Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра **Права** (№ 702)

ЗАТВЕРДЖУЮ

Гарант освітньої програми
_____ Голубов А.Є.
(підпис) (ініціали та прізвище)
« 31 » серпня 2021 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КВАЛІФІКАЦІЯ ТА ОРГАНІЗАЦІЯ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У СФЕРІ ВИКОРИСТАННЯ КОМП'ЮТЕРІВ, АВТОМАТИЗОВАНИХ СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ
(назва навчальної дисципліни)

Галузь знань: 08 Право
(шифр і найменування галузі знань)

Спеціальність: 081 Право
(код і найменування спеціальності)

Освітня програма: Право
(найменування освітньої програми)

Рівень вищої освіти:
перший (бакалаврський)

Силабус введено в дію з 01.09.2021 року

Харків – 2021 р.

Розробники: **Шинкаренко Ігор Ростиславович, кандидат юридичних наук, професор, професор кафедри права гуманітарно-правового факультету**
(прізвище та ініціали, посада, науковий ступінь і вчене звання)

(підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри Права
(назва кафедри)

Протокол № 1 від « 31» серпня 2021 р.

Завідувач кафедри д.ю.н, доцент **Спіцина Г.О.**
(Науковий ступінь і вчене звання) (підпис) (ініціали та прізвище)

Погоджено з представником здобувачів освіти:

_____ _____ _____
(підпис) (ініціали та прізвище)

1. Загальна інформація про викладача

ПІБ: Шинкаренко Ігор Ростиславович
Посада: професор
Наукова ступінь: кандидат юридичних наук
Вчене звання: професор
Перелік дисциплін, які викладає:
– «Судові і правоохоронні органи України» - бакалавр;
– «Кримінальне право. Загальна частина»- бакалавр;
– «Кримінальне право. Особлива частина» - бакалавр;
– «Кваліфікація та організація розслідування кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку»- бакалавр;
– «Актуальні питання протидії кримінальним та іншим правопорушення на об'єктах критичної інфраструктури та повітряного транспорту» - магістр;
– «Використання кримінального аналізу у протидії кримінальним правопорушенням на об'єктах критичної інфраструктури: космічної діяльності та повітряного транспорту» - магістр.

Напрями наукових досліджень:

- кримінально правові проблеми протидії окремим видам кримінальних правопорушень та удосконалення правового регулювання діяльності правоохоронних органів;
- безпека критичної інфраструктури;
- права людини та їх забезпечення під час здійснення слідчих (розшукових) дій та оперативно-розшукових заходів;
- історичні закономірності формування теорії ОРД як окремої галузі наукового знання та формування новітньої парадигми теорії та практики ОРД у сфері забезпечення загальної та спеціальної превенції, виявлення та розслідування кримінальних правопорушень на об'єктах інфраструктури авіаційного транспорту та аерокосмічної галузі;;
- теоретичні проблеми формування метатеорії та приватних правових теорій;
- теоретичні, кримінально-правові та організаційно-тактичні проблеми забезпечення державної політики протидії злочинності на об'єктах аерокосмічної галузі як складової критичної інфраструктури України.

Профайл викладача: Тел.: (097) -970-81-66
E-mail:i.shynkarenko@khai.edu
https://orcid.org/0000-0001-5524-2259;
https://education.khai.edu/lecturer/schinkarenko-igor-rostislavovich
Актуальні оголошення на сторінці дисципліни в системіMentor
Робоче місце: 205 к-2.

3.

4. Опис навчальної дисципліни

Семестр, в якому викладається дисципліна – другий

Обсяг дисципліни: 3 кредита ЄКТС / 90 годин, у тому числі аудиторних – **32** год. (*лекції - 16 год., семінарські / практичні - 16 год.)*, самостійної роботи здобувачів – 58 год.

Форма здобуття освіти – *денна*

Дисципліна *обов'язкова*

Види навчальної діяльності – *лекції, семінарські / практичні заняття*

Види контролю – *модульний контроль, диф. залік*

Мова викладання – *українська*

Пререквізити: "Теорія держави та права", "Адміністративне право", «Кримінальне право», «Кримінальний процес», «Кримінологія», «Криміналістика» та ін..

Кореквізити навчальної дисципліни: «Правове регулювання інформаційної безпеки в України», «Міжнародне приватне право», «Міжнародний захист прав людини»,, «ІТ-право».

3. Мета та завдання навчальної дисципліни

- **Мета**: формування у студентів теоретичних і практичних знань, кримінально-правової кваліфікації та формування організаційно-тактичної моделі з розслідування кримінальних правопорушень пов'язаних із втручанням у роботу комп'ютерних мереж і мереж електрозв'язку, а також використанням комп'ютерів, а також поглиблене вивчення актуальних проблем сучасної криміналістики, що виникають у зв'язку з широким використанням при скоєнні кримінальних правопорушень у сфері сучасних інформаційних технологій, комп'ютерної техніки та засобів телекомунікації.

Завдання: Формування у студентів:

1) системи знань щодо**:**

- принципів, якими слід керуватися у ході кримінально-правової кваліфікації кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку;
- розмежування протиправних діянь у ході кримінально-правової кваліфікації кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку;
- алгоритму аналізу проблемних питань кваліфікації, що виникають під час кримінально-правової характеристики кримінальних правопорушень;
- правил застосування закону про кримінальну відповідальність; формування системи знань про закономірності механізму вчинення кримінальних правопорушень у сфері комп'ютерних злочинів; вивчення особливостей механізму створення слідів при здійсненні кримінальних правопорушень у сфері сучасних інформаційних технологій, комп'ютерної техніки та засобів телекомунікації.
- і специфіки формування доказової бази;
- криміналістичної методики розслідування комп'ютерних кримінальних правопорушень;

2) системи вмінь:

- застосування техніко-криміналістичних та тактичних засобів, криміналістичної методики у практичній діяльності з розслідування окремих видів кримінальних правопорушень пов'язаних з використанням комп'ютерної техніки та інформаційних технологій.

Перелік компетентностей

Інтегральна компетентність. Здатність розв‘язувати складні спеціалізовані задачі та практичні проблеми у галузі професійної правничої діяльності або у процесі навчання, що передбачає застосування правових доктрин, принципів і правових інститутів і характеризується комплексністю та невизначеністю умов.

Загальні компетентності (ЗК).

– ЗК2. Здатність застосовувати знання у практичних ситуаціях.

– ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.

– ЗК7. Здатність вчитися і оволодівати сучасними знаннями.

Фахові (спеціальні) компетентності (ФК).

- ФК 7. Здатність застосовувати знання завдань, принципів і доктрин національного права, а також змісту правових інститутів, щонайменше з таких галузей права як: конституційне право, адміністративне право і адміністративне процесуальне право, цивільне і цивільне процесуальне право, кримінальне і кримінальне процесуальне право.

– ФК 8. Знання і розуміння особливостей реалізації та застосування норм матеріального і процесуального права.

– ФК 11. Здатність визначати належні та прийнятні для юридичного аналізу факти.

– ФК12. Здатність аналізувати правові проблеми, формувати та обґрунтовувати правові позиції.

– ФК13. Здатність до критичного та системного аналізу правових явищ і застосування набутих знань у професійній діяльності.

– ФК14. Здатність до консультування з правових питань, зокрема, можливих способів захисту прав та інтересів клієнтів, відповідно до вимог професійної етики, належного дотримання норм щодо нерозголошення персональних даних та конфіденційної інформації.

– ФК 15. Здатність до самостійної підготовки проектів актів правозастосування.

– ФК16. Здатність до логічного, критичного і системного аналізу документів, розуміння їх правового характеру і значення.

Програмні результати навчання:

– ПРН 1. Визначати переконливість аргументів у процесі оцінкизаздалегідь невідомих умов та обставин.

– ПРН 2. Здійснювати аналіз суспільних процесів у контекстіаналізованої проблеми і демонструвати власне бачення шляхів її розв‘язання.

– ПРН 3. Проводити збір і інтегрований аналіз матеріалів з різних джерел.

– ПРН 4. Формулювати власні обґрунтовані судження на основі аналізувідомої проблеми.

– ПРН 5. Давати короткий висновок щодо окремих фактичних обставин(даних) з достатньою обґрунтованістю.

– ПРН 6. Оцінювати недоліки і переваги аргументів, аналізуючи відомупроблему.

– ПРН 7. Складати та узгоджувати план власного дослідження ісамостійно збирати матеріали за визначеними джерелами.

– ПРН 8. Використовувати різноманітні інформаційні джерела дляповного

– та всебічного встановлення певних обставин.

– ПРН 9. Самостійно визначати ті обставини, у з‘ясуванні яких потрібнадопомога, і діяти відповідно до отриманих рекомендацій.

– ПРН 10. Вільно спілкуватися державною та іноземною мовами як усно,так і письмово, правильно вживаючи правничу термінологію.

– ПРН 11. Володіти базовими навичками риторики.

– ПРН 12. Доносити до респондента матеріал з певної проблематики доступно і зрозуміло.

– ПРН 13. Пояснювати характер певних подій та процесів з розумінняпрофесійного та суспільного контексту.

– ПРН14. Належно використовувати статистичну інформацію, отриманиз першоджерел та вторинних джерел для своєї професійної діяльності.

– ПРН 15. Вільно використовувати для професійної діяльності доступніінформаційні технології і бази даних.

– ПРН 16. Демонструвати вміння користуватися комп‘ютернимипрограмами, необхідними у професійній діяльності.

– ПРН 17. Працювати в групі, формуючи власний внесок у виконаннязавдань групи.

– ПРН 18. Виявляти знання і розуміння основних сучасних правових доктрин, цінностей та принципів функціонування національної правової системи.

– ПРН 19. Демонструвати необхідні знання та розуміння сутності та змісту основних правових інститутів і норм фундаментальних галузей права.

– ПРН 20. Пояснювати природу та зміст основних правових явищ і процесів.

– ПРН 21. Застосовувати набуті знання у різних правових ситуаціях, виокремлювати юридично значущі факти і формувати обґрунтовані правові висновки.

– ПРН 22. Готувати проекти необхідних актів застосування права відповідно до правового висновку зробленого у різних правових ситуаціях.

– ПРН 23. Надавати консультації щодо можливих способів захисту правта інтересів клієнтів у різних правових ситуаціях.

4. Зміст навчальної дисципліни
МОДУЛЬ 1

ЗМІСТОВНИЙ МОДУЛЬ 1. ОСОБЛИВОСТІ КВАЛІФІКАЦІЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ПІДЧАС ЇХ ПОПЕРЕДЖЕННЯ ТА ВИЯВЛЕННЯ У СФЕРІ ВИКОРИСТАННЯ КОМП'ЮТЕРІВ, АВТОМАТИЗОВАНИХ СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Тема 1. Загальна характеристика кримінальних правопорушень, що вчиняються з використанням програмних і технічних засобів, інформаційно-телекомунікаційних систем.

Обсяг аудиторного навантаження -4 год.:

Лекція 2 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Семінарське заняття 2 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з підготовки до семінарського заняття та оцінка викладачем

Самостійна робота 7 год: Опрацювання навчально- методичних матеріалів. Он-лайн консультація. Робота в форумі. Завантажена у систему Mentor матеріалу з самостійної роботи.

Зміст теми: Поняття та види кібер-правопорушень відповідно до Конвенції про кіберзлочинність та міжнародних правових актів. Реалізація положень Конвенції в КК України. Кримінально-правове поняття кримінальних кібер-правопорушень, узгоджене із законодавством України. Види кримінальних кібер-правопорушень за КК України. Загальна кримінально-правова характеристика кримінальних кіберправопорушень, що посягають на конфіденційність, цілісність і доступність комп’ютерних даних і систем. Загальна кримінально-правова характеристика кримінальних правопорушень загально кримінальної спрямованості, що вчиняються з використанням програмних і технічних засобів інформаційно-телекомунікаційних систем. Загальна кримінально-правова характеристика та особливості кваліфікації кримінальних правопорушень, що вчиняються з використанням програмних і технічних засобів інформаційно-телекомунікаційних систем, пов’язаних зі змістом даних та порушенням авторського права та суміжних прав.

Анотація: на ґрунті вивчення теоретичних положень та чинного законодавства надаються знання щодо сутності кримінальних правопорушень в сфері у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку**;** формування наукового підгрунтя кваліфікації означених правопорушень, що посягають на конфіденційність, цілісність і доступність комп’ютерних даних і систем; формування наукових алгоритмів щодо організації та тактики попередження,

виявлення та розслідування означеного виду кримінальних правопорушень.

.

Самостійна робота

Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді за однією з рекомендованих тем.

2. Виконання практичних завдань протягом семестру.

3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

Формування компетентностей: ІК, ЗК - 2, ЗК- 3, ЗК-7, ФК -7,8, ФК-11-16.

Результати навчання: ПРН1 -ПРН23.

Тема 2. Кваліфікація кримінальних правопорушень у сфері використання електронно-обчислювальних машин(комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Обсяг аудиторного навантаження – 4 год:

Лекція2 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Практичне заняття 2 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з вирішення ситуаційних задач та їх оцінка викладачем.

Самостійна робота 7 год: Опрацювання навчально - методичних матеріалів. Он-лайн консультація. Робота в форумі. Завантажена у систему Mentor матеріалу з самостійної роботи.

Зміст теми: Вимоги та алгоритм кваліфікації несанкціонованого втручання в роботу електронно- обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Вимоги та алгоритм кваліфікації створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збуту. Вимоги та алгоритм кваліфікації несанкціонованого збуту або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації. Вимоги та алгоритм кваліфікації несанкціонованих дій з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї. Вимоги та алгоритм кваліфікації порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється. Вимоги та алгоритм кваліфікації перешкоджання роботі електронно- обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку. Розмежування кримінальних кіберправопорушень, що посягають на конфіденційність, цілісність і доступність комп'ютерних даних і систем від суміжних складів кримінальних правопорушень.

Анотація. : з урахуванням теоретичних положень юридичної науки та правової доктрини України формується система знань та уявлень щодо кримінально-правової характеристики кримінальних правопорушень**,** що посягають на конфіденційність, цілісність і доступність комп'ютерних даних і систем, а також формування наукових алгоритмів щодо кваліфікації окремих кримінальних правопорушень у цій сфері.

Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді за однією з рекомендованих тем.

2. Виконання практичних завдань протягом семестру.

3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

Формування компетентностей: ІК, ЗК - 2, ЗК- 3, ЗК-7, ФК -7,8, ФК-11-16.

Результати навчання: ПРН1 -ПРН23.

Тема 3. Кваліфікація кримінальних правопорушень загально кримінальної спрямованості а також пов'язаних з розповсюдженням забороненого контенту, що вчиняються з використанням програмних і технічних засобів, інформаційно-телекомунікаційних систем.

Обсяг аудиторного навантаження- 4 год:

Лекція 2 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Практичне заняття 2 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з вирішення ситуаційних задач та їх оцінка викладачем.

Самостійна робота 7 год: Опрацювання навчально- методичних матеріалів. Он-лайн консультація. Робота в форумі. Завантажена у систему Mentor матеріалу з самостійної роботи.

Зміст теми: Вимоги та особливості кваліфікації кримінальних правопорушень загально кримінальної спрямованості а також пов'язаних з розповсюдженням забороненого контенту.

Відмежування кримінальних правопорушень загально кримінальної спрямованості з використанням програмних і технічних засобів інформаційно-телекомунікаційних систем від правопорушень, що посягають на конфіденційність, цілісність і доступність комп'ютерних данихі систем.

Кваліфікація виготовлення, розповсюдження та збуту порнографічних матеріалів, що вчиняються з використанням програмних і технічних засобів інформаційно-телекомунікаційних систем. Особливості алгоритму кваліфікації виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію, які вчиняються з використанням програмних і технічних засобів інформаційно-телекомунікаційних систем. Кваліфікація порушення авторського права і суміжних прав, яке вчиняється з використанням програмних і технічних засобів інформаційно-телекомунікаційних систем.

Анотація: з урахуванням теоретичних положень юридичної науки та правової доктрини України формується система знань та уявлень щодо формування організаційно - правового алгоритму кваліфікації кримінальних

правопорушень загально кримінальної спрямованості, виготовлення, розповсюдження та збуту порнографічних матеріалів, що вчиняються з використанням програмних і технічних засобів інформаційно-телекомунікаційних систем; виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію, які вчиняються з використанням програмних і технічних засобів інформаційно-телекомунікаційних систем; порушення авторського права і суміжних прав, що вчиняються з використанням програмних і технічних засобів інформаційно-телекомунікаційних систем.

.Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді за однією з рекомендованих тем.

2. Виконання практичних завдань протягом семестру.

3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

Формування компетентностей: ІК, ЗК - 2, ЗК- 3, ЗК-7, ФК -7,8, ФК-11-16.

Результати навчання: ПРН1 -ПРН23.

Тема 4. Кримінологічна характеристика кіберзлочинності (кримінальної кіберпротиправності) та особливості її попередження.

Обсяг аудиторного навантаження – 4 год:

Лекція 2 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Семінарське заняття 2 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з підготовки до семінарського заняття та оцінка викладачем

Самостійна робота 7 год: Опрацювання навчально- методичних матеріалів. Он-лайн консультація. Робота в форумі. Завантажена у систему Mentor матеріалу з самостійної роботи.

Зміст теми: Поняття та кримінологічна характеристика кіберзлочинності. Загрози кібербезпеці України та підстави їх класифікації. Фактори латентності кібер - правопорушень. Чинники кримінальної кібер-протиправності. Види загроз в кібернетичному просторі. Напрями протидії кіберзлочинності. Особливості протидії кіберзлочинності на загально соціальному рівні. Спеціально-кримінологічне запобігання кримінальних кібер-правопорушень. Суб'єкти протидії кіберзлочинності (кримінальній кібер-протиправності). Особливості протидії кіберзлочинності в країнах світу. Міжнародний досвід протидії кримінальній протиправності.

Анотація: урахуванням теоретичних положень юридичної науки та правової доктрини України формується система знань та практичних навичок з особливостей організації протидії кримінальним правопорушення кримінальній протиправності у сфері використання програмних і технічних засобів інформаційно-телекомунікаційних систем.

Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді за однією з рекомендованих тем.

2. Виконання практичних завдань протягом семестру.

3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

Формування компетентностей: ІК, ЗК - 2, ЗК- 3, ЗК-7, ФК -7,8, ФК-11-16.

Результати навчання: ПРН1 -ПРН23.

ЗМІСТОВНИЙ МОДУЛЬ 2. ОРГАНІЗАЦІЯ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ.

Тема 5. Особливості розслідування кримінальних проваджень за фактами вчинення кримінальних правопорушень у сфері використання електронно-обчислювальних машин(комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Обсяг аудиторного навантаження- 4 год:

Лекція 2 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Семінарське заняття 2 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з підготовки до семінарського заняття та оцінка викладачем

Самостійна робота 7 год: Опрацювання навчально- методичних матеріалів. Он-лайн консультація. Робота в форумі. Завантажена у систему Mentor матеріалу з самостійної роботи.

Зміст теми: Особливості механізму вчинення кримінальних правопорушень у сфері використання програмних і технічних засобів інформаційно-телекомунікаційних систем, а також з використанням мережі Інтернет. Характеристика осіб та організованих злочинних груп, що вчинюють кримінальні кіберправопорушення. Характеристика типових слідів кіберправопорушень.

Особливості відкриття досудових проваджень про кримінальні кібер-правопорушення: типові версії та обставини, що підлягають з'ясуванню. Сутність та форми взаємодії слідчих, оперативних та експертних служб України при розслідуванні даних видів кримінальні кіберправопорушення. Форми та особливості взаємодії слідчого з правоохоронними органами інших країн при розслідуванні кримінальних кіберправопорушень. Види та особливості тактики слідчих (розшукових) дій, які проводяться при розслідуванні кримінальні кібер-правопорушення, вчинених з використанням мережі Інтернет.

Анотація: з урахуванням теоретичних положень юридичної науки та правової доктрини України формується система знань та уявлень про сучасні методологічні основи розслідування кіберправопорушень, основні ознаки криміналістичної характеристики, проблем типологізації слідчих ситуацій та алгоритмів здійснення С(Р)Д та НС(Р)Д під час розслідування означеної групи правопорушень.

Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді

за однією з рекомендованих тем.

2. Виконання практичних завдань протягом семестру.

3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

Формування компетентностей: ІК, ЗК - 2, ЗК- 3, ЗК-7, ФК -7,8, ФК-11-16.

Результати навчання: ПРН1 -ПРН23.

Тема 6. Загальні положення методики розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

.

Обсяг аудиторного навантаження- 4 год:

Лекція 2 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Семінарське заняття 2 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з підготовки до семінарського заняття та оцінка викладачем

Самостійна робота 7 год: Опрацювання навчально- методичних матеріалів. Он-лайн консультація. Робота в форумі. Завантажена у систему Mentor матеріалу з самостійної роботи.

Зміст теми: Теоретичні та тактичні засади методики розслідування кримінальних кіберправопорушень. Обстановка досудового розслідування та її об'єктивні й суб'єктивні фактори. Зміст криміналістичної тактики. Засоби криміналістичної тактики. Поняття тактичної операції. Типові тактичні операції початкового етапу розслідування кримінальних кібер-правопорушень.

Особливості тактики провадження окремих слідчих (розшукових) дій під час досудового розслідування кримінального провадження за фактами вчинення кримінальних кіберправопорушень. Підготовка до проведення слідчих дій, спрямованих на збирання інформації в електронній формі. Тактичні правила та рекомендації, спрямовані на пошук інформації в електронній формі підчас слідчого огляду, обшуку. Тактичні особливості фіксації інформації в електронній формі підчас слідчого огляду, обшуку або тимчасового доступу до речей та документів. Тактичні прийоми вилучення інформації в електронній формі підчас слідчого огляду, обшуку або тимчасового доступу до речей та документів. Особливості допиту свідка, потерпілого під час досудового розслідування кримінального провадження за фактами вчинення кримінальних кібер-правопорушень. Питання, що вирішуються під час проведення судових експертиз у межах кримінальних проваджень за фактами вчинення кримінальних кібер-правопорушень.

Анотація: з урахуванням теоретичних положень юридичної науки та правової доктрини України формується система знань та уявлень щодо формування організаційно тактичних алгоритмів дій у типових ситуаціях під час досудового розслідування кримінального провадження за фактами вчинення кримінальних кіберправопорушень.

Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді за однією з рекомендованих тем.

2. Виконання практичних завдань протягом семестру.

3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

Формування компетентностей: ІК, ЗК - 2, ЗК- 3, ЗК-7, ФК -7,8, ФК-11-16.

Результати навчання: ПРН1 -ПРН23.

Тема 7. Методика розслідування окремих видів кримінальних правопорушень, які вчиняються з використанням електронно-обчислювальних машин, комп'ютерних програм та мережі Інтернет.

Обсяг аудиторного навантаження - 4 год:

Лек*ція 2 год:* очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Практичне заняття 2 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з вирішення ситуаційних задач та їх оцінка викладачем.

Самостійна робота 7 год: Опрацювання навчально- методичних матеріалів. Он-лайн консультація. Робота в форумі. Завантажена у систему Mentor матеріалу з самостійної роботи.

Зміст теми: Криміналістична характеристика та методика розслідування кримінальних кіберправопорушень, вчинених з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі

Криміналістична характеристика та методика розслідування кібер кримінальних правопорушень, вчинених з анти державно - політичних мотивів, пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі

Тактика проведення окремих слідчих (розшукових) дій при фксації порушень прав інтелектуальної власності у мережі Інтернет.

Особливості проведення окремих слідчих (розшукових) дій у кримінальних провадженнях, пов'язаних із розповсюдженням у мережі інтернет забороненого контенту

- **Анотація**: з урахуванням теоретичних положень юридичної науки та правової доктрини України формується система знань та уявлень щодо формування організаційно тактичних алгоритмів дій у типових ситуаціях під час досудового розслідування кримінального провадження за фактами вчинення кримінальних кіберправопорушень з корисливих мотивів, що пов'язані з фінансово економічною сферою відносин у кіберпросторі; методики розслідування кримінальних кіберправопорушень вчинених з антидержавною-політичних мотивів, що пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі.

Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді за однією з рекомендованих тем.

2. Виконання практичних завдань протягом семестру.

3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

Формування компетентностей: ІК, ЗК - 2, ЗК- 3, ЗК-7, ФК -7,8, ФК-11-16.

Результати навчання: ПРН1 -ПРН23.

Тема 8. Методика використання негласних слідчих (розшукових) дій щодо вирішенні задач кримінального провадження розслідування кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку.

Обсяг аудиторного навантаження- 4 год:

Лекція 2 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Практичне заняття 2 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з вирішення ситуаційних задач та їх оцінка викладачем.

Самостійна робота 9 год: Опрацювання навчально- методичних матеріалів. Он-лайн консультація. Робота в форумі. Завантажена у систему Mentor матеріалу з самостійної роботи.

Зміст теми: Теоретичні, соціально-правові передумови використання негласних дій під час розслідування злочинів. Поняття, завдання, види негласних слідчих (розшукових) дій та їх місце у системи слідчих (розшукових) дій. Об'єкти відносно яких можливо проводити негласні слідчі (розшукові) дії. Суб'єкти, уповноважені на прийняття рішення ініціювати проведення негласних слідчих (розшукових) дій, санкціонувати їх проведення та використання конфіденційного співробітництва під час кримінального провадження. Суб'єкти, уповноважені безпосередньо здійснювати НС(Р)Д.

Види негласних слідчих (розшукових) дій та підстави їх класифікації: за ступеню втручання в права та свободи громадян; за об'єктами та суб'єктами провадження; засобами, що використовуються під час проведення конкретних негласних слідчих (розшукових) дій; завданнями, що вирішуються під час НС(Р)Д. Формальні, матеріальні та інформаційні підстави щодо проведення НС(Р)Д визначені чинним законодавством. Тактика проведення окремих слідчих (розшукових) дій при розслідуванні даних злочинів (огляд Інтернет-сторінок, обшук, призначення судовихекспертиз).

Особливості організації проведення та використання результатів НС(Р)Д (зняття інформації з транспортних телекомунікаційних мереж; зняттяінформації з електронних інформаційних систем; установлення місцезнаходження радіоелектронного засобу; моніторинг банківських рахунків; негласне отримання зразків, необхідних для порівняльного дослідження) для вирішення завдань розслідування кримінального провадження за фактами вчинення кримінальних правопорушень.

Анотація: з урахуванням теоретичних положень юридичної науки та правової доктрини України формується система знань та уявлень щодо організаційно тактичних алгоритмів проведення НС(Р)Д у типових ситуаціях під час досудового розслідування кримінального провадження за фактами вчинення кримінальних кіберправопорушень; методики використання результатів НС(Р)Д під час розслідування кримінального провадження за фактами вчинення кримінальних кіберправопорушень

Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді

за однією з рекомендованих тем.

2. Виконання практичних завдань протягом семестру.

3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

Формування компетентностей: ІК, ЗК - 2, ЗК- 3, ЗК-7, ФК -7,8, ФК-11-16.

Результати навчання: ПРН1 -ПРН23.

4. Індивідуальні завдання

Навчальним планом не передбачено.

Реферати, аналітичні огляди та інше – це індивідуальні завдання, які сприяють розширенню та поглибленню теоретичних знань з окремих тем навчальної дисципліни, формують навички самостійної роботи з навчальною та науковою літературою, кримінальним законодавством, судовою практикою.

6. Методи навчання

Проведення аудиторних лекцій, практичних занять, індивідуальні консультації (при необхідності), самостійна робота студентів за матеріалами, опублікованими кафедрою (методичні посібники), проведення олімпіад, словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (ілюстрування, демонстрування, самостійне спостереження)

7. Методи контролю

Поточний контроль: опитування на практичних заняттях; вирішення онкретних правових ситуацій; проведення письмових контрольних робіт з окремих правових інститутів; проведення програмованого контролю (тестування); проведення групових та індивідуальних консультацій.

Підсумковий контроль: складання модульного контролю; складання диф. заліку.

8. Критерії оцінювання та розподіл балів, які отримують здобувачі

1.1.

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	0…1	5	0…5
Виконання практичних робіт	3...5	4	12...20
Модульний контроль	10…15	1	10…15
Змістовний модуль 2			
Робота на лекціях	0…1	5	0…5
Виконання практичних робіт	3...5	4	12...20

Модульний контроль	10…15	1	10…15
Виконання і захист РГР (РР, РК)	16…20	1	16…20
Усього за семестр			**60…100**

Семестровий контроль (диф. залік) проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до диф. заліку.

Білет для диф. заліку складається з**:**

І. Теоретична частина (питання для перевірки отриманих знань): складається з 2 запитань кожне оцінюється максимально 20 балів.

Приклад

1. Поняття та кримінологічна характеристика кіберзлочинності - 20 балів
2. Криміналістична характеристика кримінальних кібер - правопорушень, вчинених з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі – 20 балів.
3. **ІІ. Практична частина** (завдання для виявлення рівня сформованості умінь та практичних навичок професійної діяльності). – максимальна оцінка 60 балів

Всього – максимальна оцінка 100 балів

Під час складання семестрового іспиту/заліку студент має можливість отримати максимум 100 балів.

Критерії оцінювання роботи здобувача протягом семестру

Відповідно до п. 3.2. Положення про рейтингове оцінювання досягнень студентів у Національному аерокосмічному університеті ім. М.Є. Жуковського «Харківський авіаційний інститут» студенту можуть призначатися бали за інші активності, пов'язані з навчальною дисципліною, які нараховуються та можуть бути враховані у загальній оцінці за семестр. Бали зокрема можуть призначатися за такі активності, пов'язані з навчальною дисципліною, як:

- участь у науковому комунікативному заході (конференції, семінарі, круглому столі тощо) із написанням тез наукової доповіді за предметом навчальної дисципліни (20 балів);
- участь у другому турі Всеукраїнської олімпіади відповідного напряму 20 балів);
- участь (прослуховування) не менше у 5 вебінарах, пов'язаних з навчальною дисципліною (3-15 балів);
- участь у тренінгу, пов'язаному з навчальною дисципліною (15 балів);
- проходження он-лайн курсу, пов'язаного з навчальною дисципліною (20 балів);
- участь та отриманні рейтингового місця у тематично пов'язаному із предметом навчальної дисципліни студентському конкурсі (30 балів);
- розробка та створення дидактичного матеріалу за тематикою предмету навчальної дисципліни (15 балів) (підтвердження - дидактичний матеріал);

- проведення право освітнього заходу із учнями шкіл та інших навчальних закладів за тематикою навчальної дисципліни (20 балів);
- написання реферату (5 балів);
- участь у не менше 2-х заходах, що проводяться студентськими професійними об`єднаннями за спеціальністю (5-15 балів);
- інші активності, пов'язані з навчальною дисципліною, за попереднім погодженням із науково-педагогічним працівником, який викладає навчальну дисципліну.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

9. Політика навчального курсу

1. Письмові роботи:

Планується виконання студентами обов'язкових та додаткових декількох видів письмових робіт: письмових робіт за результатами самостійної роботи за темами курсу, тестових завдань за модулями (перелік та зміст завдань за темами курсу міститься на сторінці **в**: https://mentor.khai. edu/course/view.php?id=4247), письмових експрес-опитувань на семінарських заняттях тощо.

2. Академічна доброчесність:

Очікується, що студенти будуть дотримуватися принципів академічної доброчесності, усвідомлюючи наслідки її порушення. Порушення академічної доброчесності регулюється відповідно до Положень «Про систему забезпечення якості освітньої діяльності та вищої освіти СУЯ ХАІ-НМВ-П/011:2017» та «Про академічну доброчесність»СУЯ ХАІ-НМВ-П/004:2019 від 21.06.2019(зі змінами від 22.01.2020) (https://khai.edu/ua/university/normativnabaza/polozheniya1/polozhennya-yaki-regulyuyut-poryadok-zdijsnennya osvitnogo-procesu/; https://khai.edu/assets/files/polozhennya/polozhennya-pro-akademichnu-dobrochesnist.pdf)).

3. Відування занять

Відвідання занять є важливою складовою навчання. Очікується, що всі студенти відвідають лекції і практичні заняття курсу.

Пропуски семінарських (практичних, лабораторних) занять відпрацьовуються в обов'язковому порядку. Студент зобов'язаний відпрацювати пропущене заняття впродовж двох тижнів з дня пропуску заняття. За пропущені лекційні заняття без поважних причин в обсязі, що перевищує 10% від загальної кількості лекційних годин, які відведені на навчальну дисципліну відповідно до робочого навчального плану, керівник курсу віднімає 5 балів від підсумкового

семестрового балу студента (https://khai.edu/ua/university/normativna-baza/polozheniya1/polozhennya-pro-organizaciyu-sistemi-upravlinnya-yakistyu/polozhennya-pro-sistemu-zabezpechennya-yakosti/).

10. Методичне забезпечення

1. Силабус «Кваліфікація та організація розслідування кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку» для здобувачів вищої освіти, спеціальності 081 – «Право», другий рівень овищої освіти: денна форма. / Укладачі: І.Р. Шинкаренко. .Харків: Нац. Аерокосм. університет, 2021. 34 с. URL: https://mentor.khai.edu/course/view.php?id=3783
2. Навчально-методичне забезпечення вибіркової навчальної дисципліни "Кваліфікація та організація розслідування кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку" для бакалав: денна форма навчання / Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т" ; уклад. І. Р. Шинкаренко. Харків. Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т", 2021. 393 с. URL: http://library.khai.edu/library/fulltexts/doc/KZ_Kvalifikaciya.pdf
3. Плани практичних (семінарських) занять навчальної дисципліни «Кваліфікація та організація розслідування кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку» для здобувачів вищої освіти, спеціальності 081 – «Право», другий рівень овищої освіти: денна форма. / Укладачі: Шинкаренко І.Р. Харків: Нац. Аерокосм. університет, 2021. URL: https://mentor.khai.edu/course/view.php?id=3783
4. Завдання для самостійної роботи з навчальної дисципліни «Кваліфікація та організація розслідування кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку» для здобувачів вищої освіти, спеціальності 081 – «Право», другий рівень овищої освіти: денна форма. / Укладачі: І.Р. Шинкаренко, Філіпенко Н.Є. Харків: Нац. Аерокосм. університет, 2021. 42 с. URL: https://mentor.khai.edu/course/view.php?id=3783
5. Електронний ресурс ХАІ 081-Право: https://education.khai.edu/program /081-1-40

11. Рекомендована література

Базова література

Нормативно-правові акти:

1. Конституція України від 28.06.1996 р. *Відомості Верховної Ради* України. 1996. № 30. Ст. 141(із змінами та доп.).. URL: https://zakon.rada.gov.ua/laws/show/
2. Кримінальний кодекс України від 05.04.2001 р. *Відомості Верховної Ради України*. 2001. № 25. Ст. 131. (із змінами та доп.). URL: https://zakon.rada.gov.ua/laws/show/2341-14.
3. Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI. *Голос України* від 19.05.2012 р. № 90–91. (із змінами та доп.).URL: https://zakon.rada.gov.ua/laws/show/4651-17.
4. Кодекс України про адміністративні правопорушення від 07.12.1984 р. *Відомості Верховної Ради УРСР*. 1984. № 51. С. 1122. (із змінами та доп.). URL: https://zakon.rada.gov.ua/laws/show/80731-10/
5. Закон України "Про Національну поліцію" *Відомості Верховної Ради* (ВВР), 2015, № 40-41, ст.379. (із змінами та доп.).URL: https://zakon.rada.gov.ua/laws/show/580-19/
6. Конвенція про кіберзлочинність від 23.11.2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575.
7. 7. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, від 28.01.2003 р. (Дата набрання чинності для України: 01.04.2007) URL: http://zakon1.rada.gov.ua/laws/show/994_687.
8. Закон України «Про ратифікацію Конвенції про кіберзлочинність» від 07.09.2005 р. *Голос України.* 04.10.2005. № 186. (із змінами та доп.). URL: https://zakon.rada.gov.ua/laws/show/2824-15.
9. Закон України «Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи» від 21.07.2006 р. № 23-V. *Відомості Верховної Ради України*. 2006. № 39. Ст. 328. URL: https://zakon.rada.gov.ua/laws/show/23-16.
10. Закон України «Про інформацію» від 02.10.1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650. (із змінами та доп.). URL: https://zakon.rada.gov.ua/laws/show/994_687.
11. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 р. № 2594-IV. *Відомості Верховної Ради*. 2005. № 26. Ст. 347. (із змінами та доп.).URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
12. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 р. *Голос України*. 27.06.2003. № 119. (із змінами та доп.). URL: https://zakon.rada.gov.ua/laws/show/851-15.

13. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. *Відомості Верховної Ради (ВВР).* 2017, № 45, ст.403. (із змінами та доп.).URL: https://zakon.rada.gov.ua/laws/show/2163-19./

14. Національна стратегія у сфері прав людини: Указ Президента України від 24 березня 2021 року№ 119/2021 «Про Національну стратегію у сфері прав людини» URL: https://zakon.rada.gov.ua/laws/show/119/2021#n13

15. Стратегія боротьби з організованою злочинністю: Розпорядження Кабінета Міністрів України **№** 1126-р від 16 вересня 2020 р. «Про схвалення Стратегії боротьби з організованою злочинністю». URL: https://zakon.rada.gov.ua /laws/show/1126-2020-%D1%80#Text.

16. Постанова Кабінету Міністрів України від 29.03.2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах». Урядовий кур'єр. 18.04.2006. № 73 /73-74/. (із змінами та доп.).URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF.

17. Постанова Кабінет Міністрів України від 11.04.2012 р. № 295 «Про затвердження Правил надання та отримання телекомунікаційних послуг». *Урядовий кур'єр*. 20.06.2012. № 109. (із змінами та доп.). URL: https://zakon.rada.gov.ua/laws/show/295-2012-%D0%BF.

18. Про Стратегію кібербезпеки України: Указ Президента України від 26 серпня 2021 р. № 447/2021. «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року. URL: https://www.president.gov.ua/documents/4472021-40013

19. Про організаційно-правові основи боротьби з організованою злочинністю: Закон України від 30.06.1993 р. № 3341-XII (із змінами та доп.).// БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/3341-12.

20. Про захист інформації в інформаційно-телекомунікаційних системах : закон України від 5 лип. 1994 р. // БД «Законодавство України» (із змінами та доп.). / ВР України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

21. Про авторське право та суміжні права : закон України від 23 груд. 1993 р. (із змінами та доп.).// БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/3792-12.

22. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні : Наказ Міністерства внутрішніх справ України від 07.07.2017 № 575, зареєстрований в Міністерстві юстиції України 31.07.2017 р. за № 937/30805. (із змінами та доп.).// БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/z0529-20#Text

23. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : Наказ Міністерства юстиції України від 08.10.1998 № 53/5, зареєстрований в

Міністерстві юстиції України 03.11.1998 р. за № 705/3145. (із змінами та доп.).// БД «Законодавство України» / ВР України. URL: http://zakon3.rada.gov.ua/laws/show/z0705-98.

24. 26. Convention on Cybercrime Budapest, 23.XI.2001. European Treaty Series - No. 185. URL: https://rm.coe.int/1680081561

Основна література:

1. Законодавство України про кримінальну відповідальність за "комп'ютерні" злочини: науково-практичний коментар і шляхи вдосконалення / А. А. Музика, Д. С. Азаров. К. : Паливода А. В. [вид.], 2005. 119 с.

2. Кримінальне право України. Особлива частина: підруч. для студентів юрид. ВНЗ / [Ю.В. Баулін та ін.] ; за ред. проф. В.Я. Тація, В.І. Борисова, В.І. Тютюгіна ; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2015. 677 с.

3. Кримінальне право України. Особлива частина: навчальний посібник. Конспект лекцій. / За загальною редакцією Топчія В.В. Ірпінь: Університет державної фіскальної служби України, 2021. 407 с.

4. Кваліфікація злочинів у діяльності Національної поліції України : навч. посіб. / за заг. ред. О. М. Литвинова ; МВС України, Харків, нац. ун-т внутр. справ. Харків : Константа, 2017. 448 с.

5. Кримінально-правова характеристика та розслідування незаконного збуту, розповсюдження комп'ютерної інформації з обмеженим доступом: Навчально-практичний посібник / Васильєв В.В., Пашнєв Д.В., Рудик М.В., Воронцов Д.В. Сімферополь : КрЮІ ОДУВС, 2010. 170 с.

6. Криміналістика: підручник: у 2 т. Т.1 / [А.Ф. Волобуєв, М.В. Даньшин, А.В. Іщенко та ін.] ; за заг. ред. А.Ф. Волобуєва, Р.Л. Степанюка, В.О. Малярової ; МВС України, Харків. нац. ун-т внутр. справ. Харків: ХНУВС, 2018. 384 с.

7. Криміналістика : підручник : у 2 т. Т.2 / [А.Ф. Волобуєв, М.В. Даньшин, А.В. Іщенко та ін.] ; за заг. ред. А.Ф. Волобуєва, Р.Л. Степанюка, В.О. Малярової ; МВС України, Харків. нац. ун-т внутр. справ. Харків: ХНУВС, 2018. 364с.

8. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / [О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін.]. Київ : Видавничий дім «Скіф», 2012. 728 с.

9. Процесуальний порядок та тактичні особливості здійснення слідчих (розшукових) дій: науково-методичні рекомендації / В.В. Кікнчук, К.Л. Бугайчук, В.О. Малярова,Т.П. Матюшкова. Харків: ХНУВС, 2018. 101с.

10. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка , 2012. 526 с.

11. Пашнєв Д. В. Особливості кваліфікації злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Вісник Кримінологічної асоціації України* : збірник наукових праць [редкол. Л. М. Давиденко, Т. А. Денисова, О. М. Джужа та ін.]. Харків: Золота миля, 2013. С. 34–42.

12. Шалгунова С.А. Кримінальне право (Особлива частина): Конспект

лекцій для денної форми навчання. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2020. 464 с.

Додаткова література:

1. Комп'ютерний тероризм: практика запобігання, протидії, розслідування : кримінолого-криміналістичний аналіз та правові, управлінські і тактико-технологічні засади запобігання, протидії, розслідування комп'ютерних терористичних актів: навч. посібник / П. Д. Біленчук [и др.] ; заг. ред. П. Д. Біленчук. Хмельницький : Хм. ЦНТЕІ, 2008. 258 с.

2. Навчально-методичне забезпечення вибіркової навчальної дисципліни "Кваліфікація та організація розслідування кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку" для бакалав: денна форма навчання / Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т" ; уклад. І. Р. Шинкаренко. Харків. Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т", 2020. 393 с. - http://library.khai. edu/library/fulltexts/doc/KZ_Kvalifikaciya.pdf

3. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій [Текст] : навч. посіб. / Бутузов В. М. [та ін. ; за ред.: Б. В. Романюка, Є. Д. Скулиша].Київ: Рада нац. безпеки і оборони України, Міжвід. наук.-дослід. центр з пробл. організованої злочинності, Служба безпеки України, Нац. акад. служби безпеки України, 2011. 404 с.

4. Особливості підготовки матеріалів для призначення судових експертиз: навч. наочн. посіб. для працівників правоохоронних органів / Укладачі: О.П. Угровецький, В.В. Аброськін, І.Р. Шинкаренко та ін. / Міністерство юстиції України; Харківський науково-дослідний інститут судових експертиз ім. Засл. проф. М.С. Бокаріуса. Харків: ХНДІСЕ, Промінь, 2019. 180 с.

5. Особливості розслідування кримінальних правопорушень, пов’язаних із розповсюдженням у мережі Інтернет забороненого контенту [Текст] : метод. рек. / [Стрільців О. М., Крижна В. В., Максименко О. В. та ін.] ; за заг. ред. Ю. Ю. Орлова. К. : Нац. акад. внутр. справ, 2014. 80 с.

6. Тактика слідчого огляду комп’ютерних систем та їх елементів: наук.-практ. посіб. Дніпро, 2010. 88 с.

7. Ричка Д.О. Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку: дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. Дніпро:Дніпровський національний університет імені Олеся Гончара, 2019. 308 с.

8. Самойленко О. А. Виявлення та розслідування кіберкримінальних правопорушень [Текст] : навчально-методичний посібник. Одеса: ТЕС, 2020. 112 с.

9. Самойленко О.А. Основи методики розслідування кримінальних правопорушень, вчиненихуу кіберпросторі: монографія / О. А. Самойленко ; за заг. ред. А. Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с.

10. Пашнєв Д. В. Необхідність кримінально-правової охорони критичної інформаційної інфраструктури. *Вісник Кримінологічної асоціації України № 6 : зб.*

наук. праць [редкол. Л. М. Давиденко, Т. А. Денисова, О. М. Джужа та ін.]. Х. : Золота миля, 2014.С. 73–82.

11. Плугатир М. В. Суб'єктивна сторона злочину, передбаченого ст. 361-1 Кримінального кодексу України. *Розкриття злочинів за новим кримінальним процесуальним кодексом України.* Київ, 2012. С. 95-96.

12. Шинкаренко І. Р., Шинкаренко І. І. Кримінальне право: склади окремих видів кримінальних правопорушень: навчально-наочний посібник: структурно-логічні схеми. Харків : Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут» ; «Факт», 2021. 312 с. ISBN 978-966-637-980-4

13. Шинкаренко І.Р. та ін. Злочини в сфері використання комп'ютерної техніки: кваліфікація, розслідування та протидія: монографія. Донецьк: ДЮІ ЛДУВС, 2007. 266 с.

14. Боротьба з тероризмом. (Рекомендовано МОН України) навчальний посібник/ Шинкаренко І.Р. розділ 4. / за заг. редакцією професора В.В. Коваленка / [Джужа О.М., Никифорчук Д.Й., Комарницький В.М. та ін.]. К.: МОН України, 2013. 584с.

15. Виявлення та розкриття кримінальних правопорушень у сфері незаконного обігу наркотичних засобів: навчальний посібник / За заг. ред. докт. юрид. наук, проф. М.А. Погорецького, канд. юрид. наук, проф. І.Р. Шинкаренка. Одеса: ОДУВС, 2011. 342с.

16. Шинкаренко И. Р., Кириченко О. В. , Дараган В. В. Правовые основы проведения оперативно-розыскных мероприятий и негласных следственных (розыскных) действий (структурно-логические схемы): учеб. пособие / под общ. ред. проф. И. Р. Шинкаренка. Днепропетровск : Днепроп. гос. ун-т внутр. дел ; Лира ЛТД, 2013. 200 с.

17. Шинкаренко І.Р., Авер'янов А.О., Поливанюк В.Д. , Дараган В.В Методика документування осіб, які займаються несанкціонованим зняттям грошових коштів з пластикових платіжних карток громадян шляхом використання їх персональних даних: методичні рекомендації. Дніпропетровськ: ДДУВС, 2013. 90 с.

18. Шинкаренко І.Р., Шинкаренко І.О., Кириченко О.В. Правове регулювання оперативно розшукової діяльності та здійснення негласних слідчих (розшукових) дій(структурно-логічні схеми): навч. посіб./ за ред. професора І.Р. Шинкаренка. Д.: ДДУВСЛіра ЛТД, 2015. 272 с. (Рекомендовано МОН від 29.01.14 №1/11-1212).

19. Шинкаренко І.Р., Шинкаренко І.О., Кириченко О.В. Правові та організаційні основи здійснення оперативно-розшукових заходів та негласних слідчих (розшукових) дій (структурно-логічні схеми) підрозділами кримінальної поліції: навчальний посібник / за ред. професора І.Р. Шинкаренка. Д. : ДДУВС, 2017. 224 с.

20. Правові та організаційні основи використання спеціальної техніки у протидії злочинності: навч. посібник / за заг. ред. проф. І.Р. Шинкаренка. Дніпропетровськ: Дніпроп. держ. ун-т внутр. справ, 2017. 260 с.

21. Шинкаренко І.Р., Чаплинський К.О. Загальні основи здійснення тактичних комбінацій під час оперативно-розшукових заходів та негласних слідчих (розшукових) дій: навч. посіб. / за заг ред. проф І.Р. Шинкаренка. Д.: ДДУВС, 2016. 158 с.

22. Шинкаренко І.Р. Організаційно-тактичні особливості проведення негласних слідчих (розшукових) дій: навчальний посібник. Дніпропетровськ: ДДУВС, 2017. 264 с.

23. Шинкаренко І. Р., Шинкаренко І. І. Кримінальне законодавство як підгрунтя формування ефективної системи протидії діяльності злочинних спільнот. Протидія організованій злочинності: проблеми теорії та практики: Матеріали регіонального науково-практичниого семінару (3 грудня 2021, м. Дніпро). Дніпро: ДДУВС, 2021.С. 112-117.

24. Шинкаренко І. Р., Шинкаренко І. І. Окремі аспекти міжнародного досвіду запобігання та протидії корупції. Протидія корупції: правове регулювання і практичний досвід: матеріали доповідей на міжнарод. наук.-практ. конф. (м. Харків, 03 грудня 2021р.) Харків: Харківський національний університет внутрішніх справ, 2021. С. 55-57

25. Шинкаренко І. Р., Шинкаренко І. І. Забезпечення прав і свобод людини під час оперативно-розшукового та кримінального провадження щодо діяльності злочинних спільнот. *Права людини в Україні: минуле, сьогодення, майбутнє : тези доп. учасників II – га Всеукр. наук.-практ. конф. (Харків, 10 груд. 2021 р.)*, 187-193.

26. Шинкаренко І. Р., Байрамова Р. Р. Охорона права на життя ненародженої дитини. Модернізація вітчизняної правової системи в умовах світової інтеграції: матеріали Міжнар. наук.-практ. конф., м. Кропивницький, 19-20 травня 2021 р. / за заг. ред. Б. Р. Стецюка. Кропивницький : ЛА НАУ, 2021. С. 171 – 173. URL: http://www.klanau.kr.ua/images/docs/sbornik/materiali_2_mnp_konferencii.pdf

27. Шинкаренко І. Р., Клетьонкіна Ю. В. Особливості звільнення від кримінальної відповідальності неповнолітніх Модернізація вітчизняної правової системи в умовах світової інтеграції: матеріали Міжнар. наук.-практ. конф., м. Кропивницький, 19-20 травня 2021 р. / за заг. ред. Б. Р. Стецюка. Кропивницький : ЛА НАУ, 2021. С. 173 -176 URL: http://www.klanau.kr.ua/images/docs/sbornik/materiali_2_mnp_konferencii.pdf

28. Шинкаренко І. Р., Нурієв М. Н., Мамедов Т. Н., Ісраіллі К. Ф. Проблемні аспекти використання інституту умовного осуду в кримінальному праві Азербайджанської республіки . Модернізація вітчизняної правової системи в умовах світової інтеграції: матеріали Міжнар. наук.-практ. конф., м. Кропивницький, 19-20 травня 2021 р. / за заг. ред. Б. Р. Стецюка. Кропивницький : ЛА НАУ, 2021. С. 176 – 179/ URL: http://www.klanau.kr.ua/images/docs/sbornik/materiali_2_mnp_konferencii.pdf

29. Ali Alkaabi, George Mohay, Adrian McCullagh, Nicholas Chantler (*2010)* Dealing with the Problem of Cybercrime/ *International Conference on Digital Forensics and Cyber CrimeICDF2C, 2010: Digital Forensics and Cyber Crime*. pp 1-18|

30. Ajayi, E. F. G. Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems.* Vol. 6(1), pp. 1-12, August 2016 URL: https://academicjournals.org/journal/JIIS/article-full-text-pdf/ 930ADF960210. DOI 10.5897/JIIS2015.0089

31. Brown CSD (2015) Investigating and Prosecuting Cyber Crime: Forensics Dependencies and Barriers to Justice. International Journal of Cyber Criminology 9:55–119

32. Jan Kleijssen and Pierluigi Perri (2017) Cybercrime, Evidence and Territoriality: Issues and Options. T.M.C. ASSER PRESS and the authors 2017. pp. 147-173. URL: https://rm.coe.int/cybercrime-evidence-and-territoriality-issues-and-ptions /168077fa98. DOI 10.1007/978-94-6265-207-1_7

33. Kamini Dashora (2011) Cyber Crime in the Society: Problems and Preventions/ *Journal of Alternative Perspectives in the Social Sciences* (2011) Vol 3, No 1, pp. 240-259. URL: https://www.japss.org/upload/11. Dashora.pdf

34. Nyman Gibson Miralis (2020) The 5 key challenges for law enforcement in fighting cybercrime. URL: ttps://www.lexology. com/library/detail.aspx?g=12513d17-cff3-4d8f-b7dc-cd91826f05d4

35. Boes, S., & Leukfeldt, E.R. (2017). Fighting cybercrime: A joint effort. *?yber-Physical Security: Protecting Critical Infrastructure at the State and Local Level , 3*(1), 185-203.

36. Donalds, C., & Osei-Bryson, K.M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior*, *92*(1), 403-418.

37. Drew, J.M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs. *Police Practice and Research , 19*(6), 537-549.

38. *Global Cybersecurity Index* . (2017). Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci. 01-2017-pdf-e.pdf.

39. Andrii Borko, Vadym Nehodchenko, Olena Volobuieva, Ivan Kharaberiush, Yevheniia Lohvynenko,Fighting against Cybercrime: Problems and Prospects in Ukraine and the World. *Journal of Legal, Ethical and Regulatory Issues/* Research Article: 2019 Vol: 22 Issue: 2S (Print ISSN: 1544-0036; Online ISSN: 1544-0044). URL: https://www.abacademies.org/articles/fighting-against-cybercrime-problems-and-prospects-in-ukraine-and-the-world-8181.html

15. Інформаційні ресурси

1. Верховна Рада України. URL : https://www.rada.gov.ua/
2. Президент України. URL : https://www.president.gov.ua/ru
3. Верховний Суд. URL: https://supreme.court.gov.ua /supreme/gromadyanam/perelik_sprav/
4. Офіс Генерального прокурора України. URL: https://www.gp.gov.ua/ua/index.html
5. Національна академія правових наук України. URL: http://www.aprnu.kharkiv.org/
6. Конституційний Суд України. URL : https://ccu.gov.ua/.

7. Газета "Урядовий кур'єр" URL :http://ukurier.gov.ua/uk/
8. Газета "Юридична практика" URL: http://presa.ua/juridicheskaja-praktika.html
9. Міністерство внутрішніх справ України. URL : https://mvs.gov.ua/uk/contacts/ministry-internal-affairs.
10. Міністерства Юстиції України www.gdo.kiev.ua
11. Єдиний державний реєстр судових рішень. URL : https://reyestr.court.gov.ua/
12. Національна бібліотека України ім. В. І. Вернадського. URL : http://www.nbuv.gov.ua/
13. Бібліотечно-бібліографічні ресурси Верховної Ради України. URL : http://lib.rada.gov.ua/static/about/wellcome.html
14. Національна бібліотека України імені Ярослава Мудрого. URL : https://nlu.org.ua/
15. Науково-технічна бібліотека Національного аерокосмічного університету ім. М.Є Жуковського (ХАІ). URL : https://library.khai.edu/
16. Website of the Budapest Convention. URL : https://www.coe.int/en/web/cybercrime/home
17. Cybercrime Convention Committee (T-CY) – Negotiations of a draft Second Additional Protocol to the Convention on Cybercrime. URL : https://www.coe.int/en/web/cybercrime/t-cy-drafting-group
18. Directorate General Human Rights and Rule of Law – Cybercrime Convention Committee (T-CY). URL : https://www.coe.int/en/web/cybercrime/tcy
19. Directorate General Human Rights and Rule of Law - European Committee on Crime Problems (CDPC). URL : https://www.coe.int/en/web/cdpc/home.