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

Кафедра права (№ 702)

ЗАТВЕРДЖУЮ

Керівник проєктної групи/
Голова НМК
_____ Голубов А. Є.
(підпис) (ініціали та прізвище)
«31» серпня 2020 р.

РОБОЧА ПРОГРАМА ВИБІРКОВОЇ 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)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2020 рік

Робоча програма КВАЛІФІКАЦІЯ ТА ОРГАНІЗАЦІЯ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У СФЕРІ ВИКОРИСТАННЯ КОМП'ЮТЕРІВ, АВТОМАТИЗОВАНИХ СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ
(назва дисципліни)
для студентів за спеціальністю 081 Право
освітньою програмою Право

«_31_» _серпня _ 2020 р., – 38 с.

Розробник: Професор кафедри права
канд. юрид. н., професор Шинкаренко І.Р.
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри права
(назва кафедри)
Протокол № 1 від «31» серпня 2020 р.

Завідувач кафедри д-р юр. наук, проф. Г.О. Спіцина
(науковий ступінь і вчене звання) (підпис) (ініціали та прізвище)

1.Опис навчальної дисципліни

<table>
<tr><td>Найменування показника</td><td>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни (денна форма навчання)</td></tr>
<tr><td>Кількість кредитів:
Денна форма навчання 3;
Заочна форма навчання 3</td><td rowspan="13">Галузь знань
<u>08 Право</u>
(шифр та найменування)

Спеціальність
<u>081 Право</u>
(код та найменування)

Освітня програма
<u>Право</u>
(найменування)
(найменування)

Рівень вищої освіти:

перший (бакалаврський)</td><td>вибіркова</td></tr>
<tr><td>Кількість модулів – 1</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістовних модулів – 2</td><td>2020/2021</td></tr>
<tr><td>Індивідуальне завдання -не має

(назва)</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин :
денна –32/90</td><td>7-й</td></tr>
<tr><td>Лекції*</td></tr>
<tr><td rowspan="8">Кількість тижневих годин для денної форми навчання:
аудиторних – 2
самостійної роботи студента – 4</td><td>16 годин</td></tr>
<tr><td>Практичні, семінарські*</td></tr>
<tr><td>16 годин</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>Годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>58 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>модульний контроль, залік</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить:

для денної форми навчання – 32/58;

[1)] Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета вивчення:

- формування у студентів теоретичних і практичних знань, кримінально-правової кваліфікації злочинів 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 злочинів сучасних інформаційних технологій, комп'ютерної техніки та засобів телекомунікації.

- формування теоретичного підгрунтя практичних навичок з формування організаційно-тактичної моделі розслідування кримінальних правопорушень у сфері використання комп’ютерів, автоматизованих систем та комп’ютерних мереж і мереж електрозв’язку;

Завдання вивчення навчальної дисципліни. 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 злочинів 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 злочинів;

- правил застосування закону про кримінальну відповідальність; формування системи знань про закономірності механізму вчинення злочинів у сфері комп’ютерних злочинів; вивчення особливостей механізму створення слідів при здійсненні злочинів у сфері комп’ютерних злочинів і специфіки формування доказової бази;

- криміналістичних методик розслідування комп’ютерних злочинів;

2) системи вмінь:

- застосування техніко-криміналістичних та тактичних засобів, криміналістичних методик у практичній діяльності з розслідування окремих видів злочинів пов'язаних з використанням комп'ютерної техніки та

інформаційних технологій.

У результаті вивчення дисципліни студент повинен

знати:

- загальні та специфічні ознаки кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку;

- загальний понятійний апарат щодо запобігання, виявлення, кваліфікації та організації розслідування кримінальних правопорушень взагалі та у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку, зокрема;

- вивчити зміст, завдання і значення інститутів Загальної, Особливої частини кримінального права України, Кримінально процесуального законодавств, криміналістичної техніки, криміналістичної тактики та методики розслідування кримінальних правопорушень;

- знати теоретичні та правові засади особливостей організації використання слідчих(розшукових) та негласних слідчих (розшукових) дій та спеціальних знань під час розслідування кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку;

вміти:

- вільно орієнтуватися в структурі чинного Кримінального кодексу України, Кримінального процесуального кодексу, відочих нормативних актах, вміти здійснювати пошук та систематизацію правових норм та застосовувати означені норми при організації попередження, виявлення та розкриття кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку, зокрема;

- використовувати знання законодавства про кримінальну відповідальність та положень Кримінального процесуального кодексу під час організації діяльності з виявлення ознак кримінальних правопорушень, аналізувати загальний їх склад, що закріплені в кримінальному законодавстві, при вирішенні практичних завдань, передбачених навчальним планом;

- вміти організовувати розслідування кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку з використанням всього комплексу сил, засобів гласних та негласних слідчих (розшукових) дій та спеціальних знань;

- вміти проводити аналіз судової та слідчої практики та використовувати її при вирішенні практичних завдань та вибору відповідних тактичних прийомів та криміналістичної методики.

Згідно з вимогами освітньо-професійної програми студенти повинні досягти таких 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 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 оцінки заздалегідь невідомих умов та обставин.
– ПРН 2. Здійснювати аналіз суспільних процесів у контексті аналізованої 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 аналізу відомої проблеми.
– ПРН 5. Давати короткий висновок щодо окремих фактичних обставин (даних) з достатньою обґрунтованістю.
– ПРН 6. Оцінювати недоліки і переваги аргументів, аналізуючи відому проблему.
– ПРН 7. Складати та узгоджувати план власного дослідження і самостійно збирати матеріали за визначеними джерелами.
– ПРН 8. Використовувати різноманітні інформаційні джерела для повного
– та всебічного встановлення певних обставин.
– ПРН 9. Самостійно визначати ті обставини, у з‘ясуванні яких потрібна допомога, 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 розумінням професійного та суспільного контексту.
– ПРН14. Належно використовувати статистичну інформацію, отриману з першоджерел та вторинних джерел для своєї професійної діяльності.
– ПРН 15. Вільно використовувати для професійної діяльності доступні інформаційні технології і бази даних.
– ПРН 16. Демонструвати вміння користуватися комп‘ютерними програмами, необхідними у професійній діяльності.
– ПРН 17. Працювати в групі, формуючи власний внесок у виконання завдань 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 прав та інтересів клієнтів у різних правових ситуаціях.

Міждисциплінарні зв'язки: Вивчення курсу " Кваліфікація та організація розслідування кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку" здійснюється на основі отриманих знань з дисциплін "Теорія держави та права", "Адміністративне право", «Кримінальне право», «Кримінально-процесуальне право», «Криміналістика» та ін. Знання, отримані під час вивчення «Кваліфікація та організація розслідування кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку», наддадуть можливість для опанування основними поняттями у сфері інформаційної безпеки.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗМІСТОВИЙ 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.

Поняття кібер-правопорушень відповідно до Конвенції про кіберзлочинність та міжнародних правових актів. Види кібер-правопорушень за Конвенцією про кіберзлочинність. 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 кібер-правопорушень, 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.

Тема 2. КВАЛІФІКАЦІЯ КРИМІНАЛЬНИХ КІБЕРПРАВОПОРУШЕНЬ ПРАВОПОРУШЕННЯ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ.

Кваліфікація несанкціонованого втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем,

комп'ютерних мереж чи мереж електрозв'язку. Кваліфікація створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збуту. Кваліфікація 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. Кваліфікація 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. Кваліфікація 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. Кваліфікація перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку. Розмежування кримінальних кібер-правопорушень, що посягають на конфіденційність, цілісність і доступність комп'ютерних даних і систем від суміжних складів кримінальних правопорушень.

Тема 3. КВАЛІФІКАЦІЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ЗАГАЛЬНОКРИМІНАЛЬНОЇ СПРЯМОВАНОСТІ А ТАКОЖ ПОВ'ЯЗАНИХ З РОЗПОВСЮДЖЕННЯМ ЗАБОРОНЕНОГО КОНТЕНТУ ТА ПОРУШЕННЯМ АВТОРСЬКОГО ПРАВА, СУМІЖНИХ ПРАВ, ЩО ВЧИНЯЮТЬСЯ З ВИКОРИСТАННЯМ ПРОГРАМНИХ І ТЕХНІЧНИХ ЗАСОБІВ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ.

Кваліфікація кримінальних кібер-правопорушень проти основ національної безпеки України. Кваліфікація кримінальних кібер-правопорушень проти виборчих, трудових та інших особистих прав і свобод людини і громадянина. Кваліфікація кримінальних кіберправопорушень (кримінальні проступки та злочини) проти власності. Кваліфікація кримінальних кіберправопорушень проти громадської безпеки. Кваліфікація

кримінальних кіберправопорушень проти безпеки руху та експлуатації транспорту. Кваліфікація кримінальних кіберправопорушень проти громадського порядку та моральності. Кваліфікація кримінальних кіберправопорушень проти миру, безпеки людства та міжнародного правопорядку. Відмежування кримінальних кіберправопорушень загальнокримінальної спрямованості від кіберправопорушення, що посягають на конфіденційність, цілісність і доступність комп'ютерних даних і систем.

Кваліфікація виготовлення, розповсюдження та збуту порнографічних матеріалів, що вчиняються з використанням програмних і технічних засобів інформаційно-телекомунікаційних систем. Кваліфікація 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. Кваліфікація порушення прав на винахід, корисну модель, промисловий зразок, топографію інтегральної мікросхеми, сорт рослин, раціоналізаторську пропозицію, яке вчиняється з використанням програмних і технічних засобів інформаційно-телекомунікаційних систем. Порушення прав на об'єкти інтелектуальної власності, що можуть бути розміщені в мережі Інтернет, та їх класифікація. Відмежування кібер-правопорушення, пов'язаних зі змістом даних та порушенням авторського права та суміжних прав від кримінальних кібер-правопорушень загально кримінальної спрямованості та кримінальних кібер-правопорушень, що посягають на конфіденційність, цілісність і доступність комп'ютерних даних і систем.

Тема № 4. Кримінологічна характеристика кіберзлочинності (кримінальної кібер-протиправності) та особливості її попередження.

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.

Модульний контроль.

ЗМІСТОВНИЙ МОДУЛЬ № 2. ОРГАНІЗАЦІЯ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У СФЕРІ ВИКОРИСТАННЯ КОМП'ЮТЕРІВ, АВТОМАТИЗОВАНИХ СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

ТЕМА №5. ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРОВАДЖЕНЬ ЗА ФАКТАМИ ВЧИНЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У СФЕРІ ВИКОРИСТАННЯ КОМП'ЮТЕРІВ, АВТОМАТИЗОВАНИХ СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ (КІБЕРЗЛОЧИНІВ).

Особливості механізму вчинення злочинів, пов'язаних з використанням мережі Інтернет. Характеристика осіб та організованих злочинних груп, що вчинюють кримінальні кібер-правопорушення. Характеристика типових слідів кіберзлочинів.

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 кібер-правопорушення. Форми та особливості взаємодії слідчого з правоохоронними органами інших країн при розслідуванні кримінальні кібер-правопорушення. Види та особливості тактики слідчих (розшукових) дій, які проводяться при розслідуванні кримінальні кібер-правопорушення, вчинених з використанням мережі Інтернет.

Тема № 6. ЗАГАЛЬНІ ПОЛОЖЕННЯ МЕТОДИКИ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ КІБЕР ПРАВОПОРУШЕНЬ.

Теоретичні та тактичні засади методики розслідування кримінальних кібер-правопорушень. 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 кібер-правопорушень. 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.

Тема №7. Методика розслідування окремих видів кримінальних правопорушень, які вчиняються з використанням електронно-обчислювальних машин, комп'ютерних програм та мережі Інтернет.

Криміналістична характеристика та методика розслідування кримінальних кібер - правопорушень, 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

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.

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 судових експертиз).

Особливості організації проведення та використання результатів НС(Р)Д (зняття інформації з транспортних телекомунікаційних мереж; зняття інформації 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.

Модульний контроль.

4. Структура навчальної дисципліни

Назва змістовного модуля і тем	Кількість годин				
	Усього	У тому числі			
		Л	С	П	с. р.
1	2	3	4	5	6
Модуль 1. Кримінальне право. Загальна частина					
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 (кіберзлочинів).	8	2	1		5
Тема 2. Кваліфікація кримінальних кібер-правопорушень, що посягають на конфіденційність, цілісність і доступність комп’ютерних даних і систем.	14	2		2	10
Тема 3. Кваліфікація кримінальних правопорушень загально-кримінальної спрямованості а також пов’язаних з розповсюдженням забороненого контенту та порушенням авторського права, суміжних прав, що вчиняються з використанням програмних і технічних засобів інформаційно-телекомунікаційних систем	12	2		2	8
Тема № 4. Кримінологічна характеристика кримінальної кібер-протиправності (кіберзлочинності) та особливості її попередження.	10	2	2		6

Модульний контроль	1				
Разом за змістовним модулем 1	45	8	3	4	29
Змістовний модуль № 2. Організація розслідування кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку					
Тема № 5. **О**собливості розслідування кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку (кіберзлочинів)	10	2	1		7
Тема № 6. Методика розслідування кримінальних кібер-правопорушень, що посягають на конфіденційність, цілісність і доступність комп’ютерних даних і систем.	11	2	2		7
Тема №7. Методика розслідування окремих видів кримінальних правопорушень, які вчиняються з використанням електронно-обчислювальних машин, комп’ютерних програм та мережі Інтернет.	12	2		2	8
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**.**	11	2		2	7
Модульний контроль	1				
Разом за змістовним модулем 2	45	8	3	4	29
Контрольний захід					
Усього годин	90	16	8	8	58

5. Теми семінарських занять

№ п/п	Назва теми	Кількість годин
1	Тема 1. Загальна характеристика кримінальних правопорушень, що вчиняються з використанням програмних і технічних засобів інформаційно-телекомунікаційних систем (кіберзлочинів).	2
2	Тема № 4. Кримінологічна характеристика кримінальної кібер-протиправності (кіберзлочинності) та особливості її попередження.	2
3	Тема № 5. **О**собливості розслідування кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку (кіберзлочинів)	2
4	Тема №6. Методика розслідування окремих видів кримінальних правопорушень, які вчиняються з використанням електронно-обчислювальних машин, комп’ютерних програм та мережі Інтернет.	2
	Разом	8

6. Теми практичних занять

№ п/п	Назва теми	Кількість годин
1	Тема 2. Кваліфікація кримінальних кібер-правопорушень, що посягають на конфіденційність, цілісність і доступність комп’ютерних даних і систем.	2
2	Тема 3. Кваліфікація кримінальних правопорушень загально-кримінальної спрямованості а також пов’язаних з розповсюдженням забороненого контенту та порушенням авторського права, суміжних прав, що вчиняються з використанням програмних і технічних засобів інформаційно-телекомунікаційних систем	2
3	Тема №7 Методика розслідування окремих видів кримінальних правопорушень, які вчиняються з використанням електронно-обчислювальних машин, комп’ютерних програм та мережі Інтернет.	2
4	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**.**	2
	Разом	8

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		Денна форма навчання	Заочна форма навчання
1			
2			
	Разом		

8. Самостійна робота

№ п/п	Назва теми	Кількість годин
1	Тема 1. Загальна характери-стика кримінальних право-порушень, що вчиняються з використанням програмних і технічних засобів інформаційно-телекомунікаційних систем (кіберзлочинів).	5
2	Тема 2. Кваліфікація кіберзлочинів, що посягають на конфіденційність, цілісність і доступність комп’ютерних даних і систем.	10
3	Тема 3. Кваліфікація кримі-нальних правопорушень зага-льнокримінальної спрямованості, що вчиняються з використанням програмних і технічних засобів інформа-ційно-телекомунікаційних систем.	8
4	Тема № 4. Кримінологічна характеристика кримінальної кіберпротиправності та особливості її попередження.	6
5	Тема № 5. **О**собливості розслідування кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку (кіберзлочинів)	7
6	Тема № 6. Методика розслідування кіберзлочинів, що посягають на конфіденційність, цілісність і доступність комп’ютерних даних і систем.	7
7	Тема №7. Методика розслідування окремих видів кримінальних правопорушень, які вчиняються з використанням електронно-обчислювальних машин, комп’ютерних програм та мережі Інтернет.	8
8	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**.**	7
	Разом	58

9. Індивідуальні завдання

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.

10. Методи навчання

Проведення аудиторних лекцій, практичних занять, індивідуальні консультації (при необхідності), самостійна робота студентів за матеріалами, опублікованими кафедрою (методичні посібники), проведення олімпіад.

11. Методи контролю

Поточний контроль:

- опитування на практичних заняттях;
- вирішення конкретних 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 екзамену;
- підготовка й захист курсової роботи.

12. Критерії оцінювання та розподіл балів, які отримують студенти

12.1. Розподіл балів, які отримують студенти (кількісні критерії оцінювання)

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**

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.

Семестровий контроль (іспит/залік) проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до іспиту/заліку. Під час складання семестрового іспиту/заліку студент має можливість отримати максимум 100 балів.

Білет для іспиту/заліку складається з**:**

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

Приклад

1. Поняття та ознаки кримінального кібер правопорушення. -20 балів
2. Типові тактичні операції початкового етапу розслідування кримінальних кібер правопорушень.

ІІ. Практична частина (завдання для виявлення рівня сформованості умінь та практичних навичок професійної діяльності). – максимальна оцінка 60 балів

Всього – максимальна оцінка 100 балів

12.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки, знати:

- основні положення, його, предмет та метод правового регулювання;
- загальні та специфічні ознаки кримінальних кібер-правопорушень;
- завдання та функції та принципи запобігання, виявлення та розслідування кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку;
- загальний понятійний апарат кримінального, кримінального процесуального права України, організації розслідування кримінальних правопорушень;
- інститути, закріплені в кримінальному права України, які узагальнюють ознаки, що властиві кримінальним правопорушенням у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку;
- правила організації запобігання, виявлення та розслідування кримінального правопорушення, складу кримінального правопорушення, кримінальної відповідальності, покарання та обставин, що виключають

кримінальну протиправність діяння у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку;

- алгоритми запобігання, виявлення, кваліфікації протиправних діянь за фактами підготовки та вчинення кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку.

Необхідний обсяг вмінь для одержання позитивної оцінки. Уміти:

- вільно орієнтуватися в структурі чинного Кримінального кодексу України;
- володіти загальними засадами організації запобігання, виявлення та розслідування кримінальних кібер-правопорушень
- здійснювати пошук та систематизацію норм кримінального кримінального процесуального права України;
- тлумачити норми Кримінального кодексу та Криінального процесуального кодексу України;
- застосовувати положення кримінального та кримінального процесуального законодавства, правил та алгоритмів кваліфікації кримінально протиправних діянь під час запобігання, виявлення та розслідування кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку;
- відтворювати основні поняття та категорії, що відображають сутність кримінального та кримінального процесуального прав;
- довільно використовувати засвоєні знання для розв’язання типових ситуацій, що виникають під час розслідування, розкриття, запобігання кримінальних кібер-правопорушень, а також організовувати свою діяльність на основі певного алгоритму;
- орієнтуватися у процесі зміни професійних завдань та ускладнення криміногенної обстановки, знаходити шляхи розв’язку нетипових задач, що виникають під час розслідування, запобігання кримінальних кібер-правопорушень;

- переосмислювати наявні знання стосовно нових змін, що відбуваються в кримінальному та кримінальному процесуальному законодавстві України;
- варіативно розв’язувати професійні завдання.

12.3 Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити всі індивідуальні завдання та здати тестування. Теоретичні знания студента мають деякі прогалини, студент значний час розшукує відповідну кримінально-правову норму, методику та тактику здійснення організаційних заходів та слідчих (розшукових) дій необхідних для вирішення практичної ситуації, хоча без нормативного підкріплення може розкрити шляхи вирішення проблеми. Студент демонструє невпевненість в знаниях теоретичного матеріалу.

Добре (75-89). Твердо знати мінімум, захистити всі індивідуальні завдання, виконати всі КР , здати тестування та поза аудиторну самостійну роботу. Відповіді на питання отримані правильні, студент продемонстрував достатні знания теоретичного матеріалу курсу, але при вирішенні практичної ситуації, обравши правильний напрямок, не зміг раціонально використати відповідні правові норми та відповідні тактичні алгоритми використання слідчих (розшукових) дій, вміє аналізувати тенденції юридичної практики та оцінювати їх з точки зору відповідності закону.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти застосовувати їх. Відповіді на питання отримані повні та правильні. Студент продемонстрував знання теоретичного матеріалу та вміння аналізувати конкретні нормативно-правові акти та окремі норми чинного законодавства, застосувати їх до вирішення практичних ситуацій, які виникають під час запобігання, виявлення та розслідування фактів вчинення кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку.

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

12.4. Дотримання вимог академічної доброчесності студентами під час вивчення навчальної дисципліни

Під час вивчення навчальної дисципліни студенти мають дотримуватися загальноприйнятих морально-етичних норм і правил поведінки, вимог академічної доброчесності, передбачених Положенням про академічну доброчесність Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут» (https://khai.edu/assets/files/polozhennya/polozhennya-pro-akademichnu-dobrochesnist.pdf)

13. Методичне забезпечення

1. Робоча програма «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, 2020. 34 с.

2. Кваліфікація та організація розслідування кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку: конспект лекцій для здобувачів вищої освіти, спеціальності 081 – «Право», другий рівень овищої освіти: денна форма / укладачі: І.Р. Шинкаренко. Харків: Нац. Аерокосм. університет, 2020. 425 с.

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, 2020. 58 с.

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, 2020. 42 с.

5. Електронний ресурс ХАІ 081-Право: https://education.khai.edu/program /081-1-40

14. Рекомендована література

Нормативно-правові акти:

1. Конституція України від 28.06.1996 р. *Відомості Верховної Ради* України. 1996. № 30. Ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

2. Кримінальний кодекс України від 05.04.2001 р. *Відомості Верховної Ради України*. 2001. № 25. Ст. 131. 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. 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. 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. 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. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, від 28.01.2003 р. 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. 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. 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. 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. 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. URL: https://zakon.rada.gov.ua/laws/show/2163-19./

14. 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/. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF.

15. 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. URL: https://zakon.rada.gov.ua/laws/show/295-2012-%D0%BF.

16.Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96/2016. *Урядовий кур'єр.* від 18.03.2016. № 52. URL: https://zakon5.rada.gov.ua/laws/show/96/2016.

17. Про заходи протидії незаконному обігу наркотичних засобів психотропних речовин і прекурсорів та зловживання ними : Закон України від 15.02.1995 р. № 62/95-ВР . БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/62/95-%D0%B2%D1%80.

18. Про наркотичні засоби, психотропні речовини, їх аналоги і прекурсори : Закон України від 15.02.1995 р. № 60/95-ВР // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/60/95-%D0%B2%D1%80.

19. Про організаційно-правові основи боротьби з організованою злочинністю: Закон України від 30.06.1993 р. № 3341-XII // 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» / 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. // 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. // БД «Законодавство України» / ВР України. URL: http://zakon4.rada.gov.ua/laws/show/z0937-17.

23. Про затвердження Інструкції з організації проведення та оформлення експертних проваджень у підрозділах Експертної служби Міністерства внутрішніх справ України : Наказ Міністерства внутрішніх справ України 17.07.2017 № 591, зареєстрований в Міністерстві юстиції України 18.08. 2017 р. за № 1024/30892. // БД «Законодавство України» / ВР України. URL: http://zakon0.rada.gov.ua/laws/show/z1024-17.

24. Про затвердження Інструкції про порядок залучення працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України як спеціалістів для участі в проведенні огляду місця події : Наказ МВС України від 03.11.2015 № 1339, зареєстровано у Міністерстві юстиції України 06.11.2015 р. за № 1392/27837. // БД «Законодавство України» / ВР України. URL: http://zakon5.rada.gov.ua/laws/show/z1392-15.

25. 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. // БД «Законодавство України» / ВР України. URL: http://zakon3.rada.gov.ua/laws/show/z0705-98.

Основна література:

26.Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження) : [монографія]. Київ : Атіка, 2007. 304 с.

27.Актуальні проблеми кримінального права: навч. посіб. / В.М. Попович, П.А. Трачук, А.В. Андрушко, С.В. Логін. Київ: Юрінком Інтер, 2009. 256 с.

28.Бутузов В. М., Остапець С. Л., Шеломенцев В. П. Злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Науково-практичний коментар. К. : Друкарня МВС України, 2005. 86 с.

29.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.

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

31.Карчевський М.В. Злочини у сфері використання комп'ютерної техніки : навч. посіб. Луганськ : РВВ ЛДУВС, 2006. 192 с.

32.Кваліфікація злочинів : Навч. посіб. / За ред. О.О. Дудорова, Є.О. Письменського. Київ: Істина, 2010. 430 с.

33.Кримінальне право України. (Особлива частина): Підручник / Кол. авторів А.В. Байлов, О.А. Васильєв, О.О. Житний, та ін.; за заг. ред. О.М. Литвинова; наук. ред. серії О.М. Бандурка. Харків: ХНУВС, 2011. 572 с.

34.Кримінальне право України. Особлива частина : підруч. для студ. вищ. навч. закл. / Г. М. Анісімов [та ін.] ; за ред. проф. В. В. Сташиса, В. Я. Тація ; Нац. юрид. акад. України ім. Ярослава Мудрого. 4-те вид., перероб. і допов. Харків: Право, 2010. 606 с.

35.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.

36. 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.

37. 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.

38. 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.

39.Навроцький В.О. Основи кримінально-правової кваліфікації : навч. посіб. 2-ге вид. Київ : Юрінком Інтер, 2009. 512 с.

40.Науково-практичний коментар до Кримінального кодексу України. Особлива частина. Розділ XVI. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку / В. М. Бутузов, С. А. Кузьмін, В. П. Шеломцев. Київ : Вид. Паливода А. В., 2010. 152 с.

41.Нехорошев А. Б. Компьютерные преступления: квалификация, расследование, экспертиза. Саратов : РИО Сарат. юрид. ин-та МВД России, 2004. 21 с.

42.Орловский Д. Л. Компьютерная преступность : конспект лекций по курсу "Информационная безопасность".Харьков : НТУ "ХПИ", 2006. 64 с.

43.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.

44.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.

45.Савінова Н. А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти : монографія. Київ: ДКС, 2012. 342 с.

46.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.

47. Щербаковський М. Г., Пашнєв Д. В. Розслідування комп'ютерних злочинів : посібник. Харків: ХНУВС, 2010. 112 с.

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

49.Щербаковский М.Г. Судова експертологія: навч. посіб. Харків: ХНУВС, 2009. 192 с.

50.Шендрик В.В., Сафронов С.О., Крєпаков І.О., Жилін Є.В. Боротьба з порнографією: криміналістичні та оперативно-розшукові аспекти. Навч. посіб. Харків, 2010. 216 с.

51.Хільченко С.В. Методика розслідування поширення порнографічних предметів: Навч. посіб. Київ: Вид. ПАЛИВОДА А.В., 2008. 152 с.

52.Карчевський М.В. Особливості розслідування шахрайств, вчинених у сфері функціонування електронних розрахунків: метод. реком., Луганськ. 2010. 56 с.

53.Карчевський М.В. Злочини у сфері використання комп'ютерної техніки: навч. Посібник. Луганськ: РВВ ЛДУВС, 2006. 192 с.

54.Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами : [монографія]. Запоріжжя : ГУ «ЗІДМУ», 2003. 250 с.

55.Злочини в сфері використання комп'ютерної техніки: кваліфікація, розслідування та протидія: монографія /І. Р. Шинкаренко, В.О. Голубєв,М.В. Карчевский, І.Ф. Хараберюш. Донецьк: ДЮІ ЛДУВС, 2007. 266 с.

Додаткова література:

56.Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : дис. … канд. юрид. наук : 12.00. Київ: Інститут держави і права ім. В. М. Корецького НАН України, 2003. 246 с.

57.Бутузов В. М. Протидія комп'ютерній злочинності в Україні

(системно-структурний аналіз) : монографія. Київ: КИТ, 2010. 408 с.

58.Вехов В. Б., Голубев В. А. Расследование компьютерных преступлений в странах СНГ : монография. Волгоград : Вол-гогр. акад. МВД России, 2004. 304 с.

59.Волеводз А. Г. Противодействие компьютерным преступлениям: Правовые основы междунар. Сотрудничества. Москва: Юрлитинформ, 2002. 485 с.

60.Голубев В. А. Информационная безопасность: проблемы борьбы с киберпреступлениями: монография. Запорожье: ГУ «ЗИГМУ», 2003. 336 с.

61.Голубев В. А., Цимбалюк В. С. Проблемы борьбы с преступлениями в сфере использования компьютерных технологий : учеб. пособие / Под общ. ред. Р. А. Калюжного. Запорожье : ГУ "ЗИГМУ", 2002. 292 с.

62.Дрьомов С. В. Сутність копіювання як форми несанкціонованих дій з інформацією, яка обробляється в ЕОМах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації. *Підприємництво, господарство і право.* 2005. № 9. С. 144–147.

63.Карчевский Н. В. Компьютерная информация как предмет криминально-правовой охраны. *Правові основи захисту комп'ютерної інформації від протиправних посягань : матеріали міжвуз. наук.-практ. конф*., (Донецьк, 22 груд. 2000 р.). Донецьк : Донецький інститут внутрішніх справ, 2001. С. 54–67.

64.Карчевський М. В. Кримінальна відповідальність за незаконне втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину) : дис... канд. юрид. наук : 12.00.08. Харків: Національна юридична академія України ім. Ярослава Мудрого, 2003. 175 с.

65.Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. Москва: Горячая линия-Телеком, 2002. 336 с.

66.Комп'ютерна злочинність : навч. посіб. / [Біленчук П. Д., Бут В. В., Гавловський В. Д. та ін.]. К. : Атіка, 2002. 240с.

67.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.

68.Компьютерные террористы: Новейшие технологии на службе преступного мира / [авт.-сост. Татьяна Ивановна Ревяко]. Минск : Литература, 1997. 639 с. (Энциклопедия преступлений и катастроф).

69.Крылов В. В. Информационные компьютерные преступления : учеб. и практ. Пособие. Москва : ИНФРА-М ; Норма, 1997. 276 с.

70.Мещеряков В. А. Преступления в сфере компьютерной информации: Основы теории и практики расследования. Воронеж : Изд-во Воронеж. гос. ун-та, 2002. 407с.

71.Міхайліна Т. Кваліфікація незаконних дій з програмними та технічними засобами, що вчиняються групою осіб. *Правничий часопис* Донец. ун-ту. 2009. – №1-2. С. 186-190.

72.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.

73. 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.

74.Правові основи охорони інформації / В. Ф. Авраменко [та ін.] ; ред. В. О. Хорошко. К. : ТОВ "ПоліграфКонсалтинг", 2003.176 с.

75.Орлов П. І. Інформація та інформатизація: нормативно-правове забезпечення : на58-ук.-практ. посіб. 2-е вид., випр. і доп. Х. : Вид-во Нац. ун-ту внутр. справ, 2003. 724 с.

76.Орлов С. О. Кримінально-правова охорона інформації в комп’ютерних системах та телекомунікаційних мережах : дис. … канд. юрид.

наук : 12.00.08. Харків: Національній університет внутрішніх справ, 2004. 213 с.

77.Панов М. І. Злочини у сфері обслуговування електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Вибрані наукові праці з проблем правознавства.* Київ: Ін Юре, 2010. С. 758-775.

78.Пашнєв Д. В. Комп'ютерні технології як засіб вчинення злочину / Д. В. Пашнєв. *Вісник Кримінологічної асоціації України*: матеріали Всеукраїнської наук.-практ. конференції, присвяченої 20-річчю заснування кафедри кримінального права та кримінології Харківського національного університету внутрішніх справ 12 травня 2012 року «Актуальні сучасні проблеми кримінального права та кримінології у світлі реформування кримінальної юстиції». Том 1. С.144-146.

79.Пашнев Д. В. Компьютерные технологии как средство совершения преступлений, связанных с терроризмом. *Противодействие ксенофобии, экстремизму и терроризму в современном обществе:* Научные труды Международной научно-практической конференции / Под общ. ред. Игнатова А.Н. ; Институт экономики и права (филиал) ОУП ВПО «Академия труда и социальных отношений» в г. Севастополе. Симферополь: КРП «Издательство «Крымучпедгиз», 2012. С. 174-177.

80. Пашнєв Д. В. Несанкціонований доступ до комп'ютерної інформації як спосіб вчинення злочину. *Кримські юридичні читання: мат-ли міжн. наук.-практ. конф.* 11 травня 2012 р. / Нац. університет «Одеська юридична академія» Економіко-правовий факультет у м. Сімферополь. Сімферополь: Кримнавчпеддержвидав, 2012. С. 58-63.

81.Пашнєв Д. В. Властивості комп'ютерної інформації як предмету злочину. *Вісник Кримінологічної асоціації України* : збірник наукових праць [Редкол. Л. М. Давиденко, Т. А. Денисова, О. М. Джужа та ін.]. № 1. Х. : ХНУВС, 2012. С. 115-125.

82.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.

83.Плугатир М. В. Комп'ютерна інформація як предмет злочинів, передбачених статтями 361–363-1 КК України. *Матеріали Міжнародної науково-практичної інтернет-конференції* ["Сучасна юридична наукова думка"] (Тернопіль, 9 груд. 2008 р.). Тернопіль, 2008. С. 32–34.

84.Плугатир М. В. Проблемні питання законодавчого визначення об'єктивної сторони злочину, передбаченого ст. 361-2 КК України. *Наука і вища освіта:* тези доповідей учасників XVII Міжнар. наук. конф. студентів і молодих науковців, (Запоріжжя, 9–10 квіт. 2009 р.) : у 4 т. / Класичний приватний університет. – Запоріжжя : КПУ, 2009. Т. 4. С. 113.

85.Плугатир М. Предмет злочинів, передбачених розділом XVI Особливої частини Кримінального кодексу України. *Підприємництво, господарство і право*. 2009. № 7. С. 127–130.

86.Плугатир М. Родовий об'єкт злочинів, передбачених розділом XVI Особливої частини КК України. *Юридична Україна.* 2009. № 4. С. 98–101.

87.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.

88.Преступления в сфере использования компьютерной техники: квалификация, расследование и противодействие : монографія / [И. Р. Шинкаренко и др.]. Донецк : РВВ ЛДУВС, 2007. 267 с.

89. Розенфельд Н. А. Кримінально-правова характеристика незаконного втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж : дис. … канд. юрид. наук : 12.00.08.Київ: Інститут держави і права ім. В. М. Корецького НАН України, 2003.– 222 с.

90. 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.

91.Юртаєва К. В., Селиванов М. В. Визначення місця вчинення злочинів з використанням. Київ: Юридическая фирма "Центр

интеллектуальной собственности «Смотров, Селиванов и партнеры».– 2007. URL: http://www.cip.in.ua/r4436/.

92.Соловьев Л. Н. Вредоносные программы: расследование и предупреждение преступлений. Москва: Собрание, 2004. 221с.

93.Шендрик В. В., Литвинов М. Ю. Проблеми визначення причинно-наслідкового зв'язку між діянням та наслідками комп'ютерного злочину. *Боротьба зі злочинами у сфері комп'ютерної інформації : проблеми та шляхи їх вирішення*: матеріали міжвуз. наук.-практ. конф. 14 груд. 2007 р. Донецьк : Донец. юрид. ін-т, 2008. С. 209-212.

94. Шинкаренко І.Р. Злочини в сфері використання комп'ютерної техніки: кваліфікація, розслідування та протидія: монографія /І. Р. Шинкаренко, В.О. Голубєв,М.В. Карчевский, І.Ф. Хараберюш. Донецьк: ДЮІ ЛДУВС, 2007. 266 с.

95. 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.

96. 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.

97. 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.

98. 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.

99. Особливості взаємодії органів досудового розслідування УМВС на залізницях з оперативними підрозділами, зокрема з підрозділами УОС та

УОТЗ в областях, під час проведення НСРД : методичні рекомендації / Укладачі: Шинкаренко І.Р., Дараган В.В., Федотенко А.В. Дніпропетровськ: ДДУВС, 2014. 75 с.

100. 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).

101. 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.

102. 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.

103. 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.

104. Алгоритм дій поліцейських підрозділів кримінальної поліції (карний розшук) щодо документування кримінальних правопорушень, що вчинюються в надзвичайних умовах: метоличні рекомендації / укладачі: І.Р. Шинкаренко, А.Є. Дідочкін, А.О. Кисельов. Дніпро: ДДУВС, ГУ НП в Дніпропетровській області, 2016. 34 с.

105. Виявлення, припинення, документування підрозділами кримінальної поліції (карний розшук) злочинних дій щодо підготовки вчинення квартирних крадіжок в умовах великих міст / А.Є. Дідочкін, В.В. Єфімов, С.М. Мороз, І.Р. Шинкаренко. Дніпро: ДДУВС, ГУ НП в Дніпропетровській області, 2016. 40 с.

106. Алгоритм дій щодо проведення оперативної комбінації, з метою забезпечення оперативно–розшукової діяльності поліцейських кримінальної

поліції (карний розшук) / укладачі: А.С. Богач, В.В. Єфімов, С.М. Мороз, І.Р. Шинкаренко. Дніпро: ДДУВС, ГУ НП в Дніпропетровській області, 2016. 47с.

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

108. Юртаєва К. В. Визначення місця вчинення злочинів з використанням комп'ютерних технологій / К. В. Юртаєва // Форум права. 2009. № 2. С. 434–441.

Інформаційні ресурси в Інтернеті

1. Офіційний сайт Верховної Ради України http://www.iportal.rada.gov.ua
2. Офіційний сайт Кабінету Міністрів України http://www.kmu.gov.ua
3. Офіційний сайт МВС України http://www.mvs.gov.ua
4. Офіційний сайт Національної поліції України https://www.npu.gov.ua/
5. Офіційний сайт Судової влади України https://court.gov.ua/
6. Інформаційне агентство ЛІГАБІЗНЕСІНФОРМ http://www.lbi.ua
7. Єдиний державний реєстр судових рішень http://www.reyestr.court.gov.ua