЧИНІВ

1. Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі.
2. Розслідування кіберзлочини, вчинені з антидержавно-політичних мотивів, пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі.
3. Розслідування злочинів, вчинених з соціально-економічних мотивів, що пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі.
4. Розслідування кіберзлочинів, вчинених з ідейних мотивів, пов'язаних зі світоглядною сферою життя суб'єктів відносин у кіберпросторі.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі				сам. роб.	усього	у тому числі				сам. роб.
		лекц.	прак	лаб	інд			лекц	прак	лаб	інд	
1	2	3	4	5	6	7	8	9	10	11	12	13
Тема 1. Загальні положення комп'ютерної криміналістики	10	2				8	11					11
Тема 2 Технічні засади комп'ютерної криміналістики	10	2	2			6	12	2	2			8
Тема 3. Тактичні засади комп'ютерної криміналістики	10	2	2			6	12	2	2			8
Тема 4. Криміналістична характеристика кіберзлочинів	12	2	2			8	11					11
Тема 5. Відкриття кримінального провадження та взаємодія під час розслідування кіберзлочинів	12	2	2			8	11					11
Тема 6. Організація розслідування злочинів у кіберпросторі	12	2	2			8	11					11
Тема 7. Використання спеціальних знань у розслідуванні кіберзлочинів	12	2	2			8	11					11
Тема 8. Особливості розслідування окремих видів кіберзлочинів	12	2	2			8	11					11
Усього годин	**90**	**16**	**14**			**60**	**90**	**4**	**4**			**82**

5. ТЕМИ СЕМІНАРСЬКИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин
1	ТЕМА 1. ЗАГАЛЬНІ ПОЛОЖЕННЯ КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ 1. Особливості кіберпростору як об'єкта криміналістичного дослідження 2. Правові основи боротьби зі злочинами, що вчиняються в кіберпросторі 3. Криміналістична класифікація кіберзлочинів	/
2	ТЕМА 2 ТЕХНІЧНІ ЗАСАДИ КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ 1. Спеціальні технічні засоби: апаратні; експертні програми; набори хешей; архівування; криміналістичні інформаційні системи; програмні засоби розслідування комп'ютерних злочинів; апаратно-програмні засоби шифрування мобільного зв'язку; захищені модульні системи зберігання даних. 2. Технічні канали витоку інформації та способи її несанкціонованого зняття. 3. Методи та засоби блокування технічних каналів витоку інформації (захист інформації від витоку акустичним, віброакустичним, оптоелектронним каналами та від закладних пристроїв).	2 / 2
3	ТЕМА 3. ТАКТИЧНІ ЗАСАДИ КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ 1. Специфіка тактики проведення слідчих (розшукових) дій у розслідуванні кіберзлочинів: огляд комп'ютера; вилучення лог-файлів та їх доказове значення; тактика обшуку; пошук інформації на диску.	2 / 2

	2. Тактичні прийоми негласних слідчих (розшукових) дій у розслідуванні кіберзлочинів: перехоплення та дослідження трафіку; дослідження статистики трафіку; інші дані про трафік (аналіз назв пакетів, поштова скринька, достовірність, посвідчення); кефлогери; інтернет-моніторинг (пошук). 3. Методи компютерно-технічної експертизи (дослідження файлових систем, копіювання носіїв, хеж-функції для встановлення тотожності, дослідження файлів; зашифровані данні).	
4	ТЕМА 4. КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИНІВ 1. Структура криміналістичної характеристики кіберзлочинів. 2. Характеристика типових предметів посягання та їх зв'язок з мотивами вчинення кіберзлочинів. 3. Характеристика та взаємозв'язок типової особи злочинця й типових слідів кіберзлочинів. 4. Характеристика типових способів/технологій вчинення кіберзлочинів.	2 / -
5	ТЕМА 5. ВІДКРИТТЯ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ ТА ВЗАЄМОДІЯ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ 1. Виявлення кіберзлочинів як напрямок правоохоронної діяльності. Джерела інформації про кіберзлочин. 2. Організаційні форми початку кримінального провадження щодо кіберзлочинів та джерела обставин, що можуть свідчити про вчинення певного виду кіберзлочинів 3. Особливості перевірки інформації про кіберзлочини, що вчинені або готуються 4. Особливості відкриття кримінального провадження за заявою та повідомленням особи про кіберзлочин.	2 / -
6	ТЕМА 6. ОРГАНІЗАЦІЯ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У КІБЕРПРОСТОРІ 1. Періодизація розслідування кіберзлочинів 2. Типові слідчі ситуації у розслідуванні кіберзлочинів, тактичні завдання та засоби їх розв'язання 3. Тактичні операції розслідування кіберзлочинів	2 / -
7	ТЕМА 7. ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ У РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ 1. Спеціальні знання та специфіка залучення спеціаліста під час розслідування кіберзлочинів. 2. Залучення експерта для проведення судової комп'ютерно-технічної експертизи під час розслідування кіберзлочинів. 3. Залучення експерта для проведення інших судових експертиз підчас розслідування кіберзлочинів: експертиза у сфері інтелектуальної власності; експертиза телекомунікаційних систем (обладнання) та засобів; комплексні експертизи (КТЕ та експертизи відео звукозапису; КТЕ і ТЕД).	2 / -
8	ТЕМА 8. ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ ОКРЕМИХ ВИДІВ КІБЕРЗЛОЧИНІВ 1. Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі. 2. Розслідування кіберзлочини, вчинені з антидержавно-політичних мотивів, пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі. 3. Розслідування злочинів, вчинених з соціально-економічних мотивів, що пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі. 4. Розслідування кіберзлочинів, вчинених з ідейних мотивів, пов'язаних зі світоглядною сферою життя суб'єктів відносин у кіберпросторі.	2 / -

6. САМОСТІЙНА РОБОТА

Самостійна робота з дисципліни складається з опрацювання навчального матеріалу:

- опрацювання лекційного матеріалу;
- самостійне опрацювання окремих питань навчальної дисципліни;
- підготовка до семінарських занять;
- підготовка до підсумкового контролю.

Конспект із виконаним завданням подається викладачу на перевірку під час проведення відповідного семінарського заняття, або в інший, визначений викладачем час. Загальний підсумок самостійної роботи з вивчення курсу фіксується під час складення заліку.

№ з/п	Назва теми	Кількість годин
1	ТЕМА 1. ЗАГАЛЬНІ ПОЛОЖЕННЯ КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ 1. Особливості кіберпростору як об'єкта криміналістичного дослідження. 2. Правові основи боротьби зі злочинами, що вчиняються в кіберпросторі. 3. Криміналістична класифікація кіберзлочинів.	8 / 11
2	ТЕМА 2 ТЕХНІЧНІ ЗАСАДИ КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ 1. Спеціальні технічні засоби: апаратні; експертні програми; набори хешей; архівування; криміналістичні інформаційні системи; програмні засоби розслідування комп'ютерних злочинів; апаратно-програмні засоби шифрування мобільного зв'язку; захищені модульні системи зберігання даних. 2. Технічні канали витоку інформації та способи її несанкціонованого зняття. 3. Методи та засоби блокування технічних каналів витоку інформації (захист інформації від витоку акустичним, віброакустичним, оптоелектронним каналами та від закладних пристроїв).	6 / 8
3	ТЕМА 3. ТАКТИЧНІ ЗАСАДИ КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ 1. Специфіка тактики проведення слідчих (розшукових) дій у розслідуванні кіберзлочинів: огляд комп`ютера; вилучення лог-файлів та їх доказове значення; тактика обшуку; пошук інформації на диску. 2. Тактичні прийоми негласних слідчих (розшукових) дій у розслідуванні кіберзлочинів: перехоплення та дослідження трафіку; дослідження статистики трафіку; інші дані про трафік (аналіз назв пакетів, поштова скринька, достовірність, посвідчення); кефлогери; інтернет-моніторинг (пошук). 3. Методи компютерно-технічної експертизи (дослідження файлових систем, копіювання носіїв, хеж-функції для встановлення тотожності, дослідження файлів; зашифровані данні).	6 / 8
4	ТЕМА 4. КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИНІВ 1. Структура криміналістичної характеристики кіберзлочинів. 2. Характеристика типових предметів посягання та їх зв`язок з мотивами вчинення кіберзлочинів. 3. Характеристика та взаємозв'язок типової особи злочинця й типових слідів кіберзлочинів. 4. Характеристика типових способів/технологій вчинення кіберзлочинів.	8 / 11
5	ТЕМА 5. ВІДКРИТТЯ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ ТА ВЗАЄМОДІЯ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ 1. Виявлення кіберзлочинів як напрямок правоохоронної діяльності. Джерела інформації про кіберзлочин. 2. Організаційні форми початку кримінального провадження щодо кіберзлочинів	8 / 11

	та джерела обставин, що можуть свідчити про вчинення певного виду кіберзлочинів 3. Особливості перевірки інформації про кіберзлочини, що вчинені або готуються 4. Особливості відкриття кримінального провадження за заявою та повідомленням особи про кіберзлочин.	
6	ТЕМА 6. ОРГАНІЗАЦІЯ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У КІБЕРПРОСТОРІ 1. Періодизація розслідування кіберзлочинів. 2. Типові слідчі ситуації у розслідуванні кіберзлочинів, тактичні завдання та засоби їх розв'язання. 3. Тактичні операції розслідування кіберзлочинів.	8 / 11
7	ТЕМА 7. ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ У РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ 1. Спеціальні знання та специфіка залучення спеціаліста під час розслідування кіберзлочинів. 2. Залучення експерта для проведення судової комп'ютерно-технічної експертизи під час розслідування кіберзлочинів. 3. Залучення експерта для проведення інших судових експертиз підчас розслідування кіберзлочинів: експертиза у сфері інтелектуальної власності, експертиза телекомунікаційних систем (обладнання) та засобів; комплексні експертизи (КТЕ та експертизи відео звукозапису; КТЕ і ТЕД).	8 / 11
8	ТЕМА 8. ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ ОКРЕМИХ ВИДІВ КІБЕРЗЛОЧИНІВ 1. Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі. 2. Розслідування кіберзлочини, вчинені з антидержавно-політичних мотивів, пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі. 3. Розслідування злочинів, вчинених з соціально-економічних мотивів, що пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі. 4. Розслідування кіберзлочинів, вчинених з ідейних мотивів, пов'язаних зі світоглядною сферою життя суб'єктів відносин у кіберпросторі.	8 / 11

7. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Індивідуальне завдання з навчальної дисципліни є формою самостійної обов'язкової роботи здобувача і виконується у вигляді реферативної роботи.

Реферат повинен мати титульний лист, вступ, основні розділи (2–4), висновки, список використаних джерел. Цитати, фактичні і статистичні матеріали, наведені в тексті, обов'язково мають супроводжуватися посиланнями на використані джерела.

При написанні реферату слід дотримуватися наступних вимог:

1. Обов'язковою умовою написання реферату є план, що складається не менше, ніж з 3-х пунктів, а також вступ та висновки, які повинні виражати власне ставлення студента до обраної теми.

2. Робота має мати обсяг не менш 10-ти друкованих сторінок тексту

3. Друкування тексту - за допомогою комп'ютера здійснюється через 1,5 міжрядкових інтервали, 14 кегль, шрифт Times New Roman. Поля: зліва - 30 мм; праворуч - 10-15 мм; вгорі і знизу - 20 мм.

Теми рефератів

1. Особливості кіберпростору як об'єкта криміналістичного дослідження.
2. Правові основи боротьби зі злочинами, що вчиняються в кіберпросторі.
3. Криміналістична класифікація кіберзлочинів.
4. Технічні канали витоку інформації та способи її несанкціонованого зняття.
5. Специфіка тактики проведення слідчих (розшукових) дій у розслідуванні кіберзлочинів.
6. Тактичні прийоми негласних слідчих (розшукових) дій у розслідуванні кіберзлочинів.
7. Методи компютерно-технічної експертизи.
8. Структура криміналістичної характеристики кіберзлочинів.
9. Характеристика типових предметів посягання та їх зв'язок з мотивами вчинення кіберзлочинів.
10. Характеристика та взаємозв'язок типової особи злочинця й типових слідів кіберзлочинів.
11. Характеристика типових способів/технологій вчинення кіберзлочинів.
12. Виявлення кіберзлочинів як напрямок правоохоронної діяльності.
13. Джерела інформації про кіберзлочин.
14. Організаційні форми початку кримінального провадження щодо кіберзлочинів.
15. Джерела обставин, що можуть свідчити про вчинення певного виду кіберзлочинів.
16. Особливості перевірки інформації про кіберзлочини, що вчинені або готуються.
17. Особливості відкриття кримінального провадження за заявою та повідомленням особи про кіберзлочин.
18. Типові слідчі ситуації у розслідуванні кіберзлочинів, тактичні завдання та засоби їх розв'язання.
19. Тактичні операції розслідування кіберзлочинів.
20. Специфіка залучення спеціаліста під час розслідування кіберзлочинів.
21. Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі.
22. Розслідування кіберзлочини, вчинені з антидержавно-політичних мотивів, пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі.
23. Розслідування злочинів, вчинених з соціально-економічних мотивів, що пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі.
24. Розслідування кіберзлочинів, вчинених з ідейних мотивів, пов'язаних зі світоглядною сферою життя суб'єктів відносин у кіберпросторі.

8. МЕТОДИ КОНТРОЛЮ

Система оцінювання та вимоги

Контроль знань і умінь здобувачів (поточний і підсумковий) з дисципліни «Комп'ютерна криміналістика» здійснюється відповідно до «Положення про організацію освітнього процесу у Міжнародному гуманітарному університеті» та «Положення про порядок оцінювання результатів навчальної діяльності здобувачів передвищої та вищої освіти». Рейтинг здобувача із засвоєння дисципліни визначається за 100 бальною шкалою.

Види контролю: поточний, підсумковий.

Методи контролю: спостереження за навчальною діяльністю здобувачів, усне опитування, письмовий контроль.

Форма контролю: залік.

Критерії оцінювання. Еквівалент оцінки в балах для кожної окремої теми може бути різний, загальну суму балів за тему визначено в навчально-методичній карті. Розподіл балів між видами занять (лекції, практичні заняття, самостійна робота) можливий шляхом спільного прийняття рішення викладача і студентів на першому занятті. Рівень знань оцінюється:

«зараховано» A - від 90 до 100 балів. Здобувач виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та семінарських заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

«зараховано» B - здобувач володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, розрахунків, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та семінарських заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

«зараховано», C - від 74 до 81 балів. Здобувач відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, реферату та активність у науково-дослідній роботі;

«зараховано», D - від 64 до 73 балів. Здобувач був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, рефератів (есе);

«зараховано» E - від 60 до 63 балів. Здобувач був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному

рівні, на всі запитання дає необгрунтовані, невичерпні відповіді, допускає помилки, має неповний конспект з завданнями до самостійної роботи.

«не зараховано» FX – від 35 до 59 балів. Здобувач володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.

«не зараховано» F – від 0 до 34 балів. Здобувач не володіє навчальним матеріалом.

Підсумкова (загальна оцінка) курсу навчальної дисципліни є сумою рейтингових оцінок (балів), одержаних за окремі оцінювані форми навчальної діяльності: поточне та підсумкове тестування рівня засвоєння теоретичного матеріалу під час аудиторних занять та самостійної роботи (модульний контроль); оцінка (бали) за виконання практичних індивідуальних завдань. Підсумкова оцінка виставляється після повного вивчення навчальної дисципліни, яка виводиться як сума проміжних оцінок за усіма видами робіт, зазначені у таблиці нижче.

Виконання навчальних завдань і робота за дисципліною має відповідати вимогам «Положення про академічну доброчесність у Міжнародному гуманітарному університеті» (затверджене ректором наказом № 112 від 01.11.2018 року).

Навчальна дисципліна «Комп'ютерна криміналістика» викладається за кредитно-модульною системою організації навчального процесу (КМСОНП). Дана система запроваджується з метою удосконалення системи контролю якості знань студентів, сприяння формуванню системних та систематичних знань, ритмічної самостійної роботи впродовж семестру, підвищення об'єктивності оцінювання знань та адаптації до вимог, визначених Європейською системою залікових кредитів (ECTS).

Оцінювання знань здобувачів повинно сприяти реалізації низки завдань, зокрема:

- підвищення мотивації здобувачів до системного навчання впродовж семестру та навчального року, переорієнтація їх цілей з отримання позитивної оцінки на формування системних, стійких знань, умінь та навичок;
- відкритість контролю, яка базується на ознайомленні здобувачів на початку вивчення дисципліни переліком, формами та змістом контрольних завдань, критеріями та порядком їх оцінювання;
- розширення можливостей для всебічного розкриття здібностей здобувачів, розвитку їх творчого мислення, та підвищення ефективності навчального процесу.

У випадку відсутності здобувача на лекції або семінарському занятті він ***зобов'язаний*** відпрацювати пропущене заняття через усне опитування в поза аудиторний час (час консультацій викладача) або відпрацювати пропущене заняття протягом одного тижня з моменту його появи. Невідпрацьовані заняття вважаються незданими і за них не нараховується оцінка в балах. За 10 днів до початку сесії викладач припиняє приймати відпрацювання.

9. КРИТЕРІЇ ОЦІНЮВАННЯ ПОТОЧНОЇ, САМОСТІЙНОЇ ТА ІНДИВІДУАЛЬНОЇ РОБОТИ ЗДОБУВАЧІВ

Денна форма навчання			
Види роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальна кількість балів**
І. Обов'язкові			
Систематичність і активність роботи на семінарських (практичних) заняттях			
1.1. Підготовка до семінарських (практичних) занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час семінарських (практичних) занять	**40**
Виконання модульних завдань			
1.2. Підготовка до модульного контролю знань	-//-	Перевірка правильності виконання модульних завдань	**35**
Виконання завдань для самостійного опрацювання			
1.3. Підготовка програмного матеріалу (тем, питань), що виноситься на самостійне вивчення	-//-	Розгляд відповідного матеріалу під час аудиторних занять або ІКР1, перевірка конспектів навчальних текстів тощо	**10**
Разом балів за обов'язкові види РС			**85**

ІІ. Вибіркові			
Виконання індивідуальних завдань			
2.1. Підготовка реферату (есе) за заданою тематикою	Відповідно до графіку ІКР	Обговорення (захист) матеріалів реферату (есе) під час ІКР	**5**
2.2. Аналітичний (критичний) огляд наукових публікацій, судової практики тощо	-//-	Перевірка та обговорення результатів проведеної роботи під час ІКР	**5**
2.3. Інші види індивідуальних завдань	-//-	Обговорення результатів проведеної роботи під час аудиторних занять або ІКР	**5**

1 Індивідуально-консультативна робота викладача зі студентами

Разом балів за вибіркові види РС			**15**
Всього балів за РС			**100**
Заочна форма навчання			
Види самостійної роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальна кількість балів**
І. Обов'язкові			
За виконання модульних (контрольних) завдань			
1.1. Підготовка до модульного контролю знань	Відповідно до розкладу	Перевірка правильності виконання модульних завдань	**70**
Разом балів за обов'язкові види СРС			**70**
ІІ. Вибіркові			
Виконання індивідуальних завдань (за бажанням студента)			
2.1. Підготовка реферату (есе) за заданою тематикою	Відповідно до графіку ІКР	Обговорення (захист) матеріалів реферату (есе) під час ІКР	**10**
2.2. Аналітичний (критичний) огляд наукових публікацій, судової практики тощо	-//-	Перевірка та обговорення результатів проведеної роботи під час ІКР	**10**
2.3. Інші види індивідуальних завдань	-//-	Обговорення результатів проведеної роботи під час ІКР	**10**
Разом балів за вибіркові види СРС			**30**
Всього балів за РС			**100**

Підсумковий контроль знань по даній дисципліні проводиться у формі *заліку (усні питання та письмове завдання)*. Питання, що включаються програми заліку є вузловими, узагальненими, комплексними, потребують творчого підходу при побудові відповіді та уміння синтезувати отриманні знання. Питання до заліку формуються в межах змісту програми дисципліни. Програмні питання доводяться до студентів на початку навчального семестру. Підсумкове оцінювання знань студентів здійснюється з урахуванням результатів оцінювання поточної роботи в семестрі та результатів заліку за 100-бальною системою.

10. ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ

1. Особливості кіберпростору як об'єкта криміналістичного дослідження.
2. Правові основи боротьби зі злочинами, що вчиняються в кіберпросторі.
3. Криміналістична класифікація кіберзлочинів.
4. Спеціальні технічні засоби: апаратні; експертні програми; набори хешей; архівування; криміналістичні інформаційні системи; програмні засоби розслідування комп'ютерних злочинів; апаратно-програмні засоби шифрування мобільного зв'язку; захищені модульні системи зберігання даних.
5. Технічні канали витоку інформації та способи її несанкціонованого зняття.
6. Методи та засоби блокування технічних каналів витоку інформації (захист інформації від витоку акустичним, віброакустичним, оптоелектронним каналами та від закладних пристроїв).
7. Специфіка тактики проведення слідчих (розшукових) дій у розслідуванні кіберзлочинів: огляд комп'ютера; вилучення лог-файлів та їх доказове значення; тактика обшуку; пошук інформації на диску.
8. Тактичні прийоми негласних слідчих (розшукових) дій у розслідуванні кіберзлочинів: перехоплення та дослідження трафіку; дослідження статистики трафіку; інші дані про трафік (аналіз назв пакетів, поштова скринька, достовірність, посвідчення); кефлогери; інтернет-моніторинг (пошук).
9. Методи компютерно-технічної експертизи (дослідження файлових систем, копіювання носіїв, хеж-функції для встановлення тотожності, дослідження файлів; зашифровані данні).
10. Структура криміналістичної характеристики кіберзлочинів.
11. Характеристика типових предметів посягання та їх зв'язок з мотивами вчинення кіберзлочинів.
12. Характеристика та взаємозв'язок типової особи злочинця й типових слідів кіберзлочинів.
13. Характеристика типових способів/технологій вчинення кіберзлочинів.
14. Виявлення кіберзлочинів як напрямок правоохоронної діяльності. Джерела інформації про кіберзлочин.
15. Організаційні форми початку кримінального провадження щодо кіберзлочинів та джерела обставин, що можуть свідчити про вчинення певного виду кіберзлочинів
16. Особливості перевірки інформації про кіберзлочини, що вчинені або готуються
17. Особливості відкриття кримінального провадження за заявою та повідомленням особи про кіберзлочин.
18. Періодизація розслідування кіберзлочинів.
19. Типові слідчі ситуації у розслідуванні кіберзлочинів, тактичні завдання та засоби їх розв'язання.
20. Тактичні операції розслідування кіберзлочинів.
21. Спеціальні знання та специфіка залучення спеціаліста під час розслідування кіберзлочинів.

22. Залучення експерта для проведення судової комп'ютерно-технічної експертизи під час розслідування кіберзлочинів.

23. Залучення експерта для проведення інших судових експертиз підчас розслідування кіберзлочинів: експертиза у сфері інтелектуальної власності; експертиза телекомунікаційних систем (обладнання) та засобів; комплексні експертизи (КТЕ та експертизи відео звукозапису; КТЕ і ТЕД).

24. Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі.

25. Розслідування кіберзлочини, вчинені з антидержавно-політичних мотивів, пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі.

26. Розслідування злочинів, вчинених з соціально-економічних мотивів, що пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі.

27. Розслідування кіберзлочинів, вчинених з ідейних мотивів, пов'язаних зі світоглядною сферою життя суб'єктів відносин у кіберпросторі.

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова

1. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР / Верховна Рада України. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.

2. Кримінальний кодекс України : Закон України від 05. 04. 2001 р. № 2341-III / Верховна Рада України. URL: http://zakon1.rada.gov.ua (дата звернення: 27.04.2021).

3. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 2213-VIII / Верховна Рада України. URL: http://zakon1.rada.gov.ua (дата звернення: 27.04.2021)

4. Про інформацію : Закон України від 02. 10. 1992 р. № 2657-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua (дата звернення: 27.04.2021).

5. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI в редакції Закону України від 09.04.2015 № 319-VIII / Верховна Рада України. URL: http://zakon1.rada.gov.ua

6. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16 листопада 1992 року № 2782-XII / Верховна Рада України. URL: http://zakon1.rada.gov.ua

7. Про Національну поліцію : закон України від 02. 07. 2015 р. № 580-VIII / Верховна Рада України. URL: http://zakon1.rada.gov.ua (дата звернення: 27.04.2021).

8. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення: 27.04.2021).

9. Про державну таємницю : Закон України від 21. 01. 1994 р. № 3855-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua (дата звернення: 27.04.2021).

10. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 року № 3475-IV. *Відомості Верховної Ради України.* 2006. № 30. Ст. 258.

11. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 року № 80/94-ВР / Верховна Рада України. URL: http://zakon1.rada.gov.ua (дата звернення: 20.06.2018).

12. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI в редакції Закону України від 19.10.2017№ 2168-VIII / Верховна Рада України. URL: http://zakon1.rada.gov.ua

13. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19

14. Про Положення про технічний захист інформації в Україні: Указ Президента України від 27 вересня 1999 р. № 1229/99. URL: https://zakon.rada.gov.ua/laws/show/1229/99

15. Про затвердження Зводу відомостей, що становлять державну таємницю: Наказ Служби безпеки України від 12.08.2005 № 440. URL: https://zakon.rada.gov.ua/laws/show/z0902-05

16. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні: Наказ Генеральної прокуратура України, Міністерства внутрішніх справ України, Служби безпеки України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16.11.2012 № 114/1042/516/1199/936/1687/5. URL: http://zakon4.rada.gov.ua/laws/show/v0114900-12.

17. Про затвердження Концепції технічного захисту інформації в Україні: Постанова Кабінету Міністрів України від 8 жовтня 1997 р. № 1126. URL: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF

18. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію: Постанова Кабінету Міністрів України від 19 жовтня 2016 р. № 736. URL: https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF

19. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія. Одеса :ТЕС, 2020. 372 с.

20. Самойленко О. А. Виявлення та розслідування кіберзлочинів : навчально-методичний посібник. Одеса, 2020. 112 с.

21. Якименко І.З. Конспект лекцій з дисципліни «Цифрова криміналістика». URL: http://dspace.wunu.edu.ua/bitstream/316497/36005/1/%.pdf

22. Криміналістика/ Під ред. В.В. Тіщенко. Одеса: Видавничий дім «Гельветика», 2017. 556 с.

23. Криміналістика: підруч. , В.Ю. Шепітько, В.О. Коновалова, В.А. Журавель [та ін.]: за ред. В.Ю. Шепітька. 5-те вид. передобл. та допов. Київ: Ін Юре, 2016. 640 с.

24. Федоров Р.Ф. Форензика – компьютерная криминалистика. Москва: «Юридический Мир», 2007. 432 с.

25. Логінова Н.І., Дробожур Р.Р. Правовий захист інформації: навчальний посібник. Одеса: Фенікс, 2015. 264 с.

26. Бем М.В., Городиський І.М., Саттон Г., Родіоненко О.М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. Київ: К.І.С., 2015. 220 с.

27. Доступ до публічної інформації: практичний посібник для державних службовців. Київ: Національне агентство України з питань державної служби, 2012. 22 с.

28. Куліш А.М., Кобзєва Т.А., Шапіро В.С. Інформаційне право України: навчальний посібник. Суми: Сумський державний університет, 2016. 108 с.

29. Кукарін О.Б. Електронний документообіг та захист інформації: навч. посібник. Київ: НАДУ, 2015. 84 с.

Допоміжна

30. Бандурка О. М. Теорія і практика оперативно-розшукової діяльності : монографія. Харків : Злота миля, 2012. 620 с.

31. Бирюков В.В. Цифровая фотография: перспективы использования в криминалистике: моногр. Луганск: РИО ЛИВД, 2000. 138 с.

32. Бірюков В.В. Теоретичні основи інформаційно-довідкового забезпечення розслідування злочинів: моногр. Луганськ: РВВ ЛДУВС, 2009. 664 с.

33. Подобний О.О. Глава 24. Загальні засади й тактика негласних слідчих (розшукових) дій. *Криміналістика: підручник* / За ред. В. В. Тіщенка. Херсон: Видавничий дім «Гельветика», 2017. С. 325-346.

34. Подобний О. О. Актуальні аспекти вдосконалення оперативно-розшукового і кримінально-процесуального законодавства. *Сучасні проблеми правового, економічного і соціального розвитку держави*: матеріали міжнародної науково-практичної конференції (Харків, 10 квітня 2012 р.). Харків: ХНУВС, 2012. С. 271-274.

35. Подобний О. О., Пасечник М. Л. Слідча таємниця як засада кримінального провадження. *Актуальні проблеми кримінальної юстиції*: матеріали Всеукраїнської науково-практичної конференції (м. Одеса, 26-27 червня 2019 р.).

36. Пасечник М. Л. Категорія «інформація» як основа визначення поняття «слідча таємниця». *Юридичний бюлетень*. 2018. № 7. С. 303-309.

37. Системна інформатизація правоохоронної діяльності / за ред. В. Дурдинця, М. Швеця. Київ: НДЦПІ АПрН України, 2007. 382 с.

38. Тіщенко В.В., Барцицька А.А. Теоретичні засади формування технологічного підходу в криміналістиці : монографія. НУ "ОЮА". Одеса : Фенікс, 2012. 199 с.

39. Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ : монографія. Одеса : Юридична література, 2011. 216 с.