МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

О. А. Самойленко

ВИЯВЛЕННЯ ТА РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Навчально –методичний посібник

Освітня програма підготовки здобувачів вищої освіти
ступеня магістра права
в Національному університеті «Одеська юридична академія»
галузь знань – 08 «Право»
спеціальність – 081 «Право»

Одеса
2020

УДК
343.346.8:004

Рекомендовано до друку навчально-методичною радою Національного університету «Одеська юридична академія» (протокол № ___ від ___.05.2020 р.).

Автор

Самойленко Олена Анатоліївна, доцент кафедри криміналістики Національного університету «Одеська юридична академія», кандидат юридичних наук, доцент

Рецензенти:

Подобний Олександр Олександрович, професор кафедри криміналістики Національного університету «Одеська юридична академія», доктор юридичних наук, професор;

Чорноус Юлія Миколаївна, професор кафедри криміналістики та судової медицини Національної академії внутрішніх справ, доктор юридичних наук, професор

Самойленко О. А.

С178 Виявлення та розслідування кіберзлочинів [Текст] : навчально-методичний посібник / О. А. Самойленко. Одеса : , 2020. 112 с.

У навчально-методичному посібнику висвітлено основи виявлення та розслідування кіберзлочинів. Розглянуто специфіку злочинної діяльності у кіберпросторі, проблемні аспекти початку кримінального провадження, специфіку використання спеціальних знань підчас розслідування кіберзлочинів особливості розслідування окремих видів злочинів, що вчиняються у обстановці кіберпростору та із застосуванням ІТ-технологій.

Матеріали призначені для науковців, викладачів та здобувачів закладів вищої юридичної освіти, а також будуть корисними суддям, прокурорам, працівникам оперативних підрозділів, захисникам (адвокатам) та іншим фахівцям юридичного профілю.

УДК 343.346.8:004

ISBN

ЗМІСТ

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Сьогодні глобальна всесвітня мережа, що об'єднує мільйони комп'ютерів у транснаціональну єдину систему Інтернет, відкриває широкі можливості для спілкування та обміну інформацією будь-якого характеру. Це зумовило виникнення нового типу суспільних відносин – відносин у кіберпросторі, що підносять на якісно новий рівень розвитку всі сфери життєдіяльності, зокрема економіку, державне управління, мистецтво, науку, освіту тощо. Втім, нарівні з позитивними здобутками Інтернет-середовище характеризується побічними, негативними явищами криміногенного характеру, до яких відносять порушення авторських прав, розповсюдження та збут творів, що пропагують культ насильства і жорстокості, порнографічних предметів, наркотичних засобів, вимагання, шахрайство через Інтернет та інші види як традиційних, так і власне комп'ютерних злочинів. Технологія вчинення таких злочинів із використанням ІТ-технологій та мережі Інтернет надзвичайно ускладнює процес розслідування порівняно з розслідуванням такої категорії злочинів, учинюваних у звичайних умовах. Зазначеним слід пояснювати необхідність вивчення методичних та практичних питань розслідування кіберзлочинів. Хоча слідчі є тими суб'єктами, котрі використовують криміналістичні рекомендації з виявлення та розслідування кіберзлочинів, сам курс «Виявлення та розслідування кіберзлочинів» може бути корисним й суддям, прокурорам, працівникам оперативних підрозділів, захисникам (адвокатам) та іншим фахівцям юридичного профілю.

Навчальна дисципліна «Виявлення та розслідування кіберзлочинів» включає в себе теоретичні і методичні положення розслідування кіберзлочинів та криміналістичну тактику і методику розслідування кіберзлочинів окремих різновидів, що розроблено на підставі загально-теоретичних положень криміналістики. Дисципліна має як теоретичне, так і практичне значення для розробки науково обґрунтованої програми боротьби зі злочинністю, а також іншими протиправними проявами у життєдіяльності суспільства і держави. Для досягнення цієї мети необхідно мати вміти орієнтуватися у теоретичних положеннях інших юридичних наук (інформаційному, цивільному, господарському, міжнародному-кримінальному праві), у сучасних досягненнях та перспективах розвитку природознавчих та технічних наук, використовувати результати аналізу та узагальнення слідчої і судової практики

Під час підготовки навчально-методичного посібника використовувалися норми діючого вітчизняного та міжнародного законодавства, що регламентують процес здійснення досудового розслідування, оперативно-розшукову діяльність, матеріали слідчої практики, а також наукові праці авторів, що досліджували проблеми боротьби із кіберзлочинами: П. Д. Біленчук, А. С. Білоусов, В. М. Бутузов, А. Ф. Волобуєв, В. Д. Гавловський, В. О. Голубєв, М. В. Гуцалюк, М. В. Карчевський, О. І. Котляревський, М. О. Кравцова, О. М. Лепеха, М. Ю. Літвінов, О. В. Манжай, А. І. Марущак, О. І. Мотлях, І. М. Осика, Л. П. Паламарчук, Д. В. Пашнєв, А. В. Реуцький, С. М. Рогозін, Б. В. Романюк, М. В. Салтевський, С. В. Самойлов, Є. Д. Скулиш, К. В. Тітуніна, Д. М. Цехан, В. С. Цимбалюк, І. Ф. Хараберюш, В. Г. Хахановський,

В. П. Шеломенцев, В. В. Чернєй, С. С. Чернявський, а також іноземних науковців (В. Б. Вехов, Р. І. Дрімлюга, Д. А. Іллюшин, В. Є. Козлов, С. В. Кригін, В. В. Крилов, О. М. Лепехін, А. Л. Осипенко та інші).

Мета вивчення навчальної дисципліни полягає у виробленні здатності використання в професійній юридичній діяльності працівників правоохоронних органів положень криміналістики відповідного виду і рівня сформованості вмінь, а саме: підчас розслідування кіберзлочинів, враховуючи головні теоретичні положення науки криміналістики, використовувати основні техніко-криміналістичні засоби, прийоми і методи, тактично правильно будувати версії, планувати розслідування, проводити слідчі дії, тактичні операції, використовувати спеціальні знання, взаємодіяти з працівниками оперативних підрозділів та іншими суб'єктами, виходячи із криміналістичної характеристики злочинів, провадити їх розслідування на початковому та наступному етапі.

Завдання вивчення навчальної дисципліни:

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

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

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

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

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

Автори висловлює вдячність рецензентам навчально-методичного посібника за пропозиції, слушні зауваження та рекомендації. Автор також дякує президенту Національного університету «Одеська юридична академія», доктору юридичних наук, професору, академіку НАПрН України Сергію Васильовичу Ківалову за надану можливість впровадження цієї навчальної дисципліни у навчальний процес Національного університету «Одеської юридичної академії».

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Форма навчання	Курс	Семестр	Лекційні заняття	Практичні заняття	Всього аудиторних занять	Курсові роботи	Контрольні роботи	Самостійна робота	Всього годин	Кількість кредитів ECTS	Екзамен	Залік
Очна	2	3	12	14	26	-	-	49	75	2,5	-	+
Заочна	2	3	4	4	8	-	-	67	75	2,5	-	+

ТЕМАТИЧНИЙ ПЛАН

№ теми	Тема	Лекції		Практичні заняття		Самостійна робота студентів	
		д	з	д	з	д	з
Тема 1	Методичні основи розслідування кіберзлочинів	1	2	2	1	6	
Тема 2	Організаційні та правові основи діяльності осіб у мережі Інтернет в Україні та за її межами	1		2	1	6	
Тема 3	Організаційні засади виявлення та початку кримінального провадження щодо кіберзлочинів	2		2		6	
Тема 4	Використання спеціальних знань під час розслідування кіберзлочинів	2		2		7	
Тема 5	Організаційно-тактичні основи розслідування кіберзлочинів	2	2	2	1	9	
Тема 6	Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов’язані з фінансово-економічною сферою відносин у кіберпросторі	2		2		9	
Тема 7	Розслідування кіберзлочини, вчинені з антидержавно-політичних мотивів, пов’язані з	2		2	1	9	

	державно-політичною сферою відносин суб’єктів у кіберпросторі						
Всього за семестр:		12	4	16	4	49	

НАВЧАЛЬНИЙ КОНТЕНТ

ЛЕКЦІЇ

Лекція № 1
(денна форма навчання)

Лекція №1
(заочна форма навчання)

Тема 1. Методичні основи розслідування кіберзлочинів

Мета вивчення

Надати уявлення та сформувати систему знань про сучасні методологічні основи розслідування кіберзлочинів, визначити основні проблеми правозастосовної практики в цій сфері, а також шляхи їх подолання.

Результати навчання

Після лекції здобувач вищої освіти буде (спроможний):

1) аналізувати і синтезувати досягнення криміналістичної науки у сфері розроблення методик боротьби з кіберзлочинами;

2) застосувати сучасні інформаційні технології та інформаційні ресурси з для розв'язання практичних задач з аналізу злочиннох діяльності у кіберпросторі;

3) орієнтуватися в термінологічному контенті в сфері протидії кіберзлочинності та злочинів, вчинених у кіберпросторі;

4) використовувати в правозастосовній діяльності нормативно-правові акти, що регулюють відносини, що виникають підчас виявлення та розслідування фактів вчинення злочинів у кіберпросторі.

План

1. Сутність поняття «кіберпростір». Особливості кіберпростору, що привертають увагу злочинців до використання його середовища з метою досягнення злочинного результату.
2. Визначення основних технічних термінів, пов'язаних із кіберпростором: телекомунікаційна мережа, комп'ютерна мережа, інформаційні технології, електричний зв'язок, мережа зв'язку, мережа Інтернет.
3. Сутність кіберзлочинів.
4. Класифікація кіберзлочинів.

Основний зміст

1. Сутність поняття «кіберпростір». Особливості кіберпростору, що привертають увагу злочинців до використання його середовища з метою досягнення злочинного результату

З урахуванням комп'ютерної складової електронного обміну інформацією, кіберпростір утворюють усі телекомунікаційні мережі, комп'ютерні системи й пристрої, обмін інформацією в яких здійснюється на базі єдиної системи стандартів і протоколів, що забезпечують процес перетворення вихідної інформації на інформаційний продукт для іншого користувача. Кібепростір сьогодні створює специфічну обстановку вчинення злочинів різних видів,

Кіберпростір слід розуміти як інформаційний простір взаємодії між людьми за допомогою інфраструктури електронних інформаційних технологій, що вміщує Інтернет, інші телекомунікаційні мережі, комп'ютерні системи та пристрої, обмін інформацією в яких здійснюється на базі єдиної системи стандартів і протоколів, що забезпечують процес перетворення вихідної інформації на інформаційний продукт для іншого користувача. Аналіз використання кіберпростору зі злочинною метою, узагальнення матеріалів судово-слідчої практики дозволяють визначити певні *особливості кіберпростору,* які злочинець використовує з метою досягнення злочинного результату: 1) віддаленість (дистанційність) доступу до предмета посягання з використанням кіберпростору, що забезпечує транскордонну складову такої злочинної діяльності, яка викликає необхідність вирішення слідчим питань територіальної юрисдикції;2) оперативність створення, поширення, модифікації або знищення інформації в кіберпросторі, що є предметом злочинного посягання або слідом злочину – це сприяє значному прискоренню та якісному приховуванню злочинної діяльності; 3) віртуальність, що забезпечує відносну конфіденційність інформації про особу злочинця та можливість упливати на свідомість певної категорії осіб;4) комунікативність, яка уможливлює створення злочинних груп та ефективну діяльність уже наявної організованої злочинності; 5) недосконаліть забезпечення інформаційної безпеки та правової охорони відносин у кіберпросторі, що надає злочинцю можливість уникати кримінальної відповідальності за вчинений злочин.

2. Визначення основних технічних термінів, пов'язаних із кіберпростором: телекомунікаційна мережа, комп'ютерна мережа, інформаційні технології, електричний зв'язок, мережа зв'язку, мережа Інтернет

Засоби комп'ютерної техніки за своїм функціональним призначенням поділяються на дві основні групи: апаратні та програмні. Під апаратними розуміють технічні засоби, які використовуються для обробки і пересилання даних. До таких належать: ПК – комплекс технічних засобів, призначених для

автоматичної обробки інформації в процесі розв'язання обчислювальних та інформаційних завдань; периферійне обладнання – таке, що має підлеглий кібернетичний статус в інформаційній системі (будь-який прилад, який забезпечує обмін даними і командами між процесором і користувачем); комплекс зовнішніх приладів ЕОМ, які не перебувають під безпосереднім керуванням центрального процесора; фізичні носії магнітної інформації. Під програмними засобами розуміють об'єктивні форми представлення сукупності даних і команд, призначених для функціонування комп'ютерів і комп'ютерних пристроїв з метою одержання визначеного результату; підготовлені й зафіксовані на фізичному носії матеріали, отримані під час їх розроблення; аудіовізуальні відображення, породжувані ними. До таких належать: програмне забезпечення, що складається з системних програм, прикладних програм (комплекс спеціалізованих програм) та інструментальних програм (систем програмування); машинна інформація власника-користувача. Телекомунікаційна мережа це системоутворювальний комплекс засобів телекомунікацій, що надає територіально розгалуженим об'єктам можливість інформаційної взаємодії шляхом обміну сигналами (радіо-, електричними або оптичними) (за ЗУ про телекомунікації називають, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів,письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням.). У технічному сенсі мережа Інтернет становить глобальну сукупність інформаційних ресурсів і систем, з'єднаних за допомогою електрозв'язку, обмін інформацією в яких здійснюється на базі єдиної системи стандартів і протоколів.

Оцінки загроз кіберзлочинності національній безпеці окремих держав та міжнародному порядку:1) небезпечна тенденція, пов'язана зі збільшенням технічної і технологічної залежності держави від транскордонних проявів кібертерористів, 2) комп'ютерні атаки практично неможливо прогнозувати або прослідити в реальному часі.

3. Сутність кіберзлочинів

Трмін «комп'ютерний злочин» має розширене тлумачення. Ним позначають діяння, в яких комп'ютер є предметом, знаряддям або засобом скоєння злочину. Н відміну від кримінального права, у криміналістиці вид злочину називають навіть не за засобом (знаряддям) вчинення злочину, а за видом злочинної діяльності. На стику XX й XXI століть опубліковано цілу низку праць щодо «комп'ютерного злочину» в такому трактуванні. У більшості джерел чітко визначають дві категорії злочинів, зокрема: 1) коли комп'ютер або інформація в ньому виступає предметом посягання (дії, що кваліфікуються за статтями Розділу XVI КК України); 2) коли комп'ютер є засобом вчинення злочину (традиційно ст. 185, 190, 191 КК України).

Терміносполучення «злочини у сфері комп'ютерної інформації» зумовлено важливістю та значенням об'єкта посягання – комп'ютерної інформації. До

таких відносять злочини, передбачені Розділом XVI КК України, а також ч. 3 ст. 190 КК (шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки) та ст. 200 КК (використання підроблених електронних засобів доступу до банківських рахунків). Класифікація «комп'ютерних злочинів», «злочинів у сфері комп'ютерної інформації» та «інформаційних злочинів», як правило, здійснювалась за кримінально-правовими ознаками відповідної групи злочинів.

Тривала наукова та законодавча невизначеність наведеного соціально-правового явища призвела в країнах СНД до запозичення з міжнародної практики боротьби зі злочинами терміна «кіберзлочин» («cybercrime»). Аналіз сучасних публікацій, тем дисертаційних досліджень та інших джерел інформації дозволяє доволі впевнено стверджувати про всезагальне визнання українською науковою спільнотою цього терміна. При цьому проблему недостатньої аргументованості й хаотичного подання поняття «кіберзлочин», що властиво розробкам закордонних дослідників та зарубіжним правовим актам, екстрапольовано в національну науку. На останньому форумі Конгресу ООн з проблем протидії кіберзлочинам (2015 р.) до категорії «кіберзлочинність» віднесено такі діяння, об'єктом злочину яких є комп'ютерні дані або системи, а також діяння, за яких використання комп'ютерних або інформаційних систем є невід'ємною складовою способу вчинення злочину. До першої класифікаційної групи відносять отримання незаконного доступу до комп'ютерних даних або систем (іноді їх називають «основними» кіберзлочинами). До другої – використання комп'ютерних даних або систем для шахрайства, розкрадання чи спричинення шкоди іншим особам; злочини, пов'язані з використанням комп'ютерів та інтернет-контенту, включаючи пропаганду ненависті, дитячу порнографію, злочини з використанням особистих даних і продаж заборонених товарів. Сутність кіберзлочинів або IT-злочинів, полягає в тому, що це протиправні суспільно небезпечні діяння тобто злочини, під час яких використовується інформаційний простір взаємодії між людьми за допомогою інфраструктури електронних інформаційних технологій, що вміщує Інтернет, інші телекомунікаційні мережі, комп'ютерні системи та пристрої, обмін інформацією в яких здійснюється на базі єдиної системи стандартів і протоколів, що забезпечують процес перетворення вихідної інформації на інформаційний продукт для іншого користувача.

4. Класифікація кіберзлочинів

Для цілей основної криміналістичної класифікації злочинів, вчинених у кіберпросторі, на групи потрібно виходити саме з традиційних сфер суспільного життя суб'єктів кіберпростору, класифікуючи мотиви вчинення злочинів на такі групи:

1) корисливі мотиви, пов'язані з фінансово-економічною сферою відносин суб'єктів у кіберпросторі;

2) соціально-економічні мотиви, пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі;

3) антидержавно-політичні мотиви, пов’язані з державно-політичною сферою відносин суб’єктів у кіберпросторі;

4) ідейні мотиви, пов’язані зі світоглядною сферою життя суб’єктів відносин у кіберпросторі.

Тож, на підставі класифікації мотивів можна класифікувати злочини, вчинені у кіберпросторі, на відповідні чотири групи:

1) злочини, вчинені з корисливих мотивів, що пов’язані з фінансово-економічною сферою відносин у кіберпросторі;

2) злочини, вчинені з соціально-економічних мотивів, що пов’язані з соціальною сферою відносин суб’єктів у кіберпросторі;

3) злочини, вчинені з антидержавно-політичних мотивів, пов’язані з державно-політичною сферою відносин суб’єктів у кіберпросторі;

4) злочини, вчинені з ідейних мотивів, пов’язані зі світоглядною сферою життя суб’єктів відносин у кіберпросторі.

Звичайно ці групи злочинів характеризуються різноманітністю їх кримінально-правових ознак, тому виникає питання поділу на підгрупи в межах виділених груп злочинів, які традиційно утворюють визначену множину злочинів в одному акті розслідування. В цьому сенсі важливим є беззаперечне визнання в юридичній літературі наявності у суб’єкта вчинення злочину, крім основного мотиву, також й додаткових мотивів. З криміналістичної точки зору ці мотиви мають системоутворююче значення в технологіях вчинення злочинів, забезпечуючи досягення кінцевої злочинної мети, відповідно зумовлюють суб’єктний склад організованої групи, відповідний комплекс злочинів, обрання певного предмету посягання. Організовані злочинні групи вчиняють не окремі злочини, а їх комплекси, розробляючи цілі технології злочинної діяльності, які забезпечують їм систематичне одержання кримінального доходу.

Контрольні запитання для перевірки досягнення результатів навчання

1. Які особливості кіберпростору, що привертають увагу злочинців до використання його середовища з метою досягнення злочинного результату?

2. Порівняйте зміст понять «комп’ютерний злочин», «кіберзлочин», «злочини у сфері високих технологій» та «злочини у сфері комп’ютерної інформації». Теоретичні та нормативні позиції вказаних термінів в Україні та за кордоном.

3. Визначення сутності кіберзлочинів. Класифікація кіберзлочинів (комплекс злочинів).

4. Класифікація кіберзлочинів в Європейської конвенції по боротьбі з кіберзлочинністю.

Лекція № 1
(денна форма навчання)

Тема 2. Організаційні та правові основи діяльності осіб у мережі Інтернет в Україні та за її межами

Мета вивчення

Надати уявлення та сформувати систему знань щодо особливостей реалізації та застосування норм матеріального і процесуального права стосовно відносин у традиційних сферах суспільного життя суб'єктів кіберпростору,

Результати навчання

Після лекції здобувач вищої освіти буде (спроможний):

1) визначати належні та прийнятні для юридичного аналізу факти щодо сфери боротьби з кіберзлочинами;

2) застосувати сучасні інформаційні технології та інформаційні ресурси за для розв'язання практичних задач з аналізу правової бази діяльності суб'єктів у кіберпросторі;

3) використовувати в правозастосовній діяльності нормативно-правові акти, що регулюють відносини, що виникають підчас виявлення та розслідування фактів вчинення злочинів у кіберпросторі;

4) розвивати здатність до критичного та системного аналізу правових явищ у кіберпросторі і застосування набутих знань у професійній діяльності юриста;

5) розуміти міжнародні стандарти прав людини як користувача кіберпростору, перспективи розвитку кіберпростору.

План

1. Міжнародні організації, що здійснюють регулювання Інтернет та особливості їх діяльності.
2. Особливості організації національного сегменту кіберпростору, ключові суб'єкти ринку телекомунікаційних послуг в Україні.
3. Основи правового регулювання відносин в кіберпросторі.
4. Кримінально-правова охорона суспільних відносин у кіберпросторі в України. Конвенція Ради Європи про кіберзлочинність.
5. Характеристика інших міжнародних правових актів, які є частиною національного законодавства України, що регулюють правила та принципи охорони суб'єктів відносин у кіберпросторі.

Основний зміст

1. Міжнародні організації, що здійснюють регулювання Інтернет та особливості їх діяльності.

Управління глобальною мережею Інтернет не здійснюється одноосібно певною організацією чи державою.

Ключовими регуляторами мережі Інтернет в світі виступують наступні організації. *Міжнародний союз електрозв'язку (*МСЕ) (англ. International Telecommunication Union, ITU) міжнародна організація, що визначає стандарти (точніше, за термінологією МСЕ – Рекомендації, англ. Recommendations) в галузі телекомунікацій та радіо. *Internet Society (ISOC)* – Інтернет організація (рос. Общество Інтернета) – недержавна громадська організація, фінансовою підосновою діяльності якої є внески учасників і пожертви спонсорів. Ця організація виступає основою для багатьох консультаційних та дослідницьких груп, які займаються розвитком Інтернета та по-суті утворюють технічні комітети, що розробляють та підтримують системи стандартів, на яких базується вся мережа, зокрема: Internet Activities Board (IAB) – Рада з архітектури Інтернету, яка по-суті здійснює нагляд за протоколами та пов'язаними з цим процесом процедурами; Internet Engineering Task Force (IETF) – Комісія з технологій Інтернет розробляє протоколи ехнічні специфікації та стандарти, що застосовуються у Інтернет «Request for Comments», комітет має первинное право публікації стандіртів; WWW консорціум (World Wide Web Consortium) розробляє стандарти WWW (World Wide Web), через які здійснюється обмін між комп'ютерами завдяки протоколу HTTP (Hypertext Transfer Protocol). Інтернет-корпорація по розподілу адрес та номерів (ICANN (Internet Corporation of Assigned Names and Numbers) також виграє важливу роль в організації діяльності мережі Інтернет. До її завдань належать координація систем унікальних ідентифікаторів мережі, присвоєння доменних імен (DNS, Domain Name System – Доменна система імен) що являє собою ієрархічну розподілену систему перетворення імені хоста (комп'ютера або іншого мережевого пристрою) в IP-адресу). Проте зазвичай інтернет-користувачі реєструють нові імена сайтів через регіональних інтернет-реєстраторів або через провайдерів.

Провайдери (ISP – Internet Service provider) – це організації, які надають доступ до мережі Інтернет (як безкоштовно, так і на платній основі). Постачальник послуг хостингу – особа, яка надає власникам веб-сайтів послуги і (або) ресурси для розміщення веб-сайтів або їх частин у мережі Інтернет та із забезпечення доступу до них через мережу Інтернет. Власник веб-сайта, який розміщує свій веб-сайт або його частину в мережі Інтернет на власних ресурсах і (або) самостійно забезпечує доступ до нього з використанням мережі Інтернет, одночасно є постачальником послуг хостингу. Користувачі широко використовують послуги міжнародних провайдерів, таких, наприклад, як Google, Yahoo та ін.

Інформація, доступна в мережі Інтернет, у тому числі й та, що на веб-сайтах, фізично розміщена на комп'ютерному обладнанні, об'єднаному каналами зв'язку з цією мережею, та має свій ідентифікатор – IP-адресу. Унікальність IP-адрес забезпечується централізованим розподілом діапазонів адрес Адміністрацією адресного простору Інтернет (Internet Assigned Numbers Authority – IANA) між *регіональними інтернет-реєстраторам* (Regional Internet Registries – RIR). Слід наголосити, що будь-який пристрій, підключений до мережі, також має свою унікальну апаратну адресу – Адресу управління доступом до середовища (Media Access Control address, MAC-address) тобто – MAC-адресу. MAC-адреса . Веб-сайти мають свої власні веб-адреси алфавітно-цифрового позначення – Єдиний покажчик ресурсу (Uniform Resource Locator, URL), що є зручним для запам'ятовування користувачами, наприклад, http://www.naiau.kiev.ua (сайт Національної академії внутрішніх справ). Переведення алфавітно-цифрових назв сайтів та електронних адрес (включно написаних кирилицею) до IP-адрес здійснюється за допомогою системи DNS – Domain Name System.

2. Особливості організації національного сегменту кіберпростору, ключові суб'єкти ринку телекомунікаційних послуг в Україні

Особливості організації національного сегменту кіберпростору.

По-перше, в огляду на географічне розташування України, її телекомунікаційні мережі є точками транзиту трафіка щодо передачі даних Європи, Росії та Азії. Саме тому самостійну роль на ринку телекомунікаційних послуг в Україні виконують організації, що надають послуги з обміну трафіком (зазвичай використовують термін «піринг» (від англ. peering – сусідство) – угода про обмін трафіком).

По-друге, у технічному аспекті магістральна мережа Інтернет огортає всю планету, поєднуючи континенти, країни й окремі міста. *Великі оператори та провайдери* мають Інтернет-вузли й магістральні лінії в Україні та за її межами; *регіональні оператори та провайдери* охоплюють своєю мережею регіон, декілька або одну область (причому більшість з них не мають своєї магістральної мережі); *локальні оператори та провайдери* – один або кілька населених пунктів.

По-третє, суб'єкт господарювання традиційно отримує право на здійснення діяльності у сфері телекомунікацій після включення Національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації (далі – НКРЗІ), зі статусом «провайдер» або «оператор» до відповідного реєстру операторів, провайдерів телекомунікацій[1]. *Діяльність провайдера обмежується географічною територією дії конкретного оператора (фактичної діяльності як зареєстрованого суб'єкта або тієї, що передбачена ліцензією на обслуговування телекомунікацій).*

По-четверте, на ринку телекомунікаційних (інформаційних) послуг також

[1] Реєстр операторів, провайдерів телекомунікацій. URL: https://nkrzi.gov.ua/index.php?r=site/index&pg=55&language=uk.

присутні й володільці інформації в системах. Володілець інформації – це фізична або юридична особа, якій належать права на інформацію в інформаційній системі. У значенні інформації вона набуває форми інформаційного продукту або інформаційного ресурсу (сукупності продуктів, об'єднаних технологією зберігання або передачі даних). Таким ресурсом є веб-сайт та електронно-інформаційні системи різного призначення (платіжні системи, автоматизовані системи технологічного виробництва, інформаційно-пошукові, робочі автоматизовані місця тощо).

Особливості організації національного сегменту кіберпростору зумовлюють суб'єктів взаємодії зі слідчим в процесі розслідування злочинів, вчинених у кіберпросторія. Взаємодія слідчого із оперативними підрозділами, власниками (розпорядниками) телекомунікаційних систем, володільцями інформації в системах та іншими суб'єктами на ринку телекомунікаційних послуг є невід'ємною складовою процесу виявлення та розслідування злочинів, вчинених у кіберпросторі.

3. Основи правового регулювання відносин в кіберпросторі

Існування різних сфер життя суспільства у кібепросторі забезпечує людська діяльність, яка здійснюється з приводу того чи іншого матеріального або духовного об'єкта для задоволення соціальних потреб та інтересів. Таким чином виникають суспільні відносини (з приводу того чи іншого об'єкта) або соціальні відносини (як особливий вид суспільних, що відображають статус особи і соціальних груп у суспільстві). Основним засобом регулювання тих чи інших суспільних відносин у кіберпросторі постає відповідне право: інформаційні відносини підлягають регулюванню інформаційним правом; відносини з приводу інтелектуальної власності – інтелектуальним правом; майнові та особисті немайнові відносини – цивільним, господарським правом; відносини, що виникають унаслідок учинення злочину та відкриття відповідного кримінального провадження – кримінальним та кримінальним процесуальним правом.

Окремо акцетуємо увагу на електронному підпису – це дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації програмно цих даних; електронний цифровий підпис – це вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа; засіб електронного цифрового підпису – програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису; особистий ключ – параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу)

Господарське право також регулює відносини суб'єктів кіберпростору,

зокрема через положення Законів України: «Про державну реєстрацію юридичних осіб та фізичних осіб – підприємців» від 15 травня 2003 р. (щодо комерційного (фірмового) найменування та торговельної марки), «Про платіжні системи та переказ коштів в Україні», Закон України «Про електронні документи та електронний документообіг», «Про електронну комерцію», Останній не обмежує суб'єктыв у виборі правових форм ведення е-бізнесу, тому допустиме здійснення діяльності як у формі юридичної особи, так і без створення такої (фізична особа-підприємець). Універсальної рекомендації щодо оптимальної моделі роботи немає. Онлайн торгівля нічим не відрізняється від звичайної торгівлі, яку кожен звик бачити щоденно, «в реальному житті», а тому отримання дозвільних документів у випадках, передбачених законодавством – необхідність.

4. Кримінально-правова охорона суспільних відносин у кіберпросторі в України. Конвенція Ради Європи про кіберзлочинність

Сучасний стан правового регулювання боротьби зі злочинами, вчиненими у кіберпросторі, характеризується: відносною цілісністю системи актів у цьому напрямку на національнальному рівні; дезорганізованості системи нормативно-правових актів на міжнародному рівні регулювання. Центральне місце на національному рівні в механізмі правового регулювання боротьби з такими злочинами займають норми: Конвенції Ради Європи про кіберзлочинність від 23 листопаду 2001 року, Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15 листопада 2000 року, загальні та спеціальні норми КК України, які передбачають численні конвенційні та альтернативні Конвенціям склади кримінальних правопорушень, що вчиняються в обстановці кіберпростору. Складовими національної системи правового регулювання боротьби з такими злочинами виступають також норми галузевого законодавства, зокрема у сфері забезпечення національної, економічної та кібернетичної безпеки, захисту суспільства, дітей, інформації, авторських та суміжних прав. ***Конвенція Ради Європи про кіберзлочинність*** (прийнята європейськими державами в м. Будапешт 23 листопада 2001 року; Україна приєдналася із застереженнями шляхом ратифікації 7 вересня 2005 року; ратифікована 58 державами, серед яких усі держави-члени Ради Європи (за винятком Російської Федерації) й такі, що не входять до європейської спільноти, зокрема Канада, Ізраїль, США, Японія та країни південної Америки) – це договір, згідно з яким держави, що до неї приєдналися, узяли на себе зобов'язання відносно зближення між собою внутрішньодержавних положень кримінального права щодо кіберзлочинів та створення можливостей для застосування ефективних засобів розслідування таких правопорушень. Тому Конвенцією прямо передбачено заходи, що мають здійснюватися на національному рівні в матеріальному кримінальному праві (ч.1 розділ 2) й кримінально-процесуальному (так званому «процедурному») праві (ч. 2 розділ

2), а також систему міжнародного співробітництва (розділ 3) та питання юрисдикційного характеру (ч. 3 розділ 2)[2].

Проблеми боротьби з кібертероризмом у міжнародному законодавчому полі відображено лише у вигляді проектів актів або локальних, двосторонніх міжнародних договорів з питань процедурного права. Країни Європейського Союзу обговорюють міжрегіональний проект Clean IT, метою якого є організація оперативного реагування у разі виникнення загрози акту кібернетичного тероризму[3]. В Україні цю сферу боротьби з тероризмом зачіпають галузеві акти у сфері кібербезпеки та двосторонні договори, укладені з США, Республікою Словенія, Чорногорією, Королівством Бельгія, Королівством Нідерланди.

Однією із загроз національній безпеці є саме кібернетична загроза. У березні 2016 року Указом Президента України було введено в дію Рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України». 5 жовтня 2017 року Верховна Рада України прийняла Закон «Про основні засади забезпечення кібербезпеки України». Не дивлячись на те, що у ньому лише частково враховано висловлені раніше зауваження Комітету Верховної Ради України з питань інформатизації та зв'язку та Головного юридичного управління, цей закон став відправною точкою для протидії кібератакам, актам кібертероризму та іншим злочинним проявам у куіберпрострі.

Окрема частка правопорушень, визначених у Конвенції, набула закріплення в спеціальних нормах, які об'єднано в Розділі XVI «Злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Іншу ж кількість конвенційних правопорушень зафіксовано в статтях КК України, якими регламентовано використання для вчинення злочину електронно-обчислювальної техніки, мереж, систем, інших апаратних та програмних засобів. КК України також містить кримінальні правопорушення, що є *альтернативними правопорушенням, визнаним Конвенцією про кіберзлочинність*, тобто вчинювані у кіберпросторі, але в цьому міжнародному акті про них взагалі не йдеться.

5. Характеристика інших міжнародних правових актів, які є частиною національного законодавства України, що регулюють правила та принципи охорони суб'єктів відносин у кіберпросторі.

Процес імплементації положень Конвенції у кримінальне законодавство України супроводжується приєднанням України до інших багатосторонніх міжнародних угод в цій сфері. Україною визнано обов'язковість норм не лише Конвенції про кіберзлочинність, а й інших багатосторонніх міжнародних угод, що стосуються питання боротьби зі злочинами, вчиненими у кіберпросторі.

Стандарти окремих з таких договорів безпосередньо визнані Конвенцією про кіберзлочинність. Зокрема, в тексті Конвенції міститься посилання на ряд

[2] Конвенція про кіберзлочинність : міжнар. док. від 23 лисопт. 2001 р. URL: http://zakon3.rada.gov.ua/laws/show/994_575?nreg=994_575&find= 1&text=%F7%E0%F1&x=0&v=4#w11.

[3] Clean IT – Leak shows plans for large-scale, undemocratic surveillance of all communications. 2012. 21 sep. URL: https://edri.org/cleanit.

міжнародних актів, ратифікованих Україною. 12 грудня 2003 року на п’ятому пленарному засіданні Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства, що відбувалася в Женеві (Швейцарія), на підставі рішення Ради Міжнародного союзу електрозв’язку (МСЕ) і резолюцій 56/183 і 57/238 Генеральної Асамблеї ООН, вповноваженими від 103 держав, включно й України, одноголосно було прийнято Декларацію принципів., в якій піднято багато питань не конвенційних злочинів.

Контрольні запитання для перевірки досягнення результатів навчання

1. Які основні галузі права регулюють відносини суб’єктів у кіберпросторі в Україні?
2. Охарактеризуйте особливості організації національноо сегменту кіберпростору.
3. Які Ви знаєте міжнародні організації, що здійснюють регулювання Інтернет?
4. Джерела національного законодавства України в сфері кримінально-правової охорони суспільних відносин у кіберпросторі України?
5. Що таке IP-адреса та MAC-адреса? Чим виступають ці відомості підчас розслідування злочинів?
6. Які види кіберзлочинів визначені за Конвенцією Ради Європи «Про кіберзлочинність» від 23 листопада 2001 року?
7. Охарактеризуйте процес та ступінь імплементації норм Конвенції в національне кримінальне законодавство.
8. Охарактеризуйте механізм правового регулювання боротьби з кіберзлочинами.

Лекція № 2
(денна форма навчання)

Тема 3. Організаційні засади виявлення та початку кримінального провадження щодо кіберзлочинів

Мета вивчення

Надати уявлення та сформувати систему знань щодо організаційних засад виявлення кіберзлочинів та відкриття кримінального провадження щодо такої категорії злочинів.

Результати навчання

Після лекції здобувач вищої освіти буде (спроможний):

1) визначати належні та прийнятні для юридичного аналізу факти щодо сфери боротьби з кіберзлочинами;

2) застосувати сучасні інформаційні технології та інформаційні ресурси за для розв'язання практичних задач щодо організації виявлення кіберзлочинів та початку кримінального провадження;

3) використовувати в правозастосовній діяльності нормативно-правові акти, що регулюють відносини, що виникають підчас оперативно-розшукової діяльності щодо фактів вчинення злочинів у кіберпросторі, а також підчас відкриття кримінального провадження за такими фактами;

4) розвивати здатність до критичного та системного аналізу правових явищ у кіберпросторі і застосування набутих знань у професійній діяльності юриста;

5) аналізувати правові та правозастосовчі проблеми, формувати та обґрунтовувати власну право застосовну позицію в межах питань виявлення та розслідування кіберзлочинів.

План

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

Основний зміст

1. Виявлення кіберзлочинів як напрямок правоохоронної діяльності. Джерела інформації про кіберзлочин.

Виявлення як вид діяльності передує розслідуванню (згідно ЗУ «Про оперативно-розшукову діяльність» (ст.7 ч.3)). Основні засоби та пошукові процедури, які застосовують у процесі виявлення кіберзлочинів, вивчають у курсі оперативно-розшукової діяльності. Сьогодні можна визначити наступних *суб'єктів оперативно-розшукової діяльності, котрі прямо або опосередковано здійснюють виявлення кіберзлочинів.*

1. Національна поліція України (НП), відповідно до § 3 Стратегії кібербезпеки України, належить до Національної системи кібербезпеки як орган, що забезпечує захист прав і свобод людини та громадянина, інтересів суспільства й держави від злочинних посягань у кіберпросторі та здійснює заходи із запобігання, виявлення, припинення та розкриття таких злочинів. Як суб'єктів виявлення кіберзлочинів можна структурні підрозділи НП можна поділити на дві групи.

1.1. Підрозділи Департаменту кіберполіції (ДКП), які згідно з п. 2.1. Положення про ДКП НП України, уповноважені щодо протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Ця сфера діяльності іменується в Положенні «протидія кіберзлочинності». В Україні правові основи боротьби з кіберзлочинами визначаються передусім Конвенцією Ради Європи про кіберзлочинність. Тому оперативні підрозділи ДКП прямо зобов'язані здійснювати оперативно-розшукову діяльність властивими їм методами з метою протидії конвенційним злочинам (відповідальність за які фактично передбачена ст. 163, 176, 185, 190, 200, 301, 361–363-1 КК України).

ДКП є міжрегіональним територіальним органом , юридичною особою публічного права. До складу Департаменту входять структурні підрозділи, які діють за міжрегіональним принципом та безпосередньо підпорядковані начальникові Департаменту (Донецьке, Карпатське, Київське, Подільське, Поліське, Придніпровське, Причорноморське та Слобожанське управління кіберполіції, а також управління інформаційних технологій та програмування в західному, південному та східному регіонах).

1.2. Інші оперативні підрозділи НП (Департамент карного розшуку, або Департаменту захисту економіки[*], або Департаменту протидії наркозлочинності тощо), що здійснюють протидію іншим, альтернативним

[*] Згідно Постанові Кабінету Міністрів України від 2 вересня 2019 р. № 841 «Про ліквідацію територіального органу Національної поліції» Департамент зхисту економіки ліквідовано як міжрегіональний територіальний орган Національної поліції; в стадії розробки нормативна база для створення іншого органу – Служби фінансових розслідувань.

Конвенції, злочинам, що вчиняються у кіберпросторі та підслідні слідчим НП України. ДКП стосовно таких злочинів можуть тільки сприяти в порядку, передбаченому чинним законодавством, іншим підрозділам НП України у попередженні, виявленні та припиненні кримінальних правопорушень – забезпечує своєчасне отримання інформації про злочини, що вчинені в кіберпросторі, або відповідні злочинні наміри..

2. Підрозділи контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, захисту національної державності Служби безпеки (ДКІБ СБ України). До завдань СБ України також входить попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, тероризму, корупції та організованої злочинної діяльності у сфері управління і економіки та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України.

Типовими джерелами оперативної інформації про кіберзлочини є: 1) електронні та письмові повідомлення про злочин; 2) запитах і повідомленнях правоохоронних органів інших держав, міжнародних правоохоронних організацій (в результаті перевірки цієї інформації співробітниками ДКП складається рапорт (ст.6 Закону України «Про оперативно-розшукову діяльність»); 3) матеріали, складені в результаті перевірки заяв і повідомлень громадян, з якими встановлено негласне співробітництво (в результаті перевірки цієї інформації співробітниками ДКП складається рапорт (ст.6 Закону України «Про оперативно-розшукову діяльність»); 4) письмові доручення, постанови слідчого; 5) матеріали інших правоохоронних органів; 6) інші відомості, отримані унаслідок оперативно-розшукової діяльності (в результаті оперативного пошуку). Слідчі НП України, СБ України підчас здійснення досудового розслідування в уже дорученому для здійснення розслідування кримінальному провадженні також можуть виявити кіберзлочин.

2. Організаційні форми початку кримінального провадження щодо кіберзлочинів та джерела обставин, що можуть свідчити про вчинення певного виду кіберзлочинів

З позицій слідчої практики процесуальний порядок початку кримінального провадження триває з моменту, коли суб'єкту розслідування стало відомо про джерело обставин, що можуть свідчити про кримінальне правопорушення, до моменту внесення ним інформації до ЄРДР. Внутрішня організація слідчим початку кримінального провадження залежатиме від двох чинників: правового та неправового (організаційного) характеру. Правові чинники, що зумовлюють форми початку кримінального провадження, пов'язані з характером джерела обставин, що можуть свідчити про вчинення певного виду кримінального правопорушення. Особливості використання функціоналу оперативно-розшукової діяльності з метою виявлення кримінального правопорушення є *організаційними чинниками, що зумовлюють особливості форми початку кримінального провадження щодо окремого виду злочинів*.

Існують чотири організаційні форми початку кримінального провадження: 1) кримінальне провадження розпочато за заявою потерпілого/повідомлення особи про кримінальне правопорушення (безальтернативна форма); 2) кримінальне провадження розпочато за матеріалами оперативних підрозділів, отриманими в результаті перевірки оперативної інформації (альтернативна форма) – визнано складність реалізації матеріалів перевірки щодо нетяжких і середньої тяжкості злочинів, чим і пояснюється формалізованість застосування безальтернативної форми початку провадження; 3) кримінальне провадження розпочато в межах реалізації матеріалів ОРС (безініціативна форма) – констатовано її поширеність щодо злочинів, вчинених у кіберпросторі з політичних мотивів (90%), злочинів, що порушують встановлений порядок обігу певних речей (40%); 4) кримінальне провадження розпочато унаслідок виявлення слідчим злочину, вчиненого у кіберпросторі, під час розслідування іншого кримінального провадження (ініціативна форма) – визнано її нетиповість, слідчий виявляє такі злочини, як правило, випадково.

3. Особливості перевірки інформації про кіберзлочини, що вчинені або готуються

Фактичні дані, отримані під час ОРД, повинні мати значення доказу в кримінальному провадженні. Для того, щоб інформація про вчинення або готування кіберзлочину мала перспективу досудового слідства, вона повинна бути підтверджена достовірними для слідчого джерелами, які закономірно пов’язані з документальністю факту її перевірки оперативним підрозділом. Для цього варто характеризувати про два напрями роботи оперативних підрозділів, а саме: 1) оформлення отриманої інформації у вигляді матеріалів первинної перевірки, що підлягають передачі керівнику органу досудового розслідування для внесення до ЄРДР; 2) документування злочинної діяльності (в рамках оперативно-розшукової справи).

Матеріали первинної перевірки, які підлягають передачі керівникові органу досудового розслідування для внесення до ЄРДР, типово можуть містити: рапорт працівника оперативного підрозділу про виявлення ознак злочину; можливі офіційні матеріали ревізій, документальних і інших технічних перевірок (ініційованих особою, що повідомила про злочин); матеріали опитування очевидців, свідків, потерпілого тощо (можливі пояснення службових осіб, фахівців банків, підприємств, установ); матеріали перевірки за оперативними, криміналістичними й іншими обліками (в тому числі система Інтерполу I-24/7, захищений канал зв’язку Європолу «SIENA»); протокол огляду місця події, в тому числі як додаткі паперові роздруки інформації з вилучених машинних носіїв інформації і інформації, що знаходилася на жорсткому диску переносного комп’ютера підозрюваного; офіційні матеріали різних суб’єктів ринку телекомунікаційних послуг (див. Тема 2), наприклад від операторів і провайдерів телекомунікаційних послуг про зв’язок, абонента, надання телекомунікаційних послуг, отримання послуг, їх тривалість, зміст, маршрути передавання тощо; інструкції, довідки, інші технічні документи і

матеріали. Недоцільно персоналізувати в матеріалах перевірки інформацію про користувача (можливого злочинця) з гласного джерела. Адже децентралізовані технології обміну й зберігання інформації, технології анонімізації доступу до ресурсів мережі Інтернет (проксі-сервісів (комплекси програм), віртуальних приватних мереж (VPN-технологій) інших засобів-анонімайзерів) ускладнюють можливість підтвердження персональних даних користувача-злочинця – володільці інформаційних систем та інформації часто фізично перебувають за межами держави або ж нададуть таку інформацію лише на підставі ухвали слідчого судді.

Щодо документування злочинної діяльності (в рамках оперативно-розшукової справи, то існує певна проблема – неузгодженість абз. 1, 2 п. 1 ч. 1 ст. 6 Закону України «Про оперативно-розшукову діяльність» з ч. 1 ст. 214 КПК України. З одного боку, підставою проведення оперативно-розшукової діяльності є наявність достатньої інформації про злочини, що готуються, або осіб, які готують його вчинення, а з іншого – ознака караності характеризує готування як самостійний вид злочину (готування до злочину або замах відповідно до ст. 13 КК України). Тому слідчий буде зобов'язаний внести інформацію щодо готування злочину до ЄРДР. За таких обставин за ОРС не можна здійснювати оперативно-розшукову діяльність. Мета документування полягає в отриманні фактичних даних про спробу окремої особи/групи осіб вчинити конкретні дії, що дають змогу дійти висновку про наявність/відсутність ознак складу конкретного тяжкого злочину.

4. Особливості відкриття кримінального провадження за заявою та повідомленням особи про кіберзлочин. Організаційні заходи слідчого для перевірки отриманої первинної інформації

Узагальнення відкритих публікацій, дозволяє визначити такі початкові умови (обставини) виявлення кіберзлочинів заявником (як користувачем): 1) самостійно запідозрив вчинення незаконних дій у кіберпросторі та одразу звернувся до відповідного оперативного підрозділу кібеполіції, слідчого або прокурора, також сам діагностував сліди (зміни у файловій системі, в заданій раніше конфігурації комп'ютера, нестандартні прояви в його роботі тощо в залежності від ситуації); 2) у результаті проведення перевірочних заходів співробітниками служби безпеки або фахівцями із захисту інформації, що знаходяться в штаті користувача або провайдера (наприклад, при перевірки службою безпеки банка вивлються сліди вчинення кіберзлочину). *Встановлення належності сайту*. За допомогою сервісу Whois визначається провайдер, який надає послугу хостингу. Далі для встановлення належності сайта звертаються до провайдера із запитом про: реєстраційні дані (logs) та абонентську інформацію про особу, якій надаються послуги хостингу для сайта; адреси, телефонні номери та інші реквізити власника сайта; IP-адреси, використані для створення сайта; IP-адреси, використані для поповнення сайта; інформація про зміст сайта; інформація про користування сайтом. *Встановлення належності електронної поштової адреси*. Для встановлення особи, яка користується відомою адресою, необхідно за допомогою сервісу

Whois визначити провайдера, який надає послуги використання електронної пошти, і звернутися до нього із запитом (чітки позиції запиту.

Для ідентифікації особи правопорушника необхідно встановити: коло осіб, які користуються певним терміналом, а також мету та межі їх користування; технічну підготовку та навички користування певними програмними та технічними засобами; осіб, які користувалися терміналом під час вчинення протиправних дій; хто має доступ до мережі Інтернет, які при цьому використовуються логіни та паролі, через якого провайдера; з яких ще IP-адрес використовувались дані реквізити при доступі до мережі тощо. Отримання інформації у відкритих джерелах мережі Інтернет. До відкритих джерел відносяться: соціальні мережі, телефонні довідники, мобільні додатки, державні реєстри, сервіси які потребують реєстрації та на яких потрібно вказувати достовірні персональні дані.

Контрольні запитання для перевірки досягнення результатів навчання

1. Назвіть суб’єктів оперативно-розшукової діяльності, котрі прямо або опосередковано здійснюють виявлення кіберзлочинів?
2. Назвіть типові джерела оперативної інформації про кіберзлочини?
3. Окреслить чинники, що зумовлюють форми початку кримінального провадження.
4. Охарактеризуйте організаційні форми початку кримінального провадження щодо кіберзлочинів?
5. Який типовий перелік матеріалів перевірки, що є джерелом обставин про кримінальне правопорушення, вчинене із використанням кіберпростору?
6. Охарактеризуйте процес виявлення кіберзлочинів заявником (як користувачем).
7. Як здійснюється встановлення належності сайту?

Лекція № 3
(денна форма навчання)

Тема 4. Використання спеціальних знань під час розслідування кіберзлочинів

Мета вивчення

Надати уявлення та сформувати систему знань щодо організаційних засад виявлення та розслідування кіберзлочинів.

Результати навчання

Після лекції здобувач вищої освіти буде (спроможний):

1) визначати належні та прийнятні для юридичного аналізу факти щодо сфери боротьби з кіберзлочинами;

2) застосувати сучасні інформаційні технології та інформаційні ресурси за для розв'язання практичних задач щодо організації розслідування кіберзлочинів;

3) використовувати в правозастосовній діяльності нормативно-правові акти, що регулюють відносини, що виникають підчас використання спеціальних знань та призначення судових експертиз в процесі розслудвання злочинів у кіберпросторі, а також підчас збирання матеріалів попередньої перевірки за такими фактами;

4) розвивати здатність до критичного та системного аналізу правових явищ у кіберпросторі і застосування набутих знань у професійній діяльності юриста;

5) аналізувати правові та правозастосовчі проблеми, формувати та обґрунтовувати власну право застосовну позицію в межах питань залучення спеціаліста та експерат в процес розслідування кіберзлочинів.

План

1. Спеціальні знання та специфіка залучення спеціаліста під час розслідування кіберзлочинів.
2. Залучення експерта для проведення судової комп'ютерно-технічної експертизи під час розслідування кіберзлочинів.
3. Залучення експерта для проведення інших судових експертиз підчас розслідування кіберзлочинів: експертиза у сфері інтелектуальної власності; експертиза телекомунікаційних систем (обладнання) та засобів; комплексні експертизи (КТЕ та експертизи відео звукозапису; КТЕ і ТЕД).

Основний зміст

1. Спеціальні знання та специфіка залучення спеціаліста під час розслідування кіберзлочинів

Поняття «спеціальні знання» тлумачать як наукові, технічні або інші з позицій кримінального процесуального закону неюридичні знання, отримані внаслідок спеціальної підготовки та практики суб'єктом, процесуальний статус якого визначається як експерт або прирівнюється до спеціаліста. Говоримо про три процесуальні форми використання спеціальних знань під час досудового розслідування: 1) залучення спеціаліста для надання письмової консультації; 2) залучення спеціаліста для надання безпосередньої технічної допомоги під час процесуальних дій; 3) залучення експерта для проведення судової експертизи й виконання обов'язків судового експерта. Високим рівнем апробованості слідчою практикою доведена ефективність таких непроцесуальних форм використання спеціальних знань, як: 1) усне консультування слідчого зі спеціалістом; 2) залучення спеціаліста під час перевірки оперативної інформації про злочини, що вчинені або готуються. Повсякденна практика розслідування злочинів, вчинених у кіберпросторі, засвідчує наявність безлічі організаційних і тактичних питань використання таких форм спеціальних знань. У справах щодо кіберзлочинів письмові пояснення спеціаліста є додатковим способом підтвердження джерела формування такого доказу, як документ – електронний носій інформації. В абсолютній більшості проваджень пояснення надають штатні працівники кіберполіції, які є фахівцями з інформаційних технологій або електроніки й телекомунікацій, і в процесуальному статусі спеціаліста були залучені під час проведення огляду місця події. У письмовому поясненні такий спеціаліст описує методи так званого експрес-аналізу (процес встановлення фактичних даних, що мають значення для конкретного факту правопорушення); методи вилучення (копіювання) та збереження нетрадиційних (цифрових) слідів злочину. Специфіка основного злочину в злочинній сукупності зрідка є підставою для залучення спеціалістів вужчого профілю, зокрема: спеціаліста в роботі з банківським комп'ютерним обладнанням, системного адміністратора, системного оператора; спеціаліста у сфері мережевих технологій та систем зв'язку (за умови використання для дистанційного передання даних каналів електрозв'язку); іншої категорії спеціалістів (бухгалтер, економіст, інженер-електрик, спеціаліст супутникових систем зв'язку, оператор стільникових, пейджингових, інтернет-мереж тощо). *З метою техніко-криміналістичного забезпечення проведення* слідчих оглядів, оглядів місця події, обшуків і тимчасових доступів до речей та документів переважно залучають інспекторів-криміналістів, старших інспекторів-криміналістів, техніків-криміналістів або керівника сектору техніко-криміналістичного забезпечення слідчого відділу. *Залучення спеціаліста під час НС(Р)Д* є правом слідчого, прокурора, а не їхнім обов'язком. Тому з дотриманням режиму секретності (спеціаліст повинен мати

допуск до державної таємниці відповідної форми) під час проведення НС(Р)Д та відповідно до специфіки питань її проведення, складності та її змісту, що потребують залучення спеціальних знань, слідчий і прокурор самостійно приймають рішення про можливість залучення до НС(Р)Д спеціаліста відповідного фаху та кваліфікації.

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

Сутність експертизи полягає в тому, що експерт самостійно на підставі спеціальних знань у галузі науки, техніки, мистецтва, ремесла тощо досліджує надані йому об'єкти, явища й процеси з метою надання висновку з питань, що є або будуть предметом судового розгляду.

Унаслідок вчинення кіберзлочинів утворюються як традиційні в криміналістичному сенсі, так і нетрадиційні або «цифрові» сліди, що потребує проведення в таких справах широкого спектру судових експертиз, а саме: експертизи комп'ютерної техніки і програмних продуктів; експертизи телекомунікаційних систем (обладнання) та засобів; технічної експертизи документів; експертизи відеозвукозапису; експертизи у сфері інтелектуальної власності; інших видів експертиз, без проведення яких неможливо отримати необхідні відомості, що свідчать про ознаки складу одного зі злочинів злочинної сукупності (наприклад, економічних експертиз під час розслідування злочинів, пов'язаних із фінансово-економічною сферою відносин у кіберпросторі; психологічної, мистецтвознавчої експертизи або відповідної комплексної експертизи – злочинів, пов'язаних із соціальною сферою відносин суб'єктів у кіберпросторі; трасологічних експертиз – злочинів, що вчинені з антидержавно-політичних або корисливих мотивів, лінгвістичної експертизи мовлення (семантико-текстуальний аналіз писемного й усного мовлення) – злочинів, що вчинені з антидержавно-політичних мотивів; судово-балістичних, судово-хімічних експертиз тощо – злочинів, що порушують встановлений порядок обігу певних речей).

Під час розслідування всіх класифікаційних груп і підгруп злочинів, вчинених у кіберпросторі, типово призначається ***експертиза комп'ютерної техніки і програмних продуктів.*** В практиці для позначення цієї експертизи використовують термін «комп'ютерно-технічна експертиза» (КТЕ). Залежно від завдання, специфіки дослідження та видів об'єктів, які досліджують, у теорії виокремлюють різні її види, а саме: апаратно-комп'ютерну експертизу, програмно-комп'ютерну експертизу; експертизу даних (інформаційно-комп'ютерну); комп'ютерно-мережеву експертизу; комплекс цих експертиз. Об'єктами судової експертизи є комп'ютери з носіями інформації (будь-які накопичувачі інформації – дискети, жорсткі диски, CD-диски, флеш-карти тощо), програмні продукти й інша комп'ютерна техніка (наприклад, мобільні телефони, банкомати, гральні автомати, карт-ридери, електронні записні книжки, пейджери, принтери тощо), а також документація до обладнання. Базовим документом з питань визначення орієнтовного переліку питань для

проведення КТЕ є Інструкція про призначення та проведення судових експертиз та експертних досліджень та Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень (п. 13 розділу ІІ Рекомендацій). Важливого значення мають вимоги щодо формулювання питань на експетизу. З метою оптимізації процесу проведення КТЕ пропонуються алгоритми заходів.

3. Залучення експерта для проведення інших судових експертиз підчас розслідування кіберзлочинів

Комплексна КТЕ і ТЕД – це дослідження, що проводять для вирішення спільних (інтеграційних) питань стосовно документів, виготовлених за допомогою комп'ютерної техніки. У сучасних умовах злочинці мають доступ до різноманітних принтерів, витратних матеріалів та багатофункціонального поліграфічного обладнання, які через порівняно невисоку ціну та можливість анонімного придбання (стосовно поліграфічного обладнання для підроблення банківських карт) надають можливість виготовити високої якості підроблені документи як знаряддя для вчинення злочинів надалі. Документи на пластиковій основі науковці класифікують за різними критеріями та розглядають стосовно них ознаки підробки. Комплексну КТЕ і ТЕД проводять для: встановлення типу й ідентифікації комп'ютерної та копіювально-розмножувальної техніки за виготовленими за їх допомогою матеріальними документами; пошуку даних з наданого на експертизу документа (фактів і способів створення та внесення змін до документів, виявлення їх первинного змісту); ідентифікації знайденої комп'ютерної інформації з даними на паперовому носієві. Систематизовані обов'язкові вимоги до об'єктів, що надають таку експерту.

Комплекс КТЕ й експертизи відеозвукозапису є також типовим під час розслідування злочинів, вчинених у кіберпросторі, адже злочинці активно використовують мультимедійні технології, що ґрунтуються на представлених даних у цифровому форматі відеозображення із застосуванням анімації та звукового супроводу. У цій експертизі спільні (інтеграційні) питання пов'язані зі встановленням їх оригінальності та незмінності (відсутністю монтажу) запису за допомогою комп'ютерної техніки. Основним об'єктом дослідження є файли зі звуковими, відеоформатами. Їх носіями, що відправляють на дослідження, переважно є мобільні телефони, смартфони. Ця техніка становить різновид терміналу стільникового зв'язку, SIM-карти до неї є необхідним компонентом для функціонування такого терміналу як телекомунікаційного засобу. Тому дослідження їх є завданням експертизи телекомунікаційних систем (обладнання) та засобів. Проте, виконуючи функції цифрового органайзера або персонального комп'ютера (спеціалізованого комп'ютера з відповідним програмним забезпеченням для роботи з електронною поштою, перегляду текстових або мультимедійних файлів тощо), ця техніка одночасно є об'єктом КТЕ. Мобільні телефони оснащені слотом для карти пам'яті, та/або їх можна підключити до комп'ютера як звичайний зовнішній накопичувач інформації з файловою системою.

Експертизу телекомунікаційних систем (обладнання) та засобів фактично проводили лише в 10 % проваджень щодо кіберзлочинів. Проте такий показник міг бути значно вищим, основні причини цього – висока вартість такої експертизи, потреба в постійному оновленні матеріально-технічного забезпечення експертних служб для її проведення та нестача відповідних експертних кадрів у системі Експертної служби МВС України. Експертиза телекомунікаційних систем (обладнання) та засобів – це дослідження телекомунікаційних систем і засобів, мереж, їхніх складових та інформації, яку вони передають, приймають та обробляють, з метою встановлення технічних параметрів і стану об'єкта, визначення їх функціонального призначення. Цей вид досліджень потребує окремих знань, пов'язаних із розумінням інформаційних процесів у комп'ютерних мережах, мережах зв'язку, спеціалізованих телекомунікаційних пристроях, чим і зумовлене виокремлення відповідної експертної спеціальності. Під час розслідування кіберзлочинів, об'єктами цієї експертизи часто є: Інтернет IP вузли, веб-сторінки, приймачі радіосигналів, вузли комутації; первинні мережі зв'язку, наземні станції супутникового зв'язку, обставини (адресації в мережі Інтернет; передачі радіосигналів; використання доменних імен у мережі Інтернет тощо). Таку експертизу призначають здебільшого під час розслідування злочинів, вчинених у кіберпросторі, за умови, якщо способом вчинення (приховування або підготовки) злочину є: втручання в роботу мереж операторів зв'язку, заміна, спотворення, витікання, втрата трафіку і спотворення процесу його обробки; порушення встановленого порядку маршрутизації трафіку.

Експертиза у сфері інтелектуальної власності. Сучасне науково-методичне забезпечення проведення таких експертиз стосується різних за походженням об'єктів інтелектуальної творчості[4]. У межах розслідування злочинів, вчинених у кіберпросторі, традиційно здійснюють два види таких досліджень: дослідження, пов'язані з комп'ютерними програмами й компіляціями даних (базами даних), та/або дослідження, пов'язані з виконанням, фонограмами, відеограмами, програмами (передачами) організацій мовлення. Експерти використовують і відповідні методики та методичні рекомендації щодо: проведення судових експертиз оптичних носіїв, які містять об'єкти авторського права й суміжних прав; дослідження ознак контрафактності лазерних компакт-дисків, аудіо- і відеокасет; проведення судово-експертних досліджень веб-сайту як об'єкта інтелектуальної власності. Експертиза у сфері інтелектуальної власності є обов'язковою під час розслідування інтелектуального піратства.

[4] Реєстр методик проведення судових експертиз. *Міністерство юстиції України :* [сайт]. URL: http://rmpse.minjust.gov.ua/search.

Контрольні запитання для перевірки досягнення результатів навчання

1. Назвіть організаційні і тактичні особливості залучення спеціаліста для надання письмової та усної консультації підчас розслідування кіберзлочинів.
2. Назвіть організаційні і тактичні особливості залучення спеціаліста для надання безпосередньої технічної допомоги.
3. Назвіть організаційні і тактичні особливості залучення спеціаліста з метою техніко-криміналістичного забезпечення слідчих (розшукових) та негласних слідчих (розшукових) дій.
4. Які вимоги до питань на комп'ютерно-технічну експертизу (КТЕ)?
5. Охарактеризуйте та назвіть особливості залучення підчас розслідування кіберзлочинів експерта для проведення експертиза телекомунікаційних систем (обладнання) та засобів
6. Охарактеризуйте об'єкти та завдання комплексної КТЕ та експертизи відео звукозапису.

Лекція № 4
(денна форма навчання)

Лекція № 2
(заочна форма навчання)

Тема 5. Організаційно-тактичні основи розслідування кіберзлочинів

Мета вивчення

Надати уявлення та сформувати систему знань щодо організаційно-тактичні засад розслідування кіберзлочинів.

Результати навчання

Після лекції здобувач вищої освіти буде (спроможний):

1) визначати належні та прийнятні для юридичного аналізу факти щодо сфери боротьби з кіберзлочинами;

2) застосувати сучасні інформаційні технології та інформаційні ресурси за для розв'язання практичних задач щодо організації розслідування кіберзлочинів;

3) використовувати в правозастосовній діяльності нормативно-правові акти, що регулюють відносини, що виникають в процесі розслудвання злочинів у кіберпросторі;

4) використовувати в професійній юридичній діяльності основні техніко-криміналістичні засобів, прийомів і методів розслідування;

5) проводити слідчі (розшукові) дії, тактичні операції, взаємодіяти з працівниками оперативних підрозділів;

6) аналізувати правові та правозастосовчі проблеми, формувати та обґрунтовувати власну правозастосовну підчас здійснення або участі в слідчих (розшукових) діях в ході розслідування злочинів, вчинених у кіберпросторі.

План

1. Типові слідчі ситуації та завдання початкового та наступного етапів розслідування кіберзлочинів.

2. Характеристика тактичних операцій розслідування кіберзлочинів: їх послідовність, специфіка їх внутрішьої структури.

3. Особливості тактики провадження окремих слідчих (розшукових) дій у справах про кіберзлочин.

3.1. Підготовка до проведення слідчих дій, спрямованих на збирання інформації в електронній формі.

3.2. Тактичні правила та рекомендації, спрямовані на пошук інформації в електронній формі підчас слідчого огляду, обшуку.

3.3. Тактичні правила та рекомендації, спрямовані на фіксацію та вилучення інформації в електронній формі підчас слідчого огляду, обшуку або тимчасового доступу до речей та документів.

3.4. Тактичні рекомендації, спрямовані на вилучення інформації в електронній формі підчас слідчого огляду, обшуку або тимчасового доступу до речей та документів.

3.5. Особливості допиту свідка, потерпілого, підозрюваного у справах про кіберзлочин.

4. Загальні тактичні особливості проведення окремих негласних слідчих (розшукових) дій: зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК); зняття інформації з електронних інформаційних систем (ст. 264 КПК); установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК), контроль за вчиненням злочину (ст. 271 КПК).

Основний зміст

1. Типові слідчі ситуації та завдання початкового та наступного етапів розслідування кіберзлочинів

Проблематика оцінювання прокурором правильності кваліфікації дій підозрюваної особи при вчиненні кіберзлочину та достатності доказів для складання обґрунтованого повідомлення про підозру призводить до розширення переліку основних завдань початкового етапу розслідування кіберзлочинів. Тому початковому етапу надається особливе значення в методиці розслідування таких злочинів. ***Основні завдання початкового етапу розслідування кіберзлочинів***: 1) встановлення відсутності/наявності події кримінального правопорушення (час, місце, спосіб та інші обставини вчинення кримінального правопорушення); 2) встановлення складу визначеного кримінального правопорушення (час, місце, спосіб, мета/мотив, повторність, вчинення групою осіб/організованою групою, наслідки й інші обставини вчинення кримінального правопорушення); 3) встановлення фактичних даних, які вказують на конкретну особу, що могла вчинити кримінальне правопорушення (форма вини, мотив і мета вчинення кримінального правопорушення особою, стосовно якої вирішують питання щодо вручення їй повідомлення про підозру); 4) забезпечення здійснення кримінального провадження; 5) встановлення злочинної діяльності в повному обсязі; 6) встановлення характеру й тяжкості обвинувачення щодо кожного суб'єкта злочину. Чинниками типізації слідчих ситуацій початкового етапу розслідування є: 1) характер (обсяг) інформації про особу злочинця; 2) форма початку кримінального провадження. Останній відображає специфіку типових слідчих ситуацій класифікаційних груп/підгруп злочинів, вчинених у кіберпросторі. Розглядається ***така систематизація слідчих ситуацій***. 1. Ситуації, що характеризуються наявністю персоналізованих відомостей про користувача як імовірного злочинця (розгорнуті анкетні дані особи). 2. Ситуації, що характеризуються наявністю неперсоналізованих відомостей про користувача

як імовірного злочинця.3. Ситуації, що характеризуються відсутністю будь-яких відомостей про особу злочинця. У межах кожної з груп таких слідчих ситуацій схарактеризовано три різновиди: 1) ситуація, коли кримінальне провадження розпочато на підставі отримання заяви/повідомлення особи про кримінальне правопорушення; 2) ситуація, коли кримінальне провадження розпочато внаслідок перевірки оперативної інформації; 3) ситуація, коли кримінальне провадження розпочато в межах реалізації матеріалів ОРС. Розгляд ситуацій у комплексі з основними тактичними завданнями та комплексом слідчих (розшукових) дій та інших заходів пізнання визначає специфіку розслідування класифікаційних груп/підгруп злочинів, вчинених у кіберпросторі.

Основними завданнями наступного етапу розслідування кберзлочинів: встановлення характеристик особи/осіб, яких обвинувачують, зокрема, ступеня та характеру сприяння підозрюваного/обвинуваченого в проведенні кримінального провадження щодо нього або інших осіб; встановлення інших обставин, які враховує прокурор під час вирішення питання про укладення угоди про визнання винуватості (суспільного інтересу в запобіганні, виявленні чи припиненні більшої кількості кримінальних правопорушень або інших більш тяжких кримінальних правопорушень, у забезпеченні швидшого досудового розслідування, викритті більшої кількості кримінальних правопорушень). Ситуації наступного етапу розслідування злочинів, вчинених у кіберпросторі, можна розглядати лише як орієнтири для слідчого, адже слідчу ситуацію в конкретному кримінальному провадженні зумовлює зміст обставин, викладених в акті повідомлення конкретній особі про підозру. ***Типові ситуації наступного етап розслідування кіберзлочинів***: 1) с*приятлива ситуація наступного етапу розслідування* (притаманна повнота виконання тактичних завдань початкового етапу розслідування та конкретизація зайнятих кожним із підозрюваних у кримінальному провадженні позицій); 2) н*есприятлива ситуація розслідування.*

2. Характеристика тактичних операцій розслідування кіберзлочинів: їх послідовність, специфіка їх внутрішьої структури

Існують такі типові тактичні операції початкового етапу розслідування кіберзлочинів: «Персоналізація відомостей про особу/осіб злочинця/ів»; «Збирання електронних (цифрових) носіїв інформації»; «Встановлення кінцевого мотиву злочинної діяльності в кіберпосторі»; «Встановлення та подолання засобів конспірації, які використовують учасники мережевої злочинної групи»; «Встановлення технології злочинної діяльності з використанням кіберпростору»; «Матеріалізація ідеальних слідів вчинення злочину в кіберпросторі»; «Організація затримання та/або отримання свідчень злочинця, що діє в кіберпросторі».

Тактична операція «Персоналізація відомостей про особу/осіб злочинця/ів». Однойменне тактичне завдання розслідування є першочерговим для більшості слідчих ситуацій (2.1–2.3; 3.1, 3.2). Операція передбачає такі поступові слідчі (розшукові) дії, оперативно-розшукові й організаційні заходи:

1) зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи непов'язаний з подоланням системи логічного захисту; 2) встановлення місцезнаходження радіоелектронного засобу;
3) оформлення та відправлення запитів про витребування від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових осіб відомостей, що становлять інтерес для кримінального провадження та/або здійснення запитів щодо обміну інформацією між компетентними підрозділами правоохоронних органів іноземних держав з питань реагування на кіберзлочини каналами сектору Національного контактного пункту реагування на кіберзлочини (НПК ДКП НП України).

Тактична операція «Збирання електронних (цифрових) носіїв інформації». Специфічним є момент її реалізації, який характеризується обов'язковістю розв'язання на цей час тактичних завдань розслідування щодо персоналізації відомостей про особу/осіб злочинця/злочинців і подолання засобів конспірації, які використовують учасники мережевої злочинної групи. Тому первинною зазначена операція стає в ситуаціях, у яких наявні персоналізовані відомості про користувача як злочинця (ситуації 1.1–1.3), для інших ситуацій вона є вторинною. У структурі: 1) погодження клопотань про провадження тимчасових доступів до речей і документів, їх провадження з метою фіксації (копіювання) інформації, що становить інтерес для кримінального провадження; 2) погодження клопотання про проведення обшуку, його здійснення з метою фіксації інформації, що становить інтерес для кримінального провадження, або з метою вилучення електронних носіїв інформації (за необхідності подолання систем логічного захисту інформації на носії); 3) слідчий огляд електронних цифрових носіїв інформації (оригінала або дубліката) з метою дослідження носіїв електронної інформації, що становить інтерес для кримінального провадження; 4) призначення судово-бухгалтерської експертизи та/або комп'ютерно-технічної експертизи, мистецтвознавчої експертизи, інших видів судових експертиз з метою дослідження носіїв електронної інформації, що становить інтерес для кримінального провадження.

Тактична операція «Встановлення кінцевого мотиву злочинної діяльності в кіберпросторі». Розв'язання тактичного завдання щодо персоналізації відомостей про особу/осіб злочинця/ів не означає, що первинна кваліфікація події злочину відповідає дійсності (ситуації 2.3, 3.1, 3.2). Розв'язують шляхом здійснення такого комплексу дій: зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача; контроль за вчиненням злочину у формі спеціального слідчого експерименту.

Тактична операція «Встановлення та подолання засобів конспірації, які використовують учасники мережевої злочинної групи». Це тактичне завдання є типовим за наявності інформації про діяльність встановленої/невстановленої особи в складі організованої злочинної групи (ситуації 3.1–3.3). До структури операції належать такі дії: контроль за вчиненням злочину; здійснення за дорученням слідчого оперативним

підрозділом оперативного (ініціативного) пошуку з метою встановлення характеру дій особи, що становить інтерес для кримінального провадження; зняття інформації з транспортних телекомунікаційних мереж (електронних інформаційних систем) конкретного абонента.

Тактична операція «Встановлення технології злочинної діяльності з використанням кіберпростору». У змісті слідчих ситуацій, що характеризуються браком будь-яких відомостей про особу злочинця (ситуації 3.1–3.3) наявна так звана «фактична складова інформації про злочин». Має складовими такі дії: аудіо-, відеоконтроль особи та/або місця; спостереження за особою, річчю або місцем / дослідженням публічно недоступних місць, житла або іншого володіння особи; виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації (за певних умов).

Тактична операція «Організація затримання та/або отримання свідчень злочинця, що діє в кіберпросторі». У цьому комплексі слідчих та організаційних дій фізичному затриманню особи злочинця передують такі дії: 1) здійснення за дорученням слідчого оперативним підрозділом заходів оперативного (ініціативного) пошуку з метою встановлення місцеперебування особи; 2) попереднє опитування особи, яку підозрюють; 3) погодження клопотання про застосування запобіжного заходу щодо цієї особи, затримання; 4) повідомлення про підозру й допит підозрюваного.

3. Особливості тактики провадження окремих слідчих (розшукових) дій у справах про кіберзлочин

Інформація в електронній формі або електронні дані (відповідно до термінології Конвенції про кіберзлочини) або електронний документ (виходячи зі змісту положень КПК України) мають такі характеристики: не може існувати без носія інформації – ***джерелами електронних даних*** як доказів є різноманітні носії інформації (моноблоки, мобільні телефони, планшетні комп’ютери, цифрові камери, роутери, маршрутизатори, комп’ютерні мережі, глобальна мережа Інтернет, що містить звуко- та відеозаписи тощо; невидимі «неозброєним оком» і для їх сприймання та дослідження використовують програмно-технічні засоби; можуть бути змінені, пошкоджені або знищені в процесі експлуатації пристрою користувачем чи під впливом фізичних чинників; за стадіями виготовлення документи, в тому числі й електронні, поділяють на оригінали, дублікати, копії й виписки.

3.1. Підготовка до проведення слідчих дій, спрямованих на збирання інформації в електронній формі. По-перше, потрібно погодити клопотання. про провадження тимчасових доступів до речей і документів з метою фіксації (копіювання) інформації, що становить інтерес для кримінального провадження або про проведення обшуку з метою фіксації інформації, що становить інтерес для кримінального провадження, або з метою вилучення електронних носіїв інформації (за необхідності подолання систем логічного захисту інформації на

носії) По-друге, володіти визначеною інформацією про об’єкт та предмет слідчої дії. По-третє, створити та проінструктувати СОГ. По-четверте, забезпечити групу необхідними інструментами (або впевнитися в тому, що інструментів достатньо). По-п’яте, забезпечити швидкий та безпечний шлях для проникнення в приміщення та переміщення в ньому. По-шосте, у разі проведення обшуку в житлі чи нежитлових офісних приміщеннях, у яких власниками встановлені камери відеоспостереження, забезпечити їх відмикання.

3.2. Тактичні правила та рекомендації, спрямовані на пошук інформації в електронній формі підчас слідчого огляду, обшуку. Спеціальні прийоми: спеціаліст проводить пошук потрібної електронної інформації (цьому сприяють пошукові програми та програми, які фіксують попередню роботу комп’ютера); спеціаліст складає перелік програм, розміщених у комп’ютері та на лазерних дисках; слідчий повинен витребувати ліцензію чи інші документи, що підтверджують законність використання знайдених програм; у разі неможливості розкриття корпусів комп’ютерної техніки (наприклад, інформація при цьому може бути знищена або її неможливо швидко проаналізувати через великий обсяг) засоби комп’ютерної техніки слід вилучати цілком, причому виключати комп’ютерну техніку слід відповідно до технічних правил роботи на ній; усі знайдені машинні носії інформації (дискети, лазерні диски тощо) необхідно вилучати для наступного дослідження їх змісту, якщо не можна проглянути їх на місці; необхідну для слідства частину інформації з комп’ютера потрібно скопіювати на машинні носії інформації, які були заздалегідь підготовлені спеціалістом для обшуку; не можна використовувати спеціальну пошукову техніку, яка містить джерело електромагнітного або магнітного випромінювання; доцільно вилучати лише матричний принтер, оскільки лише відносно нього можна вирішити ідентифікаційні завдання (для лазерного або струменевого принтера подібний аналіз практично неможливий); якщо неможливо або не доцільно вилучати комп’ютер, то інформацію, яка цікавить, можна роздрукувати на принтері та вилучити ці документальні носії інформації, а у разі недоцільності вилучення принтера для ідентифікації можна провести контрольні роздруківки з принтера на різних зразках паперу або вилучити картриджі зі стрічкою; необхідно промаркувати всю систему підключення до того, як комунікації будуть від’єднані, для того, щоб під час експертного дослідження ЕОМ зібрати аналогічної конфігурації; комп’ютерні технології, які були вилучені, та носії, на які здійснено копіювання, необхідно належним чином упакувати та опечатати, наприклад системний блок опечатується аркушем з підписами слідчого, спеціаліста, представника особи, у власності якої знаходиться об’єкт обшуку, та понятих шляхом наклеювання на задню панель з обов’язковим накладанням на бокові стінки та разйоми електроживлення, магнітні носії інформації потрібно також захистити від запису з використання технічних прийомів.

Алгоритм дій підчас огляду локального комп'ютерного засобу[5]. 1. Після вмикання комп'ютера необхідно пересвідчитись у налаштуванні BIOS на завантаження з приводу оптичних дисків або з флеш-накопичувача (при загрузці натиснути клавішу Del, Esc або F2 – при включенні, у разі потреби внести необхідні зміни та перезавантажити. 2. Завантажити операційну систему з робочого примірника спеціаліста. 3. Підключити принтер, роздрукувати текст із правами й обов'язками учасників слідчої дії, ознайомити їх із цими документами під підпис. 4. Приєднати носій, на який здійснюватиметься запис і на якому зберігатиметься інформація, отримана під час огляду, після чого його відформатувати. 5. За допомогою відповідної програми вивести на екран монітора інформацію про апаратне та програмне забезпечення комп'ютера, необхідну для його ідентифікації, зберегти її як окремий файл. 6. У разі потреби в перегляді файлів із відеограмами запустити програму запису зображення екрана монітора. 7. Здійснити огляд вмісту носіїв інформації, демонструючи учасникам зміст та місцезнаходження (шлях розташування) файлів. 8. У разі потреби та наявності ресурсів здійснити побітове копіювання, створивши файл-образ носія. 9. Скопіювати файли з відеограмою та скриншотами зображення екрана монітора. 10. вивести на екран монітора інформацію про контрольну суму кожного файла.11. Приєднати та відформатувати другий носій, після цього скопіювати на нього всю інформацію з контрольного носія. 12. Інформацію про здійснений огляд внести до протоколу та роздрукувати його, після чого обрахувати його контрольну суму й обидва файли (протокол і файл з його контрольною сумою) зберегти на контрольному і робочому примірниках носіїв разом з каталогом із доказовою інформацією. 13. Від'єднати носії з доказовою інформацією та упакувати. До вказаного алгоритму дій можна додати додаткові пункти за умови огляду віддаленого ресурсу комп'ютерної мережі щодо встановлення IP-адреси сайта (ping), шляху проходження пакетів при обміні інформацією з ним, скопіювати їх на носій, призначений для запису та зберігання доказової інформації.

3.3. Тактичні правила та рекомендації, спрямовані на фіксацію інформації в електронній формі підчас слідчого огляду, обшуку або тимчасового доступу до речей та документів.

З метою матеріалізації носія даних запис образу оптичного диска необхідно здійснити мінімум у 2-ох примірниках на носії відповідного типу (CD або DVD), що не підлягають перезапису. Спеціаліст ДКП НП України повідомляє слідчого, учасників слідчої дії, понятих та присутніх про копіювання (знаття дампу) оперативної пам'яті, браузера з історією, логінами, паролями, копіювання файлів месенджерів та даних щодо відомих мереж, до яких здійснювалося підключення, і паролів до них. Після цього з дозволу слідчого здійснюється таке копіювання. При цьому спеціаліст кіберполіції повідомляє присутнім та учасникам слідчої дії про:інформацію, яка підлягає копіюванню, її місцезнаходження на носії інформації, програмне забезпечення,

[5] Використання електронних (цифрових) доказів у кримінальних провадженнях [Текст] : метод. рек. / [М. В. Гребенюк, В. Д. Гавловський, М. В. Гуцалюк, В. Г. Хахановський та ін.]; за заг. ред. М.В. Гребенюка. Київ: МНДЦ при РНБО України, 2017. 77 с.

за допомогою якою здійснюється таке копіювання, із зазначенням умов його ліцензування, зовнішнього носія інформації, на який здійснюється та в подальшому здійснюватиметься копіювання такої інформації, його серійних, ідентифікаційних чи інвентарних номерів. Після завершення копіювання спеціаліст кіберполіції демонструє всім учасникам обшуку та присутнім на екрані: адресу зовнішнього носія інформації, на який здійснено копіювання файлів, оголошує найменування та кількість скопійованих файлів, їхні розміри.

У разі, коли екран пристрою заблоковано, за можливості слід з'ясувати пароль користувача, а також встановити, чи увімкнене шифрування диска. Якщо пароль доступу не надається, доручити спеціалісту ДКП НП України виготовити дамп оперативної пам'яті з метою відшукування паролів, що зберігаються у ній, до моменту вимикання.

Фіксація доказової інформації в мережі Інтернет має свою специфіку. Докази можуть міститися на веб-сайтах, електронній пошті, соціальних мережах, різноманітних форумах, у пошукових системах інформації тощо. Здебільшого електронна інформація мережі Інтернет зберігається у вигляді веб-сторінок, які складаються з окремих електронних документів, що містять дані у вигляді тексту, графічних зображень, електронних таблиць, відео тощо і можуть бути переглянуті за допомогою спеціальних комп'ютерних програм – веб-переглядачів (браузерів): Internet Explorer, Mozila Firefox, Google Chrome, Opera та ін. Сукупність веб-сторінок, об'єднаних за змістом та навігацією і розміщених за певною мережевою адресою, називається веб-сайтом (website).
Код сайта допомагає отримати електронні докази щодо особливостей фактичної інформації цього сайта. Існують також **метадані**, які можуть бути джерелом високотехнічної інформації про саму веб-сторінку (інформація про дату останньої модифікації веб-ресурсу (веб-сторінки, зображення і тощо).

3.4. Тактичні рекомендації, спрямовані на вилучення інформації в електронній формі підчас слідчого огляду, обшуку або тимчасового доступу до речей та документів.

Забороняється тимчасове вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку, крім випадків, коли: їх надання разом з інформацією, що на них міститься, є необхідною умовою проведення експертного дослідження, такі об'єкти отримані в результаті вчинення кримінального правопорушення чи є засобом або знаряддям його вчинення; доступ до них обмежується їх власником, володільцем або утримувачем чи пов'язаний з подоланням системи логічного захисту. Для опечатування носіїв необхідно упакувати їх у жорстку негнучку коробку та опечатати її. Далі слід зробити на окремому аркуші паперу докладний опис упакованих носіїв (тип кожного з них, їх кількість). Коробка з носіями і опис поміщаються в поліетиленовий пакет, де горловина пакета міцно обв'язується шовковою (капроновою) ниткою і фіксується двома подвійними простими вузлами, які розміщують на діаметрально протилежних сторонах. *Недопустимо надання частини вилучених засобів у розпорядження організації (установи) з причин «виробничої необхідності», адже в процесі роботи можуть бути внесені зміни у файли інформації чи програми*. Вилучення мобільних пристроїв

має свої особливості (в залежності від заблокованості того чи заблоковано екран).

3.5. Особливості допиту свідка, потерпілого у справах про кіберзлочин.

Допит щодо дослідження доказів на електронних носіях інформації порівняно з іншими слідчими діями має високе інформаційне навантаження (зі слідчої практики відомо, що у справах 60% складають протоколи допиту осіб з приводу інформації в електронній формі; 40% – інші протоколи, що описують використання джерел ідеальної інформації) Для підтвердження або спростовування доказової інформації в електронному вигляді необхідне проведення певного комплексу допитів необхідних з цих міркувань осіб.

Вивчення кримінальних справ дозволяє визначитись із колом осіб, що підлягають допиту як свідки, це: а) службові особи та працівники установи-жертви, що можуть мати відношення до обставин вчинення злочину; б) представники та працівники юридичної особи, яка використовувалася під час вчинення злочину тим чи іншим способом; в) спеціалісти, що мають професійний досвід у галузі інформатики та комп'ютерної техніки, програмування, в тому числі особи, які приймали участь у якості спеціалістів підчас слідчих (розшукових) дій. Свідки часто володіють спеціальною, професійною освітою (у сфері КТ, банківського електронного обігу коштів) або в цілому є обізнаними у питаннях використання інформаційних технологій та ІТ-технологіях. В теоретичному аспекті важко визначитися з послідовністю проведення допитів свідків, що пов'язано з конкретними обставини справи, певними результатами ознайомлення слідчого з документами, організацією роботи установи, зокрема розподілом обов'язків та її структурою.

Як доводить слідча практика, сприятиме дотриманню принципу послідовності дослідження доказів на електронних носіях інформації проведення допитів ***у такому порядку:*** від допиту осіб, яким відома більш повна інформація про обставини злочину (зокрема це особи, які виявили злочин або проводили першочергову перевірку засобів комп'ютерної техніки) до тих, хто має орієнтовну інформацію в справі щодо КТ (всі інші).

4. Загальні тактичні особливості проведення окремих негласних слідчих (розшукових) дій

Зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи непов'язаний з подоланням системи логічного захисту, є одним з двох видів такої НС(Р)Д, як зняття інформації з електронних інформаційних систем[6]. Ця дія як компонент тактичної операції «Персоналізація відомостей про особу/осіб злочинця/ів» реалізується шляхом пошуку слідчим або інспектором кіберполіції (за дорученням слідчого) в різноманітних Інтернет-спільнотах відкритої інформації про особу злочинця.

[6] Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ ГП України, МВС України, СБ України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16 листоп. 2012 р. № 114/1042/516/1199/936/1687/5. URL: https://zakon2.rada.gov.ua/laws/show/v0114900-12.

Виконавець за результатами дії складає протокол, у якому фіксує такі відомості: персоналізовані відомості про особу злочинця; ознака, за якою об'єднують коло осіб, що потрапляють під підозру; зв'язки особи, що потрапила під підозру; відомості, що можуть сприяти розв'язанню інших тактичних завдань (пошук свідків, потерпілих, забезпечення встановлення мотивів злочину тощо). До протоколу зняття інформації з електронних інформаційних систем або її частини додають відповідні носії електронної інформації, що містять файли з відеограмою та зображенням екрана монітора (або знімками екрану, англ. *screenshot*), створеними під час дослідження системи, також їх роздруківки як додатків до протоколу.

Встановлення місцезнаходження радіоелектронного засобу. Ця НС(Р)Д, відповідно до ст. 268 КПК України, полягає в застосуванні технічного обладнання для локалізації місцезнаходження радіоелектронного засобу, зокрема мобільного терміналу, систем зв'язку й інших радіовипромінювальних пристроїв, активованих у мережах операторів рухомого (мобільного) зв'язку, без розкриття змісту повідомлень, що передаються, якщо внаслідок його проведення можна встановити обставини, які мають значення для кримінального провадження. Фактично ж слідчий ініціює її проведення в кримінальних провадженнях різного ступеня тяжкості задля визначення параметрів базових станцій операторів телекомунікацій, що забезпечують роботу в певному місці кінцевого обладнання систем зв'язку, і місцезнаходження інших радіовипромінювальних пристроїв, активованих у мережі операторів рухомого (мобільного) зв'язку.

Зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача передбачено ст. 264 КПК України НС(Р)Д, воно полягає в одержанні інформації, зокрема із застосуванням технічного обладнання, яка міститься в електронно-обчислювальних машинах (комп'ютерах), автоматичних системах, комп'ютерній мережі. Цю НС(Р)Д ініціює слідчий виключно в кримінальному провадженні щодо тяжких або особливо тяжких злочинів, її проводять на підставі дозволу слідчого судді на втручання в приватне спілкування. Проведення цієї дії потребує наявності спеціальних знань у галузі інформаційних технологій.

Контроль за вчиненням злочину.Контроль за вчиненням злочину є засобом криміналістичної тактики, шляхи оптимізації проведення якого доцільно визначати в контексті особливостей тактики його проведення підчас розслідування злочинів окремої групи чи виду.

Відсутність законодавчих критеріїв розмежування форм цього НС(Р)Д, зумовлює часто суб'єктивний характер обрання ініціатором в конкретні ситуації однієї з форм реалізації контролю за вчиненням злочину. Тому обрання тієї або іншої форми проведення контролю за вчиненням злочину розглянули через призму тактичної обумовленості конкретної з форм цієї НС(Р)Д підчас розслідування кіберзлочинів. Це дозволило сформулювати наступні тактичні рекомендації з оптимізації тактики його проведення щодо обраної категорії злочинів. По-перше, тактичною метою проведення контролю за вчиненням злочину у формі спеціального слідчого експерименту є встановлення кінцевого

мотиву злочинної діяльності в кіберпросторі; у формі імітування обстановки злочину – встановлення замовника кіберзлочину; у формах контрольованої поставки, контрольованої та оперативної закупки – подолання засобів конспірації, які використовують учасники мережевої злочинної групи. Підчас розслідування конкретного кіберзлочину ініціатор, керуючись слідчою ситуацією, практичними міркуваннями встановлює переважаючу в організаційно-тактичному плані мету проведення цієї НС(Р)Д та обирає конкретну форму проведення контролю за вчиненням злочину. По-друге, безпосереднє проведення цієї НС(Р)Д доручають оперативному підрозділу. По-третє, контрольована поставка, контрольована та оперативна закупка як форми НС(Р)Д обираються як тактичний засіб підчас розслідування тяжких та особливо тяжких кіберзлочинів, зокрема придбання чи збут зброї, бойових припасів або вибухових речовин, незаконного придбання, збут наркотичних засобів, психотропних речовин або їх аналогів та прекурсорів. Тактичні рекомендації, прийоми та методи проведення контрольованої поставки, контрольованої та оперативної закупки зумовлюються особливостями предмета їх здійснення.

Контрольні запитання для перевірки досягнення результатів навчання

1. Назвіть типові тактичні операції розслідування кіберзлочинів, охарактеризуйте їх послідовність та їх внутрішню структуру.
2. Які можна назвати тактичні рекомендації щодо підготовки до СРД, спрямованої на збирання інформації в електронному вигляді .
3. Наведіть алгоритм дій підчас огляду локального комп’ютерного засобу з метою збирання інформації в електронному вигляді.
4. Навіщо додавати до протоколу слідчої дії робочий та контрольний примірник усіх програмних засобів, а також даних, що вміщують доказову інформацію?
5. Які дії потрібно провести з мобільним пристроєм підчас його вилучання, якщо його екран заблоковано?
6. Охарактеризуйте особливості проведення контролю за вчиненням злочиу підчас розслідування кіберзлочинів.

Лекція № 5
(денна форма навчання)

Тема 6. Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі

Мета вивчення

Надати уявлення та сформувати систему знань щодо методики розслідування кіберзлочинів вчинених з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі

Результати навчання

Після лекції здобувач вищої освіти буде (спроможний):

1) визначати належні та прийнятні для юридичного аналізу факти щодо сфери боротьби з кіберзлочинами;

2) застосувати сучасні інформаційні технології та інформаційні ресурси за для розв'язання практичних задач щодо організації та планування розслідування кіберзлочинів, що вчиняються с корисливих мотивів;

3) використовувати в правозастосовній діяльності нормативно-правові акти, що регулюють відносини, що виникають в процесі розслудвання злочинів у кіберпросторі;

4) використовувати в професійній юридичній діяльності основні техніко-криміналістичні засобів, прийомів і методів розслідування;

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

План

1. Сутність та криміналістична класифікація кіберзлочинів, вчинених з корисливих мотивів.

2.Особливості розслідування злочинів, що спрямовані на заволодіння чужим майном, та пов'язані з ними злочини у сфері функціонування електронних розрахунків: криміналістична характеристика, типові слідчі ситуації початкового етапу і програми (алгоритми) розслідування; особливості тактики окремих слідчих дій.

3. Особливості розслідування кіберзлочинів, що порушують встановлений порядок обігу певних речей: криміналістична характеристика, типові слідчі ситуації початкового етапу і програми (алгоритми) розслідування;

особливості тактики окремих слідчих дій.

Основний зміст

1. Сутність та криміналістична класифікація кіберзлочинів, вчинених з корисливих мотивів.

В результаті аналізу сучасного контенту Інтернет-простору можна виділити фінансово-економічну сферу суспільного життя суб'єктів відносин у кіберпросторі як таку, що пов'язана зі здійсненням розрахункових операцій та укладанням цивільно-правових угод. Економічна сфера є цілісною підсистемою суспільства, яка відповідає за виробництво, розподіл, обмін і споживання матеріальних благ та послуг, необхідних для життєдіяльності людей. Особливу роль відіграють в економічному і соціальному розвитку фінанси. Фінансові операції відображають діяльність, пов'язану із здійсненням або забезпеченням здійснення платежів для проведення транзакцій. Саме тому у Стратегії розвитку інформаційного суспільства в Україні, схваленої розпорядженням Кабінету Міністрів України від 15 травня 2013 р. № 386-р закріплено термін електронна економіка як форма економічних відносин у сфері виробництва, розподілу, обміну та споживання товарів, робіт і послуг, наданих в електронному вигляді за допомогою інформаційно-комунікаційних технологій (далі - е-економіка). кримінальні правопорушення, вчинені у сфері фінансово-економічних відносин суб'єктів кіберпростору, являють собою злочинні діяння, пов'язані зі здійсненням розрахункових операцій та укладанням цивільно-правових угод, що об'єднують особливості механізму злочинної діяльності, зумовлені особливою обстановкою їх вчинення – кібепростором, зокрема його двома визначальними чинниками : певною сферою суспільного життя в кіберпросторі (соціальний); обраним злочинцем специфічним набором операцій, які забезпечують існування кіберпростору (технічний). Такі злочини можна класифікувати на три групи.

1. *злочини, що порушують встановлений порядок обігу певних речей*: придбання чи збут зброї, бойових припасів або вибухових речовин (ст. 263 КК України); незаконне придбання, збут наркотичних засобів, психотропних речовин або їх аналогів та прекурсорів (ст. 307, 311); незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації (ст. 359);

2. *злочини, що спрямовані на заволодіння чужим майном, та пов'язані з ними злочини у сфері функціонування електронних розрахунків*: крадіжка (ст. 185 КК України); вимагання (ст. 189); шахрайство (ст. 190); привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем (ст. 191); незаконні дії з платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення (ст. 200); зайняття гральним бізнесом (ст. 203-2); легалізація (відмивання) доходів, одержаних злочинним шляхом (ст. 209);

3. *злочини, що порушують механізми захисту від монополізму та недобросовісної конкуренції*: протидія законній господарській діяльності (ст.

206); незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару (ст. 229); незаконне збирання з метою використання відомостей, що становлять комерційну чи банківську таємницю (ст. 231); розголошення комерційної або банківської таємниці (ст. 232).

2.Особливості розслідування злочинів, що спрямовані на заволодіння чужим майном, та пов'язані з ними злочини у сфері функціонування електронних розрахунків

Типовий предмет посягання: первинний предмет – інформаційний продукт або ресурс (персональні дані, банківська таємниця: (1) відомості про банківські рахунки клієнтів, кореспондентські рахунки банків у НБУ; 2) операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди; 3) системи охорони банку та клієнтів; 5) відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація; 7) коди, що використовуються банками для захисту інформації; 8) інформація про фізичну особу; 9) документи для службового користування з питань зберігання, захисту, використання та розкриття інформації, що становить банківську таємницю. Вторинний предмет – матеріальні цінності, що мають позитивні властивості, у виді грошових готівкових або безготівкових коштів, коштовних товарів.

Типова особа злочинця. Характерні тип злочинець – упевнений користувач (зазвичай пов'язаний з організацією-жертвою за трудовою угодою або має особисті стосунки з фізичною особою-жертвою (90% матеріалів), через це має доступ до інформації, необхідної для вчинення злочину (ідеться про паролі, адреси, коди доступу, назву файлу, шлях до нього тощо), з метою приховування злочинної діяльності створює ілюзії віддаленого доступу до предмета посягання, переважа\є професійна мобільність), злочинець користувач «професіонал» зазвичай є одним з організаторів у структурі мережевої організованої групи, створеної для вчинення злочинів з корисливих мотивів.

За спеціалізацією можна визначити та охарактеризувати: кардери; кіберкруки; фішери; спамери; кіберсквотери; фрікери; «е - Бізнесмени» та інні види хакерів.

Способи злочину. Властиві технології злочинної діяльності як ть способів, зокрема: 1) технології незаконного збагачення, засновані на попередньому заволодінні персональними даними/комерційною таємницею фізичної/юридичної особи шляхом несанкціонованого втручання в роботу комп'ютерної техніки 2) технології заволодіння безготівковими коштами шляхом застосування електронних платіжних систем, засновані на попередньому несанкціонованому втручанні в роботу комп'ютерної техніки; 3) технології службових розкрадань шляхом застосування електронних платіжних систем, засновані на несанкціонованих діях з інформацією, вчинені особою, котра має право доступу до неї. 4) технології приховування незаконного походження безготівкових коштів, засновані на попередньому

несанкціонованому втручанні в роботу комп'ютерної техніки; 5) технології незаконного збагачення шляхом незаконних дій з платіжними картками. Така злочинна діяльність в Україні найчастіше кваліфікується за сукупністю ст.ст. 200, 190 КК України. Кожна з технологій має властиві їй закономірності.

Однаково поширено (40%) розпочинають провадження в результаті отримання заяви потерпілого/повідомлення особи про кримінальне правопорушення та в результаті ознайомлення з матеріалами оперативного підрозділу щодо перевірки оперативної інформації; 20 % - виявляє безпосередньо слідчий. 1 Типова ситуація характеризується наявністю на початку провадження персоналізованих відомостей про особу злочинця (внутрішнім користувачем мережі вчинені дії, що спрямовані на заволодіння чужим майном, у сфері функціонування електронних розрахунків. В матерілах є внутрішня перевірка (аудит, технічна перевірка, моніторинг мереж тощо). Типова програма першочергових дій: допити, обшук, тимчасовий доступ до речей та документів, запити, огляд, призначення судово-бухгалтерської експертизи та/або комп'ютерно-технічної експертизи, мистецтвознавчої експертизи, інших видів судових експертиз з метою дослідження носіїв електронної інформації, що становить інтерес для кримінального провадження. 2. Типова ситуація характеризується наявністю персоналізованих відомостей про особу злочинця, за такої умови передує комплекс дій, спрямованих на персоналізацію особи.

3. Особливості розслідування кіберзлочинів, що порушують встановлений порядок обігу певних речей

Типовий предмет посягання: первинний предмет – *інформаційний ресурс як знаряддя задля досягнення кінцевої мети злочинної діяльності зумовлює обрання злочинцем певного інформаційного продукту/ресурсу для злочинного впливу на нього (наприклад,* веб-сайт, що використовується для розміщення для розповсюдження інформації певного змісту); вторинні – матеріальні цінності, *що мають негативні властивості*, як-от наркотичні засоби, психотропні речовини, прекурсори, технічні засоби отримання інформації, зброя, бойові припаси та вибухові речовини, що можуть виступатий безпосереднім предметом посягання.

Типова особа злочинця. Типово характеризується як злоочинець – звичайний користувач (якщо злочинець використовує технології анонімізації доступу до ресурсів мережі Інтернет (часто Tor), то припускається вагомих помилок. Усі види мобільності (географічна, соціальна, професійна та економічна) мають усереднені схожі показники. За умови діяльності осіб в складі злочинної групи виділяютьсмя ролі: організатор, хімік, куратор, кадровик, водій, склад, кур'єр, графітчик, спортсмен.

Важливі не тільки електронні, а й *традиційні матеріальні сліди* у вигляді слідів-предмети (неофіційні документи; речі, що мають особливий порядок обігу (спеціальні технічні пристрої, зброя)); слідів-відображень (відбиток

пальця, мікрочастка одягу); слідів-речовин (наркотичні засоби; прекурсори, вибухова речовина тощо).

Способи злочину. Типово застосовують способи злочинних дій, пов'язані з функціонуванням сервісів електронної дошки оголошень (від англ. абревіатури «ВВС»), способи злочинних дій, пов'язані з функціонуванням технологій електронної комерції, створені для здійснення торгівлі через Інтернет (власне, здійснюється стандартизація всіх форм взаємодії між організаціями, залученими в повний цикл «постачання – продаж – купівля (англ. Supply – Selling – Buying)».

Часто кримінальне провадження розпочинають в рамках реалізації сматеріалів оперативно-розшукової діяльності (справ), нечасто в результаті отримання повідомлення особи про кримінальне правопорушення або попередньої перевірки інформації.(10%). Початкова слідча ситуація типово характеризується наявністю неперсоналізованих відомостей про особу злочинця,діяльність якого має ознаки готування до злочинів, що порушують встановлений порядок обігу певних речей**.** На момент початку кримінального провадження інформація, що містить ознаки готування до вчинення злочину зафіксована під час установлення місцезнаходження радіоелектронного засобу; контролю за телефонними розмовами; зняття інформації з електронних інформаційних систем. Ініціативний рапорт є формальним кроком на шляху реалізації матеріалів ОРС, основним завданням слідчого в цій ситуації вбачається фіксація мотиву злочинної діяльності встановленої особи та, у разі спроби вчинення нею злочину, виявлення інших співучасників. Фактично найефективнішим засобом розслідування таких злочинів стає контроль за вчиненням злочину у формі контрольованої поставки, контрольованої й оперативної закупки. Проводяться також типово судово-балістичні, судово-хімічні експертизи, КТЕ.

Контрольні запитання для перевірки досягнення результатів навчання

1. В чому полягає сутність та криміналістична класифікація кіберзлочинів, вчинюваних з корисливих мотивів у фінансово-еколнмоічній сфері ?
2. Які існують основні способи вчинення кіберзлочинів, що спрямовані на заволодіння чужим майном, та пов'язаних із ними злочинів у сфері функціонування електронних розрахунків?
3. Чим характеризується предмет посягання кіберзлочинів, що спрямовані на заволодіння чужим майном, та пов'язаних із ними злочинів у сфері функціонування електронних розрахунків?
4. Які існують типи злочинців, що вчиняють кіберзлочини, що спрямовані на заволодіння чужим майном?
5. Охарактеризуйте програму розслідування кіберзлочинів, що спрямовані на заволодіння чужим майном, та пов'язаних із ними злочинів у сфері функціонування електронних розрахунків.
6. Які особливості розслідування придбання чи збут зброї, бойових припасів або вибухових речовин, вчинених через мережу Інтернет?

7. Які особливості методики розслідування незаконного придбання, збуту наркотичних засобів, психотропних речовин або їх аналогів та прекурсорів, вчинених через мережу Інтернет?

Лекція № 6
(денна форма навчання)

Тема 7. Розслідування кіберзлочинів, вчинених з антидержавно-політичних мотивів, пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі

Мета вивчення

Надати уявлення та сформувати систему знань щодо методики розслідування кіберзлочинів вчинених з антидержавно-політичних мотивів, що пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі

Результати навчання

Після лекції здобувач вищої освіти буде (спроможний):

1) визначати належні та прийнятні для юридичного аналізу факти щодо сфери боротьби з кіберзлочинами;

2) застосувати сучасні інформаційні технології та інформаційні ресурси за для розв'язання практичних задач щодо організації та планування розслідування кіберзлочинів, що вчиняються с антидержавно-політичних мотивів;

3) використовувати в правозастосовній діяльності нормативно-правові акти, що регулюють відносини, що виникають в процесі розслудвання злочинів у кіберпросторі;

4) використовувати в професійній юридичній діяльності основні техніко-криміналістичні засобів, прийомів і методів розслідування;

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

План

1. Сутність та криміналістична класифікація кіберзлочинів, вчинених з антидержавно-політичних мотивів.
2. Особливості розслідування злочининів, що пов'язані з антидержавницькими діями у кіберпросторі: криміналістична характеристика, характеристика початкового етапу і програми (алгоритми) розслідування; особливості тактики окремих слідчих дій.
3. Особливості розслідування кібертероризму: криміналістична характеристика, характеристика початкового етапу розслідування та програми

(алгоритму) дій слідчого.

Основний зміст

1. Сутність та криміналістична класифікація кіберзлочинів, вчинених з антидержавно-політичних мотивів

Об’єктивні причини через які є кіберзлочини, вчинені у сфері державно-політичних відносин суб’єктів кіберпростору мають тенденцію до збільшення: 1) запровадження так званого «електронного уряду», що має забезпечити надання органами влади послуг фізичним та юридичним особам (передбачено Розпорядженням Кабінету Міністрів від 27 травня 2016 р. № 418-р «Про затвердження плану пріоритетних дій Уряду на 2016 р.»); 2) створення централізованих баз даних, заснованих на технології забезпечення електронного документообігу в державних органах та підчас організації та проведення виборів; 3) подальше впровадження автоматизованих систем керування технологічними процесами виробництв та високих сучасних комп’ютерно-інтегрованих технологій в різних галузях промисловості та економіки, в тому числі на підприємствах, що мають стратегічне значення для безпеки держави (Постанова Кабмін України від 4 березня 2015 р. № 83 Про затвердження переліку об'єктів державної власності, що мають стратегічне значення для економіки і безпеки держави»). Кіберзлочини, вчинені у сфері державно-політичних відносин суб’єктів кіберпростору – це злочинні діяння, спрямовані на дерегулювання основних сфер суспільного життя, що створюють загрозу національній безпеці держави, здатні заподіяти великі економічні, екологічні, іміджеві та інші збитки державі, що об’єднують особливості механізму злочинної діяльності, зумовлені особливою обстановкою їх вчинення – кіберпростором, зокрема його двома визначальними чинниками : певною сферою суспільного життя в кіберпросторі (соціальний) - у сфері державно-політичних відносин суб’єктів кіберпростору; обраним злочинцем специфічним набором операцій, які забезпечують існування кіберпростору (технічний). Злочини, вчинені з антидержавно-політичних мотивів, пов’язані з державно-політичною сферою відносин суб’єктів у кіберпросторі, поділяються на підгрупи: 3.1. *злочини, що пов’язані з антидержавницькими діями*: 3.1.1. злочини проти основ національної безпеки України: дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади (ст. 109); посягання на територіальну цілісність і недоторканність України (ст. 110); фінансування дій, вчинених з метою насильницької зміни чи повалення конституційного ладу або захоплення державної влади, зміни меж території або державного кордону України (ст. 110-1); державна зрада (ст. 111); диверсія (ст. 113); шпигунство (ст. 114); 3.1.2. злочини у сфері охорони державної таємниці (ст. 328, 330); 3.1.3. злочини проти судоустрою: незаконне втручання в роботу автоматизованої системи документообігу суду (ст. 376); 3.2. *злочини політико-ідеологічного спрямування*: 3.2.1. злочини

проти виборчих прав і свобод (ст. 157, 158, 159, 159-1); 3.2.2. терористичний акт (ст. 258) та злочини, пов'язані з тероризмом (публічні заклики до вчинення терористичного акту (ст. 258-2); створення терористичної групи чи терористичної організації (ст. 258-3); фінансування тероризму (ст. 258-5); 3.2.3. пропаганда війни й поширення комуністичної, нацистської символіки та пропаганда комуністичного і націонал-соціалістичного (нацистського) тоталітарних режимів (ст. 436, 436-1).

2. Особливості розслідування злочинінів, що пов'язані з антидержавницькими діями у кіберпросторі: криміналістична характеристика, характеристика початкового етапу і програми (алгоритми) розслідування; особливості тактики окремих слідчих дій

Сьогодні первинним предметом посягання виступаж: 1) державна таємниця; 2) *інформаційний ресурс(цінність має також як знаряддя задля досягнення кінцевої мети злочинної діяльності (* веб-сайт, що використовується для розміщення інформації антидержавницького характеру); Вторинний предмет посягання – автоматизовані (електронно-інформаційні) системи різного призначення (платіжні системи; об'єкт критичної інформаційної інфраструктури (наприклад, системи, що забезпечують диспетчерське керування повітряним або залізничним рухом, митне оформлення, поштові відправлення, постачання електроенергії та інші види робіт при вчиненні терористичного акту).

Особа злочинця є користувачем початкового рівня, що; характеризується високою соціальною мобільністю з різних причин (нереалізованість комунікаційних потреб (людина з обмеженими фізичними можливостями, наявність психічних хвороб), наявність географічної мобільності, за відсутності професійної та економічної мобільності (сезонний працівник; робота за кордоном вахтовим методом; кур'єр; водій; сортувальник тощо, причому злочинець виконує роботи низької кваліфікації)). Проблеми конкуренції мотивів вчинення злочину він не має, його злочинна діяльність зазвичай становить собою елементарну вольову дію, як-от розміщення в мережі Інтернет інформації певного місту. Розміщення забороненої інформації у соціальних меражах та адміністрування відповідних груп соціальних мереж здебільше стає типовим способом вчинення різноманітних злочинів з антидержавно-політичних мотивів. Наприклад, розповсюджуються матеріали із закликами про захоплення державної влади, здійснюється вербування агентури для іноземної розвідки, активно сприяють діяльності терористичних організацій. Вчиняючи злочини з антидержавно-політичних мотивів, вони можуть діяти як самостійно, так і в складі корпоративної злочинної групи, виконуючи роль організатора, виконавця чи посібника. Користувач - «професіонал» типово вчиняє на замовлення третьої особи будь-який зі злочинів з антидержавно-політичних мотивів.

Способи злочинних дій, пов'язані з функціонуванням соціально-орієнтованих мереж (від англ. social networks), діяльність яких заснована на так званій вікі(viki)-технології. Способи підготовки, пов'язані з завантаженням,

пошуком, створенням, зберіганням, редагуванням відповідних текстових, фото-, відеофайлів або інших форм публікації. Способи приховування найчастіше не застосовують. В окремих випадках для забезпечення анонімності злочинець може використовувати віртуальні приватні мережі (VPN-технології). Зустрічаються в національній практиці й з способи злочинних дій, пов'язані з функціонуванням шкідливого програмного забезпечення. (з англ. «crimeware», де «crime – злочинність, software – програмне забезпечення; часто як синонім застосовують «вірус»). Це програмне забезпечення злочинці (за типами «впевнений користувач», «досвідчений користувач» та «професіонал») за власною ініціативою або на замовлення трьої особи розробляють та/або поширюють для отримання несанкціонованого доступу до комп'ютера з метою несанкціонованого доступу до інформації та спричинення шкоди.

Типовим є відкриття провадження в результаті діяльності за ОРС. Матеріали первинної перевірки містять неперсоналізовані відомості про особу злочинця або взагалі у ініціативному рапорті оперативного співробітника відсутність відомостей про особу злочинця (що є формальним через не визначеність мотиву підготовчої до злочину діяльності конкретної особи). Алгоритм дій: аудіо-, відеоконтроль особи та/або місця; спостереження за особою, річчю або місцем / дослідженням публічно недоступних місць, житла або іншого володіння особи; виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації (за певних умов); контроль за вчиненням злочину; встановлення місцезнаходження радіоелектронного засобу, затримання, допити, обшуки, призначення експертиз.

Спеціалістами часто виступають співробітників і працівників Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України (ІСТЕ СБ України). Типовими, крім КТЄ, є також трасологічні експертизи, лінгвістичні експертизи мовлення (семантико-текстуальний аналіз писемного й усного мовлення), хімічні експертизи.

3. Особливості розслідування кібертероризму: криміналістична характеристика, характеристика початкового етапу розслідування та програми (алгоритму) дій слідчого.

Серед різновидів тероризму (національного, міжнародного, ідеологічного, релігійного, кримінального) можна виділити такий вид як технологічний. Цей вид тероризму має складний зміст. Згідно, Закону України «Про боротьбу з тероризмом» він містить в собі ядерний тероризм, хімічний тероризм та кібернетичний тероризм. Інформаційний (кібернетичний) тероризм – це новий вид терористичної діяльності, орієнтований на використання різних форм і методів тимчасового або незворотного виведення з ладу інформаційної інфраструктури держави або її елементів, а також за допомогою протиправного використання інформаційної структури для створення умов, що тягнуть за собою тяжкі наслідки для різних сторін життєдіяльності особистості, суспільства і держави (узагальнене визначення). Його різновидом є кібернетичний тероризм, який полягає в використанні сучасних інформаційних

технологій, і в першу чергу Інтернету, коли така зброя застосовується з метою пошкодження важливих державних інфраструктур (таких як енергетична, транспортна, урядова).

Способи злочину реалізуються через кібератаки здатні завдати інформаційно-телекомунікаційним системам на основних інфраструктурах значної шкоди. Кібератака – це сукупність узгоджених щодо мети, змісту та часу дій або заходів (так званих кіберакцій, спрямованих на певний об'єкт впливу з метою порушення конфіденційності, цілісності, доступності, спостережуваності або авторства інформації, що циркулює в ньому, з урахуванням її уразливості, а також порушення роботи IT-систем і мереж зазначеного об'єкта). Характерною особливістю кібератак є миттевість їх здійснення. Звідси слід виокремити основні ознаки кібератаки, серед яких: 1. за метою впливу на об'єкт атаки (спрямований, наприклад, на порушення цілісності або конфіденційності інформації, її захищеності від несанкціонованого доступу а також на порушення живучості системи та надійності її функціонування тощо); 2. за принципом впливу на об'єкт атаки: із використанням прихованих каналів (шляхів передавання інформації, що дозволяють двом процесам обмінюватися нею у спосіб, який порушує політику безпеки; застосування прав суб'єкта системи до об'єкта (файлів даних, каналів зв'язку тощо); 3. за характером впливу на об'єкт атаки (активний вплив та пасивний вплив); 4. за способом впливу на об'єкт атаки (на систему дозволів (захоплення привілеїв), безпосередній доступ до даних, програм, служб, каналів зв'язку з використанням привілеїв та інші). Також набула поширення класифікація, запропонована компанією Internet Security Systems Inc. Скоротивши кількість можливих категорій кібератак до п'яти, фахівці компанії умовно виокремили з них такі, що мають на меті: 1. сприяти збору інформації; 2. сприяти спробам несанкціонованого доступу до інформації; 3. досягти стану відмови в обслуговуванні; 4. імітувати підозрілу активність; 5. чинити вплив на операційні системи. Найбільш поширеними способами здійснення кібератак є IP-спуфінг, DoS і DDoS атаки, парольні атаки, атаки на рівні додатків типу логічних бомб і троянських коней, вірусні атаки й так звані ін'єкції.

Залежно від типових ситуацій, що складаються на початковому етапф розслідування, слідчий визначає програму дій, спрямовану не тільки на персоналізацію особи злочинця, а також на усунення негатичних наслідчів події. Доцільність і зкономичности процесу розслідування є головними принципами при обранні слідчим програми дій, оскільки тільки вона дозволяє якнайповніші встановити подію злочину.

Залежно від збереження первинної обстановки місця події, можна виделить такі типові ситуації: 1. Обстановка місця події частково або повністю збереглася (терористичному акту запобігло за допомогою технічних засобів захисту або результату терористичного акту були не значними); дозволяє найбільш зффективно встановити всю подію злочину, осіб виконавця і круг підозрюваних в організації злочину, організувати їх пошук і затримання. 2. Обстановка місця події не збереглася. Дана ситуація формується тоді, коли наслідки кібератаки виявляються у вигляді полнотного руйнування обьекта

тероризму – знищення інформаційної системи. Складно знайти місце проникнення в систему, за допомогою лише міжнародного співробітництва встановлюється особа злочинця/група осіб. Особі, що провадить розслідування, необхідно оглянути місця події, встановити і допитати потерпілих і свидетелей-очевидців, призначити технічні, технологческие і криміналістичні та типові для кіберзлочинів експертизи. Одночасно із цим проводиться комплекс негласних (слідчих) розшукових дій (див. Тему 5). Важливим є також акцент на оцінки масштабів результату кібератаки, усуненні цих наслідків, налагодження міжвідомчих зв'язків з метою забезпечення розслідування в контексті транснаціональнаї складової кібертероризма, організація взаємодії з міжнародними та національними поліцейськими установами.

Контрольні запитання для перевірки досягнення результатів навчання

1. В чому полягає сутність та криміналістична класифікація кіберзлочинів, вчинюваних з антидержавно-політичних мотивів ?
2. Які існують основні способи вчинення злочинів, що пов'язані з антидержавницькими діями у кіберпросторі?
3. Чим характеризується предмет посягання при вчиненні злочинів, що пов'язані з антидержавницькими діями у кіберпросторі?
4. Які існують типи злочинців, що вчиняють злочини, що пов'язані з антидержавницькими діями у кіберпросторі?
5. Охарактеризуйте програму розслідування злочинів, що пов'язані з антидержавницькими діями у кіберпросторі.
6. Які особливості розслідування інцидентів кібертероризма?

ПЛАНИ ПРАКТИЧНИХ ЗАНЯТЬ

Заняття № 1
(денна форма навчання)

Заняття№1
(заочна форма навчання)

Тема 1. Методичні основи розслідування кіберзлочинів

Мета вивчення

Сформувати та закріпити систему знань про сучасні методологічні основи розслідування кіберзлочинів, визначити основні проблеми правозастосовної практики в цій сфері, а також шляхи їх подолання.

Результати навчання

Після практичного заняття здобувач вищої освіти буде (спроможний):

1) застосувати сучасні інформаційні технології та інформаційні ресурси з для розв'язання практичних задач з аналізу злочиннох діяльності у кіберпросторі;

2) орієнтуватися в термінологічному контенті в сфері протидії кіберзлочинності та злочинів, вчинених у кіберпросторі;

3) використовувати в правозастосовній діяльності нормативно-правові акти, що регулюють відносини, що виникають підчас виявлення та розслідування фактів вчинення злочинів у кіберпросторі.

Література

нормативно-правові акти:

1. Конвенції ООН проти транснаціональної організованої злочинності : міжнар. док. від 15 листоп. 2000 р. URL: http://zakon3.rada.gov.ua/laws/show/995_789.

2. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : міжнар. док. від 28 січ. 1981 р. URL: http://zakon5.rada.gov.ua/laws/show/994_326.

3. Конвенція про кіберзлочинність : міжнар. док. від 23 листоп. 2001 р. URL: http://zakon3.rada.gov.ua/laws/show/994_575?nreg=994_575&find=1&text=%F7%E0%F1&x=0&y=4#w11

4. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : розпорядження Кабінету Міністрів України від 15 трав. 2013 р. № 386-р. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80.

5. Про телекомунікації : Закон України від 18 листоп. 2003 р. № 1280-IV-ВР. URL: https://zakon.rada.gov.ua/laws/show/1280-15.

спеціальна література:

6. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями / пер. с англ. М. : Мир, 1999. 351 с.

7. Бантишев О. Ф. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації) : монографія. Київ : Нац. акад. СБ України, 2001. 122 с.

8. Барцицька А. А. Криміналістичні технології: сутність та місце в системі криміналістичної науки : дис. … канд. юрид. наук : 12.00.09. Одеса, 2011. 262 с.

9. Батурин Ю. М. Проблемы компьютерного права. М. : Юрид. лит., 1991. 272 с.

10. Бауэр Ф. Л., Гооз Г. Информатика : в 2 ч. М., 1990. Ч. 1 : Вводный курс. 336 с.

11. Биленчук П. Д., Еркенов С. Е., Кофанов А. В. Транснациональная преступность: состояние и трансформация : учеб. пособие / под ред. П. Д. Биленчука. Киев : Атика, 1999. 272 с.

12. Білоусов А. С. Криміналістичний аналіз об’єктів комп’ютерних злочинів : дис... канд. юрид. наук : 12.00.09. Запоріжжя, 2008. 245 с.

13. Борисова Л. В. Транснаціональні комп’ютерні злочини як об’єкт криміналістичного дослідження : дис. … канд. юрид. наук : 12.00.09. Київ, 2007. 217 с.

14. Бранислав Трентовский и возникновеник кибернетики: из наследия Н. Н. Моисеева. *Экология и Жизнь*. 2007. № 8 (69). С. 15-19.

15. Бутузов В. М., Гавловський В. Д., Тітуніна К. В., Шеломенцев В. П. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток : наук.-практ. посіб. / за ред. І. В. Бондаренко. Київ, 2009. 182 с.

16. Вехов В. Б., Попова В. В., Илюшин Д. А. Тактические особенности расследования преступлений в сфере компьютерной информации : науч.-практ. пособие. 2-е изд., доп. и испр. М. : ЛексЭст, 2004. 160 с.

17. Взаємодія при розслідуванні економічних злочинів : монографія / [кол. авт.: А. Ф. Волобуєв, І. М. Осика, Р. Л. Степанюк та ін.] ; за заг. ред. А. Ф. Волобуєва. Харків : Курсор, 2009. 320 с.

18. Голубєв В. О., Гавловський В. Д., Цимбалюк В. С. Проблеми боротьби зі злочинами у сфері використання комп’ютерних технологій : навч посіб. / за ред. Р. А. Калюжного. Запоріжжя : ГУ ЗІДМУ, 2002. 292 с.

19. Дивак М. П. Системний аналіз : метод. посіб. Тернопіль, 2004. 136 с.

20. Динту В. А. Місце кіберпростору в системі обстановки злочину. *Науковий вісник Херсонського державного університету*. 2016. Вип. 2. Т. 3. С. 72-75

21. Журавель В. А. Криміналістичні методики: сучасні наукові концепції : монографія. Харків : Апостиль, 2012. 304 с.

22. Комп’ютерна злочинність : навч. посіб. / [П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін.]. Київ : Атіка, 2002. 240 с.
23. Криміналістика: підручник / [В. В. Пясковський, Ю. М. Чорноус, А. В. Іщенко та ін.]. Київ : Центр учб. літ., 2015. 544 с.
24. Криміналістика : підручник / [П. Д. Біленчук, В. К. Лисиченко, Н. І. Клименко та ін.] ; за ред. П. Д. Біленчука. 2-ге вид., випр. і доповн. Київ : Атіка, 2001. 544 с.
25. Криміналістика : підручник : у 2 т. / [В. Ю. Шепітько, В. А. Журавель, В. О. Коновалова та ін.] ; за ред. В. Ю. Шепітька. Харків : Право, 2019. Т. 1. 456 с.
26. Криминалистика : учебник / [Б. Е. Богданов и др.] ; отв ред. А. Н. Васильєв. М., 1971. 564 с.
27. Криміналістичне забезпечення виявлення і розслідування злочинів : монографія / [Л. І. Аркуша, О. Ю. Нетудихатка, О. О. Подобний та ін.] ; за ред. В. В. Тіщенка. Одеса : Гельветика, 2018. 412 с.
28. Протидія кіберзлочинності : бібліограф. покажчик літ. / уклад.: Н. А. Косенкова, Т. О. Сіродан. 2-е вид., доповн. Київ, 2014. 48 с.
29. Самойленко О.А. Основи методики розслідування злочинів, вчиненихуу кіберпросторі: монографія / О. А. Самойленко ; за заг. ред. А. Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с.
30. Самойленко О. А. Співвідношення термінів, що застосовуються для позначення злочинів, вчинених із використанням обстановки кіберпростору. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки»*. 2017. №5 С. 155-159.
31. Самойленко О. А. Криміналістична класифікації злочинів, вчинених з використанням обстановки кіберпростору. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2018. №49. С. 162-166.
32. Самойленко О. А. Концепція криміналістичної методики розслідування злочинів, вчинених з використанням обстановки кіберпростору. *Право та державне управління.* 2018. № 1. С. 208-213.

Питання заняття

1. Сутність поняття «кіберпростір».
2. Особливості кіберпростору, що привертають увагу злочинців до використання його середовища з метою досягнення злочинного результату.
3. Визначення основних технічних термінів, пов’язаних із кіберпростором: телекомунікаційна мережа, комп’ютерна мережа, інформаційні технології, електричний зв’язок, мережа зв’язку, мережа Інтернет.
4. Оцінки загроз кіберзлочинності національній безпеці держав та міжнародному порядку.
5. Класифікація кіберзлочинів в Європейської конвенції по боротьбі з кіберзлочинністю.
6. Криміналістичні класифікації кіберзлочинів.
7. Класифікація кіберзлочинів за кримінально-правовим критерієм, що

визначає нормативну суть класифікації, передбаченої законом України.

8. Сучасний стан дисертаційних розробок в сфері боротьби з кіберзлочинами.

9. Розроблені окремі криміналістичні методики розслідування кіберзлочинів.

10. Традиційна структура окремих криміналістичних методик розслідування кіберзлочинів.

Завдання для поточного контролю знань і вмінь здобувачів вищої освіти

1. Завдання. Розробити розгорнутий конспект для відповіді на питання за варіантами:

1.1. Особливості кіберпростору, що привертають увагу злочинців до використання його середовища з метою досягнення злочинного результату.

1.2. Сутність понять "комп'ютерний злочин", "кіберзлочин", "злочини у сфері ІТ- технологій" та "злочини у сфері комп'ютерної інформації". Теоретичні та нормативні позиції вказаних термінів в Україні та за кордоном.

1.3. Доктрина визначення сутності кіберзлочинів (обрати країну за своїм вибором).

1.4. Результати діяльності кіберполіції в Україні.

1.5. Кіберзагрози національній безпеці.

1.6. Кіберзагрози міжнародній безпеці.

1.7. Сучасний стан дисертаційних розробок в сфері боротьби з кіберзлочинами.

Методична порада: підчас оформлення письмового завдання враховувати, що питання є дискусійними, проблем криміналістики студенти можуть дотримуватися будь-якої позиції, але зобов'язані знати ту, яка відповідає змістові дисципліни. Для розуміння та кращого запам'ятовування того, що вивчається, корисно проводити порівняння 2-3 точок зору, викладених у підручниках, монографічних працях.

2. **Тестові завдання**. Метою проведення тестування є визначення рівня засвоєння викладеного матеріалу та перевірка вміння щодо практичного використання отриманих знань здобувачами вищої освіти.

Тестові питання передбачають обрання респондентом однієї правильної відповіді із запропонованих варіантів..

Тест 1. Конвенція Ради Європи про кіберзлочинність до прийняття Додаткового протоколу поділяє злочини на:

а) 2 групи;

б) 7 груп;

в) 10 груп;

г) 4 групи;

д) 5 груп.

Тест 2. Які групи злочинів не включає Конвенція Ради Європи про кіберзлочинність:

а) злочини, пов’язані з порушенням авторського права і суміжних прав;

б) злочини, пов’язані з контентом;

в) злочини, пов’язані з використанням комп’ютерних засобів;

г) поширення інформації расистського та іншого характеру, підбурює до насильницьких дій, ненависті чи дискримінації окремої особи або групи осіб;

д) злочини проти статевої свободи і недоторканості.

Тест 3. Які нормативні акти які безпосередньо визначають на цей час напрями регулювання інформаційних відносин в кіберпросторі України:

а) Закон України «Про інформацію»;

б) Закон України «Про захист інформації в автоматизованих системах»;

в) Закон України «Про електронний цифровий підпис»;

г) Кримінальний Кодекс України;

д) Закон України «Про національну програму інформатизації».

Тест 4. Кіберпростір як обстановка вчинення злочину характеризується наступними ознаками:

а) відсутністю кордонів;

б) динамікою розвитку;

в) анонімністю;

г) віртуальність;

д) комунікативність;

е) недосконаліть правової охорони відносин у кіберпросторі.

Тест 5. Загрози інформаційній безпеці в Україні не становлять:

а) ведення інформаційної війни проти України;

б) відсутність цілісної комунікативної політики держави;

в) недостатній рівень медіа-культури суспільства,

г) уразливість об’єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак;

д) оновленість системи охорони державної таємниці та інших видів інформації з обмеженим доступом

Заняття № 2
(денна форма навчання)

Тема 2. Організаційні та правові основи діяльності осіб у мережі Інтернет в Україні та за її межами

Мета вивчення

Сформувати та закріпити систему знань щодо особливостей реалізації та застосування норм матеріального і процесуального права стосовно відносин у традиційних сферах суспільного життя суб'єктів кіберпростору,

Результати навчання

Після практичного заняття здобувач вищої освіти буде (спроможний):

1) використовувати в правозастосовній діяльності нормативно-правові акти, що регулюють відносини, що виникають підчас виявлення та розслідування фактів вчинення злочинів у кіберпросторі;

2) оцінювати правові явища у кіберпросторі і застосовувати набуті знання у професійній діяльності юриста;

5) розуміти міжнародні стандарти прав людини як користувача кіберпростору, перспективи розвитку кіберпростору.

Література

нормативно-правові акти:

1. Бернська Конвенція про захист літературних та художніх творів (Паризький акт від 24 лип. 1971 р., змінений 2 жовт. 1979 р.) : міжнар. док. від 24 лип. 1971 р. URL: http://zakon3.rada.gov.ua/ laws/show/995_051/page

2. Договір між Кабінетом Міністрів України та Федеральним Урядом Республіки Австрія про співробітництво у сфері боротьби зі злочинністю : постанова Кабінету Міністрів від 17 лип. 2014 р. № 270. URL: http://zakon3.rada.gov.ua/laws/show/040_040

3. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Закон України від 21 лип. 2006 р. № 23-V. URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_687.

4. Додатковий протокол № 2 до Європейської Конвенції про взаємодопомогу у кримінальних справах від 20 квітня 1959 р. : міжнар. док. від 8 листоп. 2001 р. URL: http://zakon5.rada.gov.ua/laws/ show/994_518/page?text=%F2%E5%EB%E5%EA%EE%ECБіленький В. П. Відповідальність за кіберзлочини за кримінальним правом США,

Великобританії та України (порівняльно-правове дослідження) : дис. ... канд. юрид. наук : 12.00.08. Одеса, 2015. 230 с.

5. Європейської Конвенції про видачу правопорушників: міжнар. док. від 13 груд. 1957 р. URL: http://zakon3.rada.gov.ua/ laws/show/995_033.

6. Європейська Конвенція про захист прав людей та основоположних свобод : міжнар. док. від 4 листоп. 1950 р. URL: http://zakon5.rada.gov.ua/laws/show/995_004?nreg=995_004&find=1&text=%F1%EA%E0%F0&x=12&y=7#n150

7. Конвенції ООН проти транснаціональної організованої злочинності : міжнар. док. від 15 листоп. 2000 р. URL: http://zakon3.rada.gov.ua/ laws/show/995_789.

8. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : міжнар. док. від 28 січ. 1981 р. URL: http://zakon5.rada.gov.ua/laws/show/994_326.

9. Конвенція про кіберзлочинність : міжнар. док. від 23 листоп. 2001 р. URL: http://zakon3.rada.gov.ua/laws/show/994_575?nreg=994_575&find=1&text=%F7%E0%F1&x=0&y=4#w11.

10. Конвенція про права дитини : міжнар. док. від 20 листоп. 1989 р. (зі змінами, схваленими резолюцією 50/155 Генеральної Асамблеї ООН від 21 груд. 1995 р., Факультативні протоколи від 1 січ. 2000 р. та 2 листоп. 2014 р.). URL: http://zakon5.rada.gov.ua/ laws/show/995_021.

11. Міжнародна конвенція про ліквідацію всіх форм расової дискримінації : міжнар. док. від 4 січ. 1969 р. URL: куhttp://zakon3.rada.gov.ua/laws/show/995_105

12. Міжнародний пакт про громадянські й політичні права : міжнар. док. від 16 груд. 1966 р. URL: http://zakon3.rada.gov.ua/ laws/show/995_043

13. Угоди ВОІВ про авторське право за Міжнародною Конвенцією про захист виконавців, виробників фонограм і організацій мовлення (Римська конвенція): вчинено в Римі 26 жовт. 1961 р. URL: http://zakon3.rada.gov.ua/laws/show/995_763.

14. Угоди про торговельні аспекти прав інтелектуальної власності : міжнар. док. від 15 квіт. 1994 р. URL: http://zakon5.rada.gov.ua/laws/show/981_018.

спеціальна література:

15. Антонов В. М. Інтернет: енциклопедичне видання : навч.-метод. посіб. Київ : Комп'ютер, 2008. 128 с.

16. Бангкокська декларація про взаємодію і відповідні заходи: стратегічні союзи в галузі попередження злочинності і кримінального правосуддя : резолюція Генеральної Асамблеї ООН № 60/177, Додаток 1. URL: https://zakon3.rada.gov.ua/laws/show/995_785.

17. Батурин Ю. М. Проблемы компьютерного права. М. : Юрид. лит., 1991. 272 с.

18. Бауэр Ф. Л., Гооз Г. Информатика : в 2 ч. М., 1990. Ч. 1 : Вводный курс. 336 с.

19. Бачило И. Л. Информационное право: основы практической информатики : учеб. пособие. М. : Юринформцентр, 2001. 352 с.

20. Биленчук П. Д., Еркенов С. Е., Кофанов А. В. Транснациональная преступность: состояние и трансформация : учеб. пособие / под ред. П. Д. Биленчука. Киев : Атика, 1999. 272 с.

21. Бізнес расследование «Угроза с востока». URL: http://project.liga.net/projects/eastern_threat.

22. Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинністю. Запоріжжя : ЗІДМУ, 2003. 250 с.

23. Жаров В. О. Інтелектуальна власність в Україні: правові аспекти набуття, здійснення та захисту прав : монографія. Київ : Ін Юре, 2000. 188 с.

24. Информатика для гуманитариев : учебник / [Г. Е. Кедрова и др.]. М. : Юрайт, 2018. 439 с.

25. Карчевський М. В. Злочини у сфері використання комп'ютерної техніки : навч. посіб. Київ : Атіка, 2010. 168 с.Пастухов О. М. Авторське право в Інтернеті. Київ : Школа, 2004. 144 с.

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

27. Самойленко О. А. Інформаційний продукт як предмет посягання при вчиненні злочинів із використанням обстановки кіберпростору. *Вчені записки Таврійського університету імені В. І. Вернадського. Серія Юридичні науки*. 2018. Том 29(68). № 4. С. 165-169.

28. Самойленко О. А. Природа кіберпростору як об'єкта криміналістичного дослідження. *Криміналістика і судова експертиза*: міжвідом. наук.-метод.зб., присвяч. 105-річчю заснування судової експертизи в Україні / Київський НДІ судових експертиз; редкол.: О. Г. Рувін (голов. ред.) та ін. Київ : Видавництво Ліра-К, 2018. Вип. 63, ч. 1. С. 174-184.

29. Трунцевский Ю. В. Интеллектуальное пиратство: гражданско-правовые и уголовно-правовые меры противодействия. М. : Юрист, 2002. 148 с.

30. Узагальнення Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ «Про практику розгляду скарг на рішення, дії чи бездіяльність органів досудового розслідування чи прокурора під час досудового розслідування» (станом на 12.01.2017). URL: http://protokol.com.ua/ua/vssu_uzagalnennya_pro_praktiku_rozglyadu_skarg_na_rishennya_dii_chi_bezdiyalnist_organiv_dosudovogo_rozsliduvannya.

31. Чуприна О. Співвідношення понять «персональні дані», «інформація про особу», «конфіденційна інформація про особу». *Підприємство, господарство і право.* 2013. № 1. С. 104–108.

32. Шалева О. І. Електронна комерція : навч. посіб. Київ : Центр учб. літ., 2011. 216 с.

33. Шахбазян К. С. Міжнародно-правові основи регулювання відносин в мережі Інтернет : дис... канд. юрид. наук : 12.00.11. Київ, 2009. 222 с.

34. Шилін М. Національна безпека: проблеми правового забезпечення діяльності суб'єктів сектору безпеки та можливі шляхи вирішення. *Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку :* матеріали Міжнар. наук.-практ. конф. (Острог, 1 груд. 2017 р.) / за заг. ред. М. С. Романова. Острог : Нац. ун-т «Острозька академія», 2017. 180 с.

Питання заняття

1. Міжнародні організації, що здійснюють регулювання Інтернет та особливості їх діяльності:
2. Особливості організації національного сегменту кіберпростору.
3. Ключові суб'єкти ринку та організації телекомунікаційних послуг в Україні (суб'єкти взаємодії слідчого підчас розслідування кіберзлочинів).
4. Основи правового регулювання відносин в кіберпросторі. Особливості правового регулювання інформаційних відносин в кіберпросторі, відносин в кіберпросторі у сфері захисту прав та законних інтересів на об'єкти інтелектуальної власності.
5. Основи правового регулювання відносин у сфері електронної комерції.
6. Кримінально-правова охорона суспільних відносин у кіберпросторі в України. Конвенція Ради Європи про кіберзлочинність.
7. Характеристика інших міжнародних правових актів, які є частиною національного законодавства України, що регулюють правила та принципи охорони суб'єктів відносин у кіберпросторі.

Завдання для поточного контролю знань і вмінь здобувачів вищої освіти

1. **Завдання.** Розробити розгорнутий конспект для відповіді на питання за варіантами:

1.1. Проблема визначення юрисдикції мережі Інтернет.

1.2.Неурядові органі, що здійснюють регулювання відносин суб'єктів мережі Інтернет.

1.3. Основні галузі права для регулювання відносин у кіберпростір в Україні: проблема міжгалузевих питань.

1.4. Основи правового регулювання відносин у кіберпросторі в сфері незаконного наркообігу та торгівлі іншими товарами, що мають особливий порядок обігу в Україні та світі.

1.5. Перспективи розвитку проекту «Країна у смартфоні»?

1.6. Перспективи правового регулювання криптовалюти в Україні?

1.7. Правові основи діяльності осіб у кіберпросторі за межами України: США, Арабські країни (в аспекті порівняння).

Методична порада: підчас оформлення письмового завдання враховувати, що питання може мати дискусійні аспекти, студенти можуть дотримуватися будь-якої позиції, але зобов'язані посилатися на джерело інформації. Для розуміння та кращого запам'ятовування того, що вивчається,

корисно проводити порівняння 2-3 точок зору, викладених у підручниках, монографічних працях.

2. Тестові завдання. Метою проведення тестування є визначення рівня засвоєння викладеного матеріалу та перевірка вміння щодо практичного використання отриманих знань здобувачами вищої освіти

Тест 1. Якого злочину не передбачено в КК України?

а) шахрайство, вчинене з використанням електронно-обчислювальної техніки;

б) кіберзлочин;

в) підробку документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, а так само придбання, зберігання, перевезення, пересилання з метою збуту підроблених документів на переказ чи платіжних карток або їх використання чи збут;

г) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах;

д)перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

Тест 2. На скільки груп Конвенція Ради Європи про кіберзлочинність розділяє кіберзлочини?

а) не розділяє взагалі на групи;

б) 5 груп;

в) 7 груп;

г) 4 групи;

д) 2 групи.

Тест 3. Шахрайство в кіберпросторі, згідно Конвенції це?

а) це позбавлення іншої особи його власності шляхом будь-якого введення, зміни, видалення або блокування комп'ютерних даних або будь-якого втручання у функціонування комп'ютерної системи, з шахрайським або безчесним наміром неправомірного вилучення економічної вигоди для себе або третіх осіб;

б) це каране діяння, пов'язане з заволодінням чужим майном або придбання права на майно шляхом обману чи зловживання довірою;

в) не каране діяння, яке пов'язане з заволодінням чийогось майна шляхом придбання або зловживання довірою ;

г) Конвенція не передбачає чіткого визначення;

д) це діяння невідомої особи, яка за допомогою мережі Інтернет може увійти у іншу комп'ютерну систему.

Тест 4. Яку назву містить самостійний розділ XVI КК України:

а) злочини у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку та інтернету;

б) злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку;

в) злочини у сфері використання електронних машин та комп’ютерів, систем та комп’ютерних мереж і мереж електрозв’язку;

г) «злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та мереж електрозв’язку.

д) злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та мережі інтернет.

Тест 5. Як правильно називається підпис, який використовують в електронних документах?

а) електронний цифровий підпис ;

б) кваліфікований електронний підпис;

в) електронний підпис;

г) цифровий підпис;

д) електронно-цифровий підпис.

Заняття № 3
(денна форма навчання)

Тема 3. Організаційні засади виявлення та початку кримінального провадження щодо кіберзлочинів

Мета вивчення

Сформувати та закріпити систему знань щодо організаційних засад виявлення кіберзлочинів та відкриття кримінального провадження щодо такої категорії злочинів.

Результати навчання

Після практичного заняття здобувач вищої освіти буде (спроможний):

1) визначати належні та прийнятні для юридичного аналізу факти щодо сфери боротьби з кіберзлочинами;

2) використовувати в правозастосовній діяльності нормативно-правові акти, що регулюють відносини, що виникають підчас оперативно-розшукової діяльності щодо фактів вчинення злочинів у кіберпросторі, а також підчас відкриття кримінального провадження за такими фактами;

3) аналізувати правові та правозастосовчі проблеми, формувати та обґрунтовувати власну право застосовну позицію щодо виявлення та розслідування кіберзлочинів.

Література

нормативно-правові акти:

1. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14.

2. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/ laws/show/4651-17.

3. Інструкції про порядок ведення єдиного обліку в органах поліції заяв і повідомлень про вчинені кримінальні правопорушення та інші події : наказ МВС України від 6 листоп. 2015 р. за № 1377. URL: http://zakon.rada.gov.ua/laws/show/z1498-15.

4. Положення про порядок ведення Єдиного реєстру досудових розслідувань : наказ Генеральної прокуратури України від 17 серп. 2012 р. № 69 URL: http://zakon.rada.gov.ua/laws/show/z0680-16.

5. Про затвердження Порядку розгляду звернень та організації проведення особистого прийому громадян в органах та підрозділах Національної поліції України : наказ Міністерства внутрішніх справ України від 15 листоп. 2017 р.

№ 93. URL: http://zakon.rada.gov.ua/laws/show/z1493-17.

6. 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 МВС України від 07 лип. 2017 р. № 575. URL : https://zakon.rada.gov.ua/laws/show/z0937-17

7. Про звернення громадян : Закон України від 2 жовт. 1996 р. № 393/96-ВР. *Відомості Верховної Ради України.* 1996. № 47. Ст. 256.

спеціальна література:

8. Баев О. Я. О методических основах расследования насильственных преступлений. *Актуальные вопросы уголовного права, процесса и криминалистики* : сб. науч. тр. Калининград, 1998. 86 с. С. 74.

9. Бекетов М. Ю. Следователь органов внутренних дел и милиция: взаимодействие при расследовании преступлений : учеб. пособие. М. : Щит-М, 2004. 96 с.

10.Взаємодія при розслідуванні економічних злочинів : монографія / [кол. авт.: А. Ф. Волобуєв, І. М. Осика, Р. Л. Степанюк та ін.] ; за заг. ред. А. Ф. Волобуєва. Харків : Курсор, 2009. 320 с.

11.Волобуєв А. Ф. Наукові основи комплексної методики розслідування корисливих злочинів у сфері підприємництва : дис. … д-ра юрид. наук : 12.00.09. Харків, 2001. 426 с.

12.Волобуєв А. Ф. Проблемні питання початку досудового розслідування. *Актуальні проблеми кримінального права, процесу та криміналістики* : матеріали V Міжнар. наук.- практ. конф. (м. Одеса, 1 листоп. 2013 р.). Одеса : Фенікс, 2013. С. 237–240.

13.Иванов В. В. Методические рекомендации по совершенствованию взаимодействия следователя с оперативными подразделениями органов внутренних дел при раскрытии и расследовании преступлений. Чернигов, 1997. 34 с.

14.Криміналістика : навч. посібник / за ред. А. Ф. Волобуєва. Київ, 2011. 504 с.

15.Кудінов С.С., Шехавцов Р. М., Дроздов О. М., Гриненко С. О. Негласні слідчі (розшукові) дії та використання результатів оперативно-розшуової діяльності у кримінальному провадженні: навч.-практ. посіб. 3-е вид., розш. та допов. Х. : Оберіг, 2018. 540 с.

16.Озерський І. В. Взаємодія слідчого з органом дізнання (організаційно-правовий та психологічний аналіз) : монографія. Київ, 2004. 217 с.

17.Пивоваров В. В., Щербина Л. І. Взаємодія органів досудового слідства та дізнання при розслідуванні кримінальних справ : монографія. Харків : Право, 2006. 176 с.

18.Погорецький М. А., Кумичко А. С. Фактичні дані та їх значення для документування оперативними підрозділами злочинів у сфері рефінансування Національним банком України вітчизняних банків. *Вісник кримінального судочинства*. 2015. № 4. С. 54–62.

19. Самойленко О.А. Основи методики розслідування злочинів, вчиненихуу кіберпросторі: монографія / О. А. Самойленко ; за заг. ред. А. Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с.
20. Самойленко О. А. Початок кримінального провадження (з позицій криміналістичної науки. *Право і суспільство*. 2019. №2. С. 226-231.
21. Самойленко О. А. До питання оцінки слідчим матеріалів первинної перевірки оперативної інформації про злочин, вчинений у кіберпросторі. *Правові новели*. 2019. №7. С. 145-151.
22. Самойленко О. А. Відкриття кримінального провадження щодо злочинів, вчинених у кіберпросторі. *Підприємство, господарство і право*. 2019. №8. С. 222-225.
23. Щур Б. В. Теоретичні основи формування та застосування криміналістичних методик : дис. … д-ра юрид. наук : 12.00.09. Харків, 2011. 407 с.
24. Щур Б. В. Теоретичні основи формування та застосування криміналістичних методик : дис. … д-ра юрид. наук : 12.00.09. Харків, 2011. 407 с.

Питання заняття

1. Виявлення кіберзлочинів як напрямок правоохоронної діяльності. Типові джерела оперативної інформації про кіберзлочини.
2. Теоретичний аспект організації слідчим початку провадження та джерела обставин, що можуть свідчити про вчинення певного виду кіберзлочинів.
3. Форми початку кримінального провадження щодо кіберзлочинів.
4. Особливості перевірки інформації про кіберзлочини, що вчинені або готуються.
5. Зміст (наповнення) матеріалів первинної перевірки, які підлягають передачі керівникові органу досудового розслідування для внесення до ЄРДР інформації про кіберзлочин.
6. Відкриття кримінального провадження за заявою та повідомленням особи про кіберзлочин. Організаційні заходи слідчого для перевірки отриманої первинної від заявника інформації.

Завдання для поточного контролю знань і вмінь здобувачів вищої освіти

1. **Завдання.** Розробити розгорнутий конспект для відповіді на питання за варіантами:

1.1. Особливості виявлення кіберзлочинів, вчинених за участю службової особи або такої, яка здійснює професійну діяльність, пов’язану з наданням публічних послуг

1.2. Питання діяльності слідчо-оперативної групи (СОГ) підчас виявлення

та розслідування кіберзлочинів.

1.3. Особливості виявлення злочинів у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, вчинених із використанням обстановки кіберпростору.

1.4. Характеристика вихідної інформації, що є джерелом обставин про кримінальне правопорушення, вчинене ОЗГ із використанням кіберпростору.

1.5. Обставини, що підлягають обов'язковому встановленню підчас виявлення кіберзлочиінв, вчинених за участю службової особи або такої, яка здійснює професійну діяльність, пов'язану з наданням публічних послуг.

1.6. Альтернативні джерела інформації про особу та запропонуйте алгоритм встановлення інформації про пошуковий об'єкт з альтернативних джерел інформації.

Методична порада: підчас оформлення письмового завдання враховувати, що питання може мати дискусійні аспекти, студенти можуть дотримуватися будь-якої позиції, але зобов'язані посилатися на джерело інформації. Для розуміння та кращого запам'ятовування того, що вивчається, корисно проводити порівняння 2-3 точок зору, викладених у підручниках, монографічних працях.

1. **Тестові завдання**. Метою проведення тестування є визначення рівня засвоєння викладеного матеріалу та перевірка вміння щодо практичного використання отриманих знань здобувачами вищої освіти.

Тест 1. Оцініть наведені розуміння функцій суб'єктів оперативно-розшукової діяльності щодо виявлення кіберзлочинів та оберіть правильне:

а) підрозділи Департаменту кіберполіції (ДКП), уповноважені щодо протидії всім кримінальним правопорушенням, що вчинені у кіберпросторі (кіберзлочинам);

б) функції підрозділів контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, захисту національної державності Служби безпеки (ДКІБ СБ України) співпадають із функціями ДКП НП України;

в) підрозділи Департаменту кіберполіції (ДКП) уповноважені щодо протидії лише конвенційним кіберзлочинам;

г) всі оперативні підрозділи НП України вповноважені протидіяти кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

д) мета ріали про виявлений факт кіберзлочину може бути отриманий слідчим тільки з підрозділів ДКП.

Тест 2. Проаналізуйте наведене твердження і вкажіть, яка частина, що робить його правильним, пропущена: «Правові чинники, що зумовлюють форми початку кримінального провадження, пов'язані з...

а) передбаченими інструкціями повноваженнями оперативних підрозділів»;

б) характером джерела обставин, що можуть свідчити про вчинення певного виду кримінального правопорушення»;

в) характером матеріалів, що спрямовані до правоохоронного органу”;

г) взаємодією слідчого та оперативного підрозділу»;

д) конфіденційністю джерел оперативно-розшукової інформації».

Тест 3. Поясніть у яку форму буде розпочато кримінальне провадження за умови надання державним контролювальним органом до правоохоронного органу матеріалів, що містять дані про ознаки злочину**:**

а) безальтернативна форма початку провадження;

б) альтернативна форма початку провадження;

в) безініціативна форма початку провадження;

г) ініціативна форма початку провадження;

д) у будь-яку форму, яку обере керівник слідчого підрозділу.

Тест 4. Назвіть захід, який не можна проводити підчас документування злочинної діяльності у кіберпросторі на етапі оперативно-розшукової діяльності:

а) аудіо-, відеоконтроль особи;

б) зняття інформації з транспортних телекомунікаційних мереж, електронних інформаційних мереж;

в) накладати арешт на кореспонденцію, здійснювати її огляд та виїмку;

г) виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації;

д) здійснювати установлення місцезнаходження радіоелектронного засобу;

е) аудіо-, відео контроль місця.

Тест 5. Із запитом до провайдера не можна звернутися з метою отримання:

а) реєстраційні дані (logs) та абонентську інформацію про особу, якій надаються послуги хостингу для сайта;

б) адреси, телефонні номери та інші реквізити власника сайта;

в) змісту повідомлень електронної поштової скриньки;

г) IP-адреси, використані для створення сайта та його поповнення;

д) інформація про зміст сайта; інформація про користування сайтом.

Заняття № 4
(денна форма навчання)

Тема 4. Використання спеціальних знань під час розслідування кіберзлочинів

Мета вивчення

Сформувати та закріпити систему знань щодо організаційних засад виявлення та розслідування кіберзлочинів.

Результати навчання

Після практичного заняття здобувач вищої освіти буде (спроможний):

1) визначати належні та прийнятні для юридичного аналізу факти щодо сфери боротьби з кіберзлочинами;

2) застосувати сучасні інформаційні технології та інформаційні ресурси за для розв'язання практичних задач щодо організації розслідування кіберзлочинів;

3) використовувати в правозастосовній діяльності нормативно-правові акти, що регулюють відносини, що виникають підчас використання спеціальних знань та призначення судових експертиз в процесі розслудвання злочинів у кіберпросторі, а також підчас збирання матеріалів попередньої перевірки за такими фактами;

4) аналізувати правові та правозастосовчі проблеми, формувати та обґрунтовувати власну право застосовну позицію в межах питань залучення спеціаліста та експерат в процес розслідування кіберзлочинів.

Література

нормативно-правові акти:

1. 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 МВС України від 07 лип. 2017 р. № 575. URL : https://zakon.rada.gov.ua/laws/show/z0937-17.

2. Про затвердження Інструкції з організації проведення та оформлення експертних проваджень у підрозділах Експертної служби Міністерства внутрішніх справ України : наказ МВС України від 17 лип. 2017 р. № 591. URL: https://zakon.rada.gov.ua/laws/show/z1024-17?find=1&text=%F1%F2%F0%EE%EA#w12.

3. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ ГП України, МВС України, СБ України, Адміністрації державної прикордонної служби України, Міністерства Фінансів України, Міністерства юстиції України від 16 лист. 2012 р. № 114/1042/516/1199/936/1687/5.

URL: https://zakon2.rada.gov.ua/laws/show/v0114900-12.

4. 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 3 листоп. 2015 р. № 1339. URL: https://zakon.rada.gov.ua/laws/show/z1392-15?find=1&text=%F1%E5%EA%F2%EE%F0#w11.

5. 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 8 жовт. 1998 р. № 53/5.

URL: https://zakon.rada.gov.ua/laws/show/z0705-98?find=1&text=%EA%EE%EC%EF%27%FE%F2%E5%F0#w110.

6. Про затвердження Інструкції про участь співробітників та працівників Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України як спеціалістів в кримінальному провадженні : наказ СБ України від 19 берез. 2016 р. № 138. URL: https://zakon.rada.gov.ua/laws/show/z0564-16?lang=ru

7. Про затвердження Положення про Експертну службу Міністерства внутрішніх справ України : наказ МВС України від 9 серп. 2012 р. № 691 (втратив чинність на підставі наказу МВС України від 3 листоп. 2015 р. № 1343). URL: https://zakon.rada.gov.ua/laws/show/z1541-12.

8. Про затвердження Положення про Експертну службу Міністерства внутрішніх справ України : наказ МВС України від 3 листоп. 2015 р. № 1343. URL: https://zakon.rada.gov.ua/laws/show/z1390-15

спеціальна література:

9. Білоусов А. С. Криміналістичний аналіз об’єктів комп’ютерних злочинів : дис... канд. юрид. наук : 12.00.09. Запоріжжя, 2008. 245 с.

10. Бобрицький С. М. Методичні аспекти дослідження телекомунікаційних систем (обладнання) та засобів. *Теорія та практика судової експертизи і криміналістики.* 2008. Вип. 8. С. 445–449.

11. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / [М. В. Гребенюк, В. Д. Гавловський, М. В. Гуцалюк та ін.] ; за заг. ред. М. В. Гребенюка. Київ : МНДЦ при РНБО України, 2017. 77 с.

12. Воробей О. В. Використання спеціальних знань і призначення окремих видів судових експертиз під час розслідування кримінальних правопорушень,

пов’язаних з діяльністю конвертаційних центрів. *Криміналістичний вісник.* 2017. № 1 (27). С. 154–160.

13. Воробієнко П. П., Нікітюк Л. А., Резніченко П. І. Телекомунікаційні та інформаційні мережі : підручник. Київ : Саммит-Книга, 2010. 708 с.

14. Гончаренко В. И. Использование данных естественных и технических наук в уголовном судопроизводстве. Киев : Вища шк., 1980. 160 с.

15. Грамович Г. И. Тактика использования специальных знаний в раскрытии и расследовании преступлений : учеб. пособие. Минск : Минск. высш. шк. МВД СССР, 1987. 66 с

16. Дослідження інформації в пам’яті терміналів стільникового зв’язку : звіт НДР (заключ.) / ЛНДІСЕ ; наук. кер. Ю. С. Харабуга. Львів : ЛНДІСЕ, 2011. 65 с. № держ. реєстрації 0110U002599.

17. Ківалов С. В., Міщенко С. М., Захарченко В. Ю. Кримінальний процесуальний кодекс : наук.-практ. комент. Харків : Одіссей, 2013. 1104 с.

18. Коваленко Е. Г. Использование экспертных знаний в деятельности органов внутренних дел : учеб. пособие. Киев : Киев. высш. шк. МВД СССР им. Ф. Э. Дзержинского, 1990. 87 с.

19. Кудінов С. С. Використання спеціальних знань під час проведення негласних слідчих (розшукових) дій. *Вісник Академії адвокатури України.* 2014. Т. 11. № 3 (31). С. 154–161.

20. Кудінов С.С., Шехавцов Р. М., Дроздов О. М., Гриненко С. О. Негласні слідчі (розшукові) дії та використання результатів оперативно-розшуової діяльності у кримінальному провадженні: навч.-практ. посіб. 3-е вид., розш. та допов. Х. : Оберіг, 2018. 540 с.

21. Лисиченко В. К. Использование данных естественных и технических наук в следственной и судебной практике : учеб. пособие. Киев : Вища шк., 1979. 89 с.

22. Лисиченко В. К., Циркаль В. В. Использование специальных знаний в следственной и судебной практике : учеб. пособие. Киев : КГУ, 1987. 100 с.

23. Романюк Ю. В. Сучасні теоретичні та правові проблеми використання спеціальних знань у досудовому слідстві : дис. … канд. юрид. наук : 12.00.09. Київ, 2002. 217 с.

24. Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. М. : Право и закон, 2001. 411 с.

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

26. Самойленко О. А., Паляничко Д. Г., Маланюк О. В., Ващенко І. О. Інформаційні сліди в контексті механізму вчинення злочинів із використанням обстановки кіберпростору. Криміналістика та судова експертологія : наука, навчання, практика: матеріали 14 міжнародного Конгресу, м. Одеса, 13-15 вересня. У 2-х томах. Одеса: Гельветика, 2018. Т.2. 544 с. С. 216-222 (у співавторстві).

27. Самойленко Е. А. Психологическая характеристика пользователя компьютера как критерий для типизации преступника, действующего в

киберпространстве (криминалистический аспект). Тактика и методика расследования преступлений: теория, практика, инновации : материалы круглого стола с международным участием, 15 ноября 2018 г., Минск, Беларусь / БГУ, Юридический фак., Каф. криминалистики ; [редкол.: В. Б. Шабанов (отв. ред.) и др.]. Минск : БГУ, 2018. 182 с. С. 123-126.

28. Самойленко О. А. Види злочинних спільнот, що вчиняють кримінальні правопорушення з використанням кіберпростору. Сучасні напрями, засоби та методи протидії злочинності : матеріали Міжнародної конференції, присвяченої 105-річчю від дня народження видатного вченого-криміналіста, доктора юридичних наук, професора Віктора Павловича Колмакова (23 листопада 2018 року) / відп. за вип. проф. Тіщенко В. В., доц. Гресь Ю. О. Одеса : Видавничий дім «Гельветика», 2018. 226 с. С. 154-157.

29. Самойленко О. А. Титуніна К. В. До питання криміналістичної характеристики особи злочинця, що використовує кіберпростір. Актуальні питання протидії кіберзлочинності та торгівлі людьми (23 листоп. 2018 р., м. Харків) / МВС України, Харків, нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2018 436 с. С. 429-432 (у співавторстві).

30. Степанов Ю. В. Використання комп'ютерних засобів для відновлення інформації, яка становить інтерес у ході оперативної розробки. *Вісник Львівського державного університету внутрішніх спарв ім. Е. О. Дідоренка.* 2008. Спецвипуск. № 1. Ч. 1. С. 180–185.

31. Стецик Б.В. Особливості тактичних, процесуальних та організаційних засад підготовки, призначення та проведення судовов-подчеркознавчої експертизи. *Науковий вісник Львівської комерційної академії. Серія : Юридична*. 2015. Вип. 1. С. 246-260.

32. Теплицький Б. В., Шарай Л. Г., Ковальов К. М., Кузьмін С. А. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : наук.-практ. посіб. Київ : Паливода А. В., 2019. 168 с.

33. Щербаковський М.Г. Призначення та провадження судових експертиз. Харків : Фактор, 2011. 400 с.

34. Яремчук В. О. Організація і тактика залучення спеціаліста при проведенні слідчих (розшукових) дій : монографія / за ред. В. Ю. Шепітька. Харків : Апостіль, 2015. 227 с.

Питання заняття

1. Спеціальні знання під час розслідування кіберзлочинів.

2. Організаційні і тактичні особливості залучення спеціаліста для надання письмової та усної консультації підчас розслідування кіберзлочинів.

3. Назвіть організаційні і тактичні особливості залучення спеціаліста для надання безпосередньої техніко-криміналістичної та іншої технічної допомоги підчас слідчих (розшукових) та негласних слідчих (розшукових) дій.

4. Залучення експерта підчас розслідування кіберзлочинів для проведення судової комп'ютерно-технічної експертизи.

5. Залучення підчас розслідування кіберзлочинів експерта для проведення

експертиза телекомунікаційних систем (обладнання) та засобів.

6. Залучення експерта для комплексних судових експертиз підчас розслідування кіберзлочинів (КТЕ та експертизи відео звукозапису; КТЕ і ТЕД).

Завдання для поточного контролю знань і вмінь здобувачів вищої освіти

1. **Завдання.** Розробити розгорнутий конспект для відповіді на питання за варіантами:

1.1. Залучення спеціаліста підчас проведення слідчих (розшукових) дій у справах про кіберзлочини, вчинені у сфері незаконного обігу наркотиків.

1.2. Особливості призначення та проведення технічної експертиза документів при розслідуванні кіберзлочинів.

1.3. Особливості призначення та проведення експертизи телекомунікаційних систем (обладнання) та засобів при розслідуванні кіберзлочинів

1.4. Особливості призначення та проведення експертиза у сфері інтелектуальної власності. при розслідуванні кіберзлочинів.

1.5. Особливості призначення та проведення лінгвістичної експертизи мовлення (семантико-текстуальний аналіз писемного й усного мовлення) при розслідуванні кіберзлочинів.

1.6. Особливості призначення та проведення судово-бухгалтерської експертизи.

1.7. Особливості призначення та проведення психологічної експертизи при розслідуванні кіберзлочинів.

1.8. Особливості призначення та проведення мистецтвознавчої експертизи при розслідуванні кіберзлочинів.

Методична порада: підчас оформлення письмового завдання враховувати положення Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень.

2. **Тестові завдання**. Метою проведення тестування є визначення рівня засвоєння викладеного матеріалу та перевірка вміння щодо практичного використання отриманих знань здобувачами вищої освіти.

Тест 1. Які є процесуальні форми використання спеціальних знань під час досудового розслідування?

а) залучення спеціаліста для письмової консультації, безпосередньої технічної допомоги;

б) залучення спеціаліста для письмової консультації, безпосередньої технічної допомоги судової експертизи й виконання обов’язків судового експерта;

в) залучення спеціаліста для усного консультування та письмової консультації;

г) залучення спеціаліста для безпосередньої технічної допомоги під час процесуальних дій;

д) залучення спеціаліста для проведення судової експертизи й виконання обов'язків судового експерта.

Тест 2. Комп'ютерно-технічна експертиза – це

а) одна з різновидів судових експертиз, об'єктом якої є комп'ютерна техніка та (або) комп'ютерні носії інформації, а метою — пошук особи;

б) одна з різновидів судових експертиз, об'єктом якої є пошук і закріплення доказів;

в) одна з різновидів судових експертиз, об'єктом якої є комп'ютерна техніка та (або) комп'ютерні носії інформації;

г) одна з різновидів судових експертиз, об'єктом якої є комп'ютерна техніка та (або) комп'ютерні носії інформації, а метою — пошук і закріплення доказів;

д) одна з різновидів судових експертиз, об'єктом якої є техніка та (або) комп'ютерні носії інформації, а метою — пошук і закріплення доказів;

Тест 3. Відповідно до ст. 71 КПК України, спеціаліст залучається під час проведення процесуальної дії для:

а) фотографування, складення схем, планів, креслень, відбору зразків для проведення експертизи;

б) дослідження, пов'язані з комерційними (фірмовими) найменуваннями, торговельними марками (знаками для товарів і послуг), географічними зазначеннями;

в) дослідження, пов'язані з комерційними (фірмовими) найменуваннями, торговельними марками (знаками для товарів і послуг), географічними зазначеннями

г) фотографування, планів, креслень, відбору зразків для проведення експертизи;

д) фотографування, складення схем, планів, креслень.

Тест 4. Завдання комп'ютерно-мережевої експертизи:

а) виявлення властивостей і характеристик обчислювальної мережі, встановлення її архітектури, конфігурації, виявлення встановлених мережевих компонент, організація доступу до даних;

б) дослідження документів бухгалтерського обліку і звітності

в) дослідження, пов'язані з охороною прав на конфіденційну інформацію;

г) дослідження документів про фінансово-кредитні операції;

д) економічні дослідження, пов'язані з використанням прав на об'єкти інтелектуальної власності.

Тест 5. Спеціаліст з інформаційних технологій та/або електроніки й телекомунікацій, що залучається під час проведення процесуальних дій, нині є штатним працівником:

а) СБУ;

б) органів доходів і зборів;

в) кіберполіції;

г) Міністерства надзвичайних справ;

д) Міністерства юстиції.

Заняття№ 5
(денна форма навчання)

Заняття № 2
(заочна форма навчання)

Тема 5. Організаційно-тактичні основи розслідування кіберзлочинів

Мета вивчення

Сформувати та закріпити систему знань щодо організаційно-тактичні засад розслідування кіберзлочинів.

Результати навчання

Після практичного заняття здобувач вищої освіти буде (спроможний):

1) визначати належні та прийнятні для юридичного аналізу факти щодо сфери боротьби з кіберзлочинами;

2) застосувати сучасні інформаційні технології та інформаційні ресурси за для розв'язання практичних задач щодо організації розслідування кіберзлочинів;

3) використовувати в професійній юридичній діяльності основні техніко-криміналістичні засоби, прийоми і методи розслідування;

5) проводити слідчі (розшукові) дії, тактичні операції, взаємодіяти з працівниками оперативних підрозділів;

6) аналізувати правові та правозастосовчі проблеми, формувати та обґрунтовувати власну правозастосовну підчас здійснення або участі в слідчих (розшукових) діях в ході розслідування злочинів, вчинених у кіберпросторі.

Література

нормативно-правові акти:

1. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/ laws/show/4651-17.

2. 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 МВС України від 07 лип. 2017 р. № 575. URL : https://zakon.rada.gov.ua/laws/show/z0937-17.

3. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ ГП України, МВС України, СБ України, Адміністрації

державної прикордонної служби України, Міністерства Фінансів України, Міністерства юстиції України від 16 лист. 2012 р. № 114/1042/516/1199/936/1687/5. URL: https://zakon2.rada.gov.ua/laws/show/v0114900-12.

4. Про оперативно-розшукову діяльність: Закон України від 18 лют. 1992 р. № 2135-XII URL: https://zakon.rada.gov.ua/laws/show/2135-12.

5. Про організацію діяльності органів досудового розслідування Національної поліції України : наказ МВС України від 6 лип. 2017 р. № 570. URL:https://zakon.rada.gov.ua/laws/show/z0918-17?find=1&text=%EA%F0%E8%EC%B3%ED %E0%EB%B3%F1%F2#w136.

6. Про основи національної безпеки України : Закон України від 19 черв. 2003 р. № 964-IV. URL: http://zakon2.rada.gov.ua/ laws/show/964-15.

7. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

спеціальна література:

8. Бутузов В. М., Гавловський В. Д., Тітуніна К. В., Шеломенцев В. П. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток : наук.-практ. посіб. / за ред. І. В. Бондаренко. Київ, 2009. 182 с.

9. Васильев В. Л. Юридическая психология : учеб. пособие. 5-е изд., доп. и перераб. СПб. : Питер, 2005. 655 с.

10. Вехов В. Б., Попова В. В., Илюшин Д. А. Тактические особенности расследования преступлений в сфере компьютерной информации : науч.-практ. пособие. 2-е изд., доп. и испр. М. : ЛексЭст, 2004. 160 с.

11. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / [М. В. Гребенюк, В. Д. Гавловський, М. В. Гуцалюк та ін.] ; за заг. ред. М. В. Гребенюка. Київ : МНДЦ при РНБО України, 2017. 77 с.

12. Грібов М. Л. Розмежування спеціального слідчого експерименту й іметування обстановки злочину. *Науковий вісник Національної академії внутрішніх спр*ав. 2016. № 4 (101). С. 64–73.

13. Захарова І. В., Філіпова Л. Я. Основи інформаційно-аналітичної діяльності : навч. посіб. Київ : Центр учб. літ., 2013. 335 с.

14. Ковальчук С. О. Вчення про речові докази у кримінальному процесі: теоретико-правові та практичні основи : монографія. Івано-Франківськ : Супрун В. П., 2017. 618 с.

15. Коновалова В. О., Шепітько В. Ю. Юридична психологія : підручник. 2-ге вид., переробл. і доповн. Харків : Право, 2008. 240 с.

16. Криміналістичне забезпечення виявлення і розслідування злочинів : монографія / [Л. І. Аркуша, О. Ю. Нетудихатка, О. О. Подобний та ін.] ; за ред. В. В. Тіщенка. Одеса : Гельветика, 2018. 412 с.

17. Кудінов С.С., Шехавцов Р. М., Дроздов О. М., Гриненко С. О. Негласні слідчі (розшукові) дії та використання результатів оперативно-

розшуової діяльності у кримінальному провадженні: навч.-практ. посіб. 3-е вид., розш. та допов. Х. : Оберіг, 2018. 540 с.

18. Кузьмін С. А. Комп'ютерна (кібернетична) інформація як предмет вчинення злочину (кримінально-правовий аспект). *Інформація і право.* 2012. № 3 (6). С. 159–163.

19. Кузьмічов В. С., Чорноус Ю. М. Розслідування злочинів: міжнародне і національне законодавство. *Теорія і практика :* навч. посіб. Київ : КНТ, 2008. 448 с.

20. Лисенко В. В. Використання у доказовому процесі інформації, що міститься в електронному вигляді. Організація протидії злочинам у сфері інтелектуальної власності та комп'ютерних технологій: доповіді провідних вчених, представників громадськості, державних службовців та працівників підрозділів ДСБЕЗ на міжвідомчому семінарі-нараді / відп. ред. Л. П. Скалозуб, В. І. Василинчук, С. А. Лебідь. Київ, 2009. 114 с.

21. Лукашевич В. Г. Криминалистическая теория общения: постановка проблемы, методика исследования, перспективы использования: монографія. К. : Издательство Украинской академии внутренних дел, 1993. 194 с.

22. Лук'янчиков Є. Д. Інформаційне забезпечення розслідування злочинів (правові і тактико-криміналістичні аспекти) : дис. … д-ра юрид. наук : 12.00.09. Київ, 2005. 430 с.

23. Михальчук Т. В. Використання інформації, отриманої телекомунікаційним шляхом, у розслідуванні злочинів : дис. … канд. юрид. наук : 12.00.09. Київ, 2009. 222 с.

24. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій : навч. посіб. / [В. М. Бутузов, В. Д. Павловський, Л. П. Скалозуб та ін.] ; за ред. Б. В. Романюка, Є. Д. Скулиша. Київ, 2011. 404 с.

25. Погорецький М. А., Кумичко А. С. Фактичні дані та їх значення для документування оперативними підрозділами злочинів у сфері рефінансування Національним банком України вітчизняних банків. *Вісник кримінального судочинства*. 2015. № 4. С. 54–62.

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

27. Самойленко О. А. Типові ситуації наступного етапу розслідування злочинів, скоєних у кіберпросторі. *Актуальні проблеми держави і права.* 2019. Вип. 82. С. 188-194.

28. Самойленко О. А. Типові слідчі ситуації початкового етапу розслідування злочинів, вчинених у кіберпросторі. *Наукові праці Національного університету «Одеська юридична академія».* 2019. Том 23. С. 121-128.

29. Тарасюк А. В. Доказування у справах про несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку у стадії досудового розслідування : монографія. Харків : ФІНН, 2011. 192 с.

30. Шевчук В. М. Тактичні операції у криміналістиці: теоретичні засади формування та тактика реалізації : монографія Харків : Апостіль, 2013. 440 с.
31. Шепітько В. Ю. Допит : наук.-практ. посіб. Харків : Крим-Арт, 1998. 214 с.
32. Шепитько В. Ю. Тактика расследования преступлений, совершаемых организованными группами и преступными организациями. Харьков, 2000. 88 с.

Питання заняття

1. Типові слідчі ситуації початкового та наступного етапів розслідування кіберзлочинів.
2. Типові тактичні операції розслідування кіберзлочинів та їх зв'язок із типовими слідчими ситуаціями, внутрішня структура кожної операції.
3. Ознаки інформації в електронній формі (електронних даних або документів (виходячи зі змісту положень КПК України), що мають значення для тактики провадження окремих слідчих (розшукових) дій у справах про кіберзлочини.
4. Загальні положення тактики підготовки до проведення слідчих дій, спрямованих на збирання інформації в електронній формі.
5. Тактичні правила та рекомендації, спрямовані на пошук інформації в електронній формі підчас слідчого огляду, обшуку.
6. Тактичні правила та рекомендації, спрямовані на фіксацію та вилучення інформації в електронній формі підчас слідчого огляду, обшуку або тимчасового доступу до речей та документів.
7. Тактичні рекомендації, спрямовані на вилучення інформації в електронній формі підчас слідчого огляду, обшуку або тимчасового доступу до речей та документів.
8. Особливості вилучення мобільних пристроїв.
9. Особливості допиту свідка, потерпілого, підозрюваного у справах про кіберзлочин.
10. Загальні тактичні особливості проведення зняття інформації з транспортних телекомунікаційних мереж, зняття інформації з електронних інформаційних систем; установлення місцезнаходження радіоелектронного засобу підчас розслідування кіберзлочинів.
11. Загальні тактичні особливості проведення контролю за вчиненням злочину підчас розслідування кіберзлочинів.

Завдання для поточного контролю знань і вмінь здобувачів вищої освіти

1. **Завдання.** Розробити розгорнутий конспект для відповіді на питання за варіантами:

1.1. Тактика проведення слідчого огляду підчас розслідування кіберзлочинів: огляд місця події, предметів (носіїв електронної інформації; документів).

1.2. Тактика проведення обшуку підчас розслідування кіберзлочинів.

1.3. Особливості тактики проведення негласних слідчих (розшукових) дій.

1.4. Типові тактичні операції, що містять негласні слідчі (розшукові) дії.

1.5. Тактика допиту підозрюваних осіб підчас розслідування кіберзлочинів. Подолання протидії розслідуванню.

Методична порада: підчас оформлення письмового завдання враховувати, що питання може мати дискусійні аспекти, студенти можуть дотримуватися будь-якої позиції, але зобов'язані посилатися на джерело інформації. Для розуміння та кращого запам'ятовування того, що вивчається, корисно проводити порівняння 2-3 точок зору, викладених у підручниках, монографічних працях.

2. **Тестові завдання**. Метою проведення тестування є визначення рівня засвоєння викладеного матеріалу та перевірка вміння щодо практичного використання отриманих знань здобувачами вищої освіти.

Тест 1. Поясніть, що мається на увазі, коли ведуть мову про слідчу ситуацію розслідування кіберзлочинів, що характеризується наявністю неперсоналізованих відомостей про користувача як імовірного злочинця

а) є відомості про особу злочинця, які прямо вказують на його персональні дані;

б) немає жожних відомостей про особу злочинця;

в) є відомості про IP-адресу користувача-злочинця та його спільника;

г) є відомості про користувача веб-сторінки соціальної мережі, дошці оголошень, дані абонентського номеру користувача, його IP-адреси, MAC-адреси обладнання, що використовувалось при вчиненні або готуванні кіберзлочинів;

д) є відомості про IP-адресу, MAC-адресу обладнання, що використовувалось при вчиненні або готуванні кіберзлочинів.

Тест 2. Тактична операція «Встановлення кінцевого мотиву злочинної діяльності в кіберпросторі» має наступні складові:

а) зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи непов'язаний з подоланням системи логічного захисту; встановлення місцезнаходження радіоелектронного засобу;

б) зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача; контроль за вчиненням злочину у формі спеціального слідчого експерименту;

в) контроль за вчиненням злочину у формі контрольованої поставки чи закупки; допит свідка; обшук чи тимчасовий доступ до речей та документів;

г) не має чіткого переліку слідчих (розшукових) дій;

д) контроль за вчиненням злочину як обов'язкова складова цієї операції; інші слідчі (розшукові) дії.

Тест 3. Назвіть необов'язкові з точки зору криміналістичної тактики дії в алгоритмі огляду віддаленого ресурсу комп'ютерної мережі :

а) запустити браузер та ввести доменне ім'я (інший прийнятний ідентифікатор) віддаленого ресурсу та здійснити огляд змісту сайта чи іншого ресурсу;

б) продемонструвати учасникам слідчої дії зміст та місцезнаходження (шлях розміщення) всіх файлів на віддаленому ресурсі, які виявлені слідчим або оперуповноваженим підчас огляду;

в) застосувати програмні засоби для встановлення IP-адреси сайта (ping), шляху проходження пакетів при обміні інформацією з ним, скопіювати їх на носій, призначений для запису та зберігання доказової інформації;

г) скопіювати файли з відеограмою та скриншотами зображення екрана монітора, створеними під час огляду, та зберегти їх на носієві, призначеному для запису та зберігання доказової інформації, в окремому каталозі;

д) встановити контрольну суму кожного файла (з інформацією, що стосується справи), зафіксованого на носієві, призначеному для запису та зберігання доказової інформації, зберігаючи при цьому дані про контрольну суму в окремих файлах.

Тест 4. Оцініть правильність вислову: «Після закінчення слідчої дії, спрямованої на збирання інформації в електронному вигляді НЕ обов'язковим є долучення до протоколу слідчої дії:

а) робочих примірників усіх програмних засобів, а також даних, що вміщують доказову інформацію;

б) контрольного примірнику програмного засобу, що використаний для виявлення, копіювання і записування досліджуваних даних на інший носій, а також контрольний примірник файла – еталона;

б) контрольного примірнику носія, що містить файли з доказовою інформацією;

в) безпосередньо самого носія, що був об'єктом огляду;

г) пластикові картки, що зберігалися на місці проведення слідчої (розшукової) дії.

Тест 5. Носій електронної інформації, що був предметом пошуку підчас обшуку вилучається та вважається тимчасово вилученим майном у разі якщо:

а) наявні специфічні сліди, які потребують дослідження в лабораторних умовах;

б) це предмет злочину;

в) це знаряддя вчинення злочину;

г) в будь-якому разі вилучається;

д) не вилучається в жодному разі.

Заняття № 6
(денна форма навчання)

Тема 6. Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі

Мета вивчення

Сформувати та закріпити систему знань щодо методики розслідування кіберзлочинів вчинених з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі

Результати навчання

Після практичного заняття здобувач вищої освіти буде (спроможний):

1) визначати належні та прийнятні для юридичного аналізу факти щодо сфери боротьби з кіберзлочинами;

2) застосувати сучасні інформаційні технології та інформаційні ресурси за для розв'язання практичних задач щодо організації та планування розслідування кіберзлочинів, що вчиняються с корисливих мотивів;

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

Література

нормативно-правові акти:

1. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14.
2. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/ laws/show/4651-17.
3. Про оперативно-розшукову діяльність: Закон України від 18 лют. 1992 р. № 2135-XII URL: https://zakon.rada.gov.ua/laws/show/2135-12
4. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.
5. Інструкції про порядок ведення єдиного обліку в органах поліції заяв і повідомлень про вчинені кримінальні правопорушення та інші події : наказ МВС України від 6 листоп. 2015 р. за № 1377. URL: http://zakon.rada.gov.ua/laws/show/z1498-15.

6. Положення про порядок ведення Єдиного реєстру досудових розслідувань : наказ Генеральної прокуратури України від 17 серп. 2012 р. № 69 URL: http://zakon.rada.gov.ua/laws/show/z0680-16.

7. Про затвердження Порядку розгляду звернень та організації проведення особистого прийому громадян в органах та підрозділах Національної поліції України : наказ Міністерства внутрішніх справ України від 15 листоп. 2017 р. № 93. URL: http://zakon.rada.gov.ua/laws/show/z1493-17.

8. 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 МВС України від 07 лип. 2017 р. № 575. URL : https://zakon.rada.gov.ua/laws/show/z0937-17

9. 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 МВС України від 07 лип. 2017 р. № 575. URL : https://zakon.rada.gov.ua/laws/show/z0937-17.

10. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ ГП України, МВС України, СБ України, Адміністрації державної прикордонної служби України, Міністерства Фінансів України, Міністерства юстиції України від 16 лист. 2012 р. № 114/1042/516/1199/936/1687/5. URL: https://zakon2.rada.gov.ua/laws/show/v0114900-12.

спеціальна література:

11. Анапольська А. І. Розслідування шахрайств, пов’язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків : дис. ... канд. юрид. наук : 12.00.09. Луганськ, 2008. 225 с.

12. Аркуша Л. І. Основи виялення та розслідування легалізації доходів, одержаних в результаті організованої злочинної діяльності: Интернет : дис. … д-ра юрид. наук : 12.00.09. Одеса, 2011. 496 с.

13. Борисова Л. В. Транснаціональні комп’ютерні злочини як об’єкт криміналістичного дослідження : дис. … канд. юрид. наук : 12.00.09. Київ, 2007. 217 с.

14. Бутузов В. М., Гавловський В. Д., Тітуніна К. В., Шеломенцев В. П. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток : наук.-практ. посіб. / за ред. І. В. Бондаренко. Київ, 2009. 182 с.

15. Взаємодія при розслідуванні економічних злочинів : монографія / [кол. авт.: А. Ф. Волобуєв, І. М. Осика, Р. Л. Степанюк та ін.] ; за заг. ред. А. Ф. Волобуєва. Харків : Курсор, 2009. 320 с

16. Волобуєв А. Ф. Наукові основи комплексної методики розслідування корисливих злочинів у сфері підприємництва : дис. … д-ра юрид. наук : 12.00.09. Харків, 2001. 426 с.
17. Корнилов Г. А. Расследование преступлений, совершаемых в финансово-кредитной сфере. М. ; Якутск, 2002. 252 с.
18. Кузьмічов В. С., Чорноус Ю. М. Розслідування злочинів: міжнародне і національне законодавство. *Теорія і практика :* навч. посіб. Київ : КНТ, 2008. 448 с.
19. Куликов В. И. Основы криминалистической теории организованной преступной деятельности. Ульяновск : Филиал МГУ, 1994. 256 с.
20. Матусовский Г. А. Экономические преступления: криминалистический анализ. Харьков : Консум, 1999. 480 с.
21. Мащенко П. Л., Пилипенко М. О. Технология Блокчейн и ее практическое применение. *Наука, техника, образование.* 2017. № 32. С. 61-64.
22. Михальчук Т. В. Використання інформації, отриманої телекомунікаційним шляхом, у розслідуванні злочинів : дис. … канд. юрид. наук : 12.00.09. Київ, 2009. 222 с.
23. Розслідування злочинів, вчинених з використанням шкідливих програмних чи технічних засобів : метод. рек. / [О. Ф. Вакуленко, О. М. Стрільців, О. С. Тарасенко та ін.]. Київ, 2016. 56 с.
24. Розслідування злочинів, пов'язаних з незаконним розповсюдженням у мережі Інтернет недійного контенту провайдерами програмних послуг та Інтернет-провайдерами : метод. рек. / [О. М. Стрільців, О. С. Тарасенко, І. Р. Курилін та ін.]. Київ, 2017. 44 с.
25. Романов С. Ю. Обман як спосіб злочинної діяльності : автореф. дис. ... канд. юрид. наук : 12.00.08. Харків, 1998. 16 с.
26. Романюк Б. В., Гавловський В. Д., Гуцалюк М. В., Бутузов В. М. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій / за ред. Я. Ю. Кондратьєва. Київ : Паливода А. В., 2004. 144 с.
27. Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : дис. … канд. юрид. наук : 12.00.09. Харків, 2007. 250 с.
28. Самойленко О.А. Основи методики розслідування злочинів, вчиненихуу кіберпросторі: монографія / О. А. Самойленко ; за заг. ред. А. Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с.
29. Самойленко О. А. Питання персоналізації відомостей про особу злочинця, що вчиняє кримінальне правопорушення у обстановці кіберпростору. Протидія організованій злочинній діяльності : матеріали всеукраїнської наук.-практ. інтернет-конф. м. Одеса, 19 квіт. 2019 р. Одеса, 2019. 116 с. С. 94-97.
30. Тіщенко В. В. Концептуальні основи розслідування корисливо-насильницьких злочинів : дис. … д-ра юрид. наук : 12.00.09. Одеса, 2003. 445 с.
31. Тіщенко В. В. Теоретичні і практичні основи методики розслідування злочинів : монографія. Одеса : Фенікс, 2007. 260 с.
32. Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування : монографія. Київ : Хай-Тек Прес, 2010. 624 с.

Питання заняття

1. Сутність та криміналістична класифікація кіберзлочинів, вчинених з корисливих мотивів.

2.Криміналістина характеристика злочинів, що спрямовані на заволодіння чужим майном, та пов'язані з ними злочини у сфері функціонування електронних розрахунків.

3. Слідчі ситуації початкового етапу і програми (алгоритми) розслідування злочинів, що спрямовані на заволодіння чужим майном, та пов'язані з ними злочини у сфері функціонування електронних розрахунків.

4.Криміналістична характеристика кіберзлочинів, що порушують встановлений порядок обігу певних речей.

5.Типові слідчі ситуації початкового етапу і програми (алгоритми) розслідування кіберзлочини що порушують встановлений порядок обігу певних речей.

Завдання для поточного контролю знань і вмінь здобувачів вищої освіти

1. **Завдання.** Розробити розгорнутий конспект для відповіді на питання за варіантами:

1.1. Криміналістична характеристика вимагань, вчинених із використанням кіберпростору, та особливості розслідування таких злочинів.

1.2. Криміналістична характеристика привласнення, розтрати майна або заволодіння ним шляхом зловживання службовим становищем, що вчинені з використанням кіберпростору, та особливості розслідування таких злочинів.

1.3. Методика розслідування незаконних дій з платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення.

1.4. Розслідування зайняття гральним бізнесом із застосуванням мережі Інтернет.

1.5. Розслідування відмивання за допомогою високих інформаційних технологій доходів, одержаних злочинним шляхом.

Методична порада: підчас оформлення письмового завдання враховувати, що питання може мати дискусійні аспекти, студенти можуть дотримуватися будь-якої позиції, але зобов'язані посилатися на джерело інформації. Для розуміння та кращого запам'ятовування того, що вивчається, корисно проводити порівняння 2-3 точок зору, викладених у підручниках, монографічних працях, а також звертатись до практики (користуючись прикладами з вироків суду, що містяться в Реєстрі судових рішень) .

2. **Тестові завдання**. Метою проведення тестування є визначення рівня засвоєння викладеного матеріалу та перевірка вміння щодо практичного використання отриманих знань здобувачами вищої освіти.

Тест 1. Поясніть, чим визнаються в криміналістичній методиці розслідування корисливих злочинів, вчинених із використанням кіберпростору банківська таємниця:

а) обставиною, що не має ніякого значення для розслідування цього злочину;

б) обов'язковою ознакою провадження за ст. 200 КК України, без якої немає підстави для відкриття кримінального провадження про цей злочин;

в) обставиною, що має бути встановлена під час допиту свідків;

г) завжди предмет посягання;

д) завжди засіб вчинення злочину.

Тест 2. Визначте, що з наведеного не належить до криміналістичної характеристики привласнення, розтрати майна або заволодіння ним шляхом зловживання службовим становищем, вчинене із використанням кіберпростору:

а) об'єкт злочину;

б) предмет безпосереднього посягання;

в) слідова картина злочину;

г) спосіб вчинення привласнення, розтрати майна або заволодіння ним шляхом зловживання службовим становищем;

д) дані про особу злочинців, які вчиняють цей злочин.

Тест 3. Спосіб вчинення корисливого злочину в кіберпросторі частіше за все визнається як:

а) усічений (підготовка і приховування злочину);

б) простий безпосереднього вчинення (заволодіння грошима);

в) усічений (вчинення та приховування злочину);

г) повний (підготовки, безпосереднього вчинення, приховування злочину);

д) усічений (підготовки і безпосереднього вчинення (заволодіння майном).

Тест 4. Оцініть наведені твердження, оберіть логічно обгрунтоване. «Злочинець упевнений користувач при вчиненні злочинів, що спрямовані на заволодіння чужим майном, та пов'язані з ними злочини у сфері функціонування електронних розрахунків зазвичай …

а) має віддалені стосунки з фізичною особою-жертвою»;

б) не має доступ до інформації, необхідної для вчинення злочину»;

в) пов'язаний з організацією-жертвою за трудовою угодою або має особисті стосунки з фізичною особою-жертвою;

г) може бути пов'язаний з організацією-жертвою;

д) завжди знаходить для допомоги спеціаліста з інформаційних технологій».

Тест 5. До типової слідової картини вчинення кіберзлочинів що порушують встановлений порядок обігу певних речей не відносяться:

а) нетрадиційні (цифрові) сліди;

б) офіційні документи;

в) речі що мають особливий порядок обігу (спеціальні технічні пристрої, зброя тощо);

г) сліди-відображення (відбиток пальця, ноги, взуття);

д) слідів-речовин (наркотичні засоби; прекурсори, вибухова речовина тощо).

3. **Кейс**. Використовуючи Реєстр судових рішень або матеріали практики самостійно обрати конкретний факт злочинної діяльності в межах Теми заняття та здійснити аналіз процесу його розслідування. Обрати, керуючись рішенням і умовами конкретної фабули події злочину, що випливає зі змісту вироку або матеріалів практики, програму (алгоритм) дій слідчого.

Заняття № 7
(денна форма навчання)

Тема 7. Розслідування кіберзлочинів, вчинених з антидержавно-політичних мотивів, пов'язаних з державно-політичною сферою відносин суб'єктів у кіберпросторі

Мета вивчення

Сформувати та закріпити систему знань щодо методики розслідування кіберзлочинів, вчинених з антидержавно-політичних мотивів, що пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі

Результати навчання

Після практичного занятт я здобувач вищої освіти буде (спроможний):

1) визначати належні та прийнятні для юридичного аналізу факти щодо сфери боротьби з кіберзлочинами;

2) застосувати сучасні інформаційні технології та інформаційні ресурси за для розв'язання практичних задач щодо організації та планування розслідування кіберзлочинів, що вчиняються с антидержавно-політичних мотивів;

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

Література

нормативно-правові акти:

1. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14.

2. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/ laws/show/4651-17.

3. Про оперативно-розшукову діяльність: Закон України від 18 лют. 1992 р. № 2135-XII URL: https://zakon.rada.gov.ua/laws/show/2135-12

4. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

5. Інструкції про порядок ведення єдиного обліку в органах поліції заяв і

повідомлень про вчинені кримінальні правопорушення та інші події : наказ МВС України від 6 листоп. 2015 р. за № 1377. URL: http://zakon.rada.gov.ua/laws/show/z1498-15.

6. Положення про порядок ведення Єдиного реєстру досудових розслідувань : наказ Генеральної прокуратури України від 17 серп. 2012 р. № 69 URL: http://zakon.rada.gov.ua/laws/show/z0680-16.

7. Про затвердження Порядку розгляду звернень та організації проведення особистого прийому громадян в органах та підрозділах Національної поліції України : наказ Міністерства внутрішніх справ України від 15 листоп. 2017 р. № 93. URL: http://zakon.rada.gov.ua/laws/show/z1493-17.

8. 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 МВС України від 07 лип. 2017 р. № 575. URL : https://zakon.rada.gov.ua/laws/show/z0937-17

9. 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 МВС України від 07 лип. 2017 р. № 575. URL : https://zakon.rada.gov.ua/laws/show/z0937-17.

10.Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ ГП України, МВС України, СБ України, Адміністрації державної прикордонної служби України, Міністерства Фінансів України, Міністерства юстиції України від 16 лист. 2012 р. № 114/1042/516/1199/936/1687/5. URL: https://zakon2.rada.gov.ua/laws/show/v0114900-12.

спеціальна література:

11. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / [М. В. Гребенюк, В. Д. Гавловський, М. В. Гуцалюк та ін.] ; за заг. ред. М. В. Гребенюка. Київ : МНДЦ при РНБО України, 2017. 77 с.

12.Галаган В. І. Проблеми вдосконалення кримінальнопроцесуальної діяльності органів внутрішніх справ України : монографія. К. : Нац. академія внутр. справ України, 2002. 300 с.

13.Зелінська Н. А. Міжнародно-правова концепція міжнародного злочину : автореф. дис. … д-ра юрид. наук : 12.00.11. Київ, 2007. 37 с.

14.Ищенко Е. П. Расследование преступлений, связанных с профессиональной деятельностью. М., 2009. 352 с.

15.Кудінов С.С., Шехавцов Р. М., Дроздов О. М., Гриненко С. О. Негласні слідчі (розшукові) дії та використання результатів оперативно-розшуової діяльності у кримінальному провадженні: навч.-практ. посіб. 3-е вид., розш. та допов. Х. : Оберіг, 2018. 540 с.

16.Мазуров В. А. Компьютерные преступления: классификация и способы противодействия : учеб.-практ. пособие. М. : Палеотип, 2002. 148 с.

17.Марущак А. І. Інформаційне право: доступ до інформації : навч. посіб. Київ, 2007. 531 с.

18.Марущак А. І. Правові основи захисту інформації з обмеженим доступом. Київ, 2007. 208 с.

19.Масол Д. І. Мотиви расової, національної чи релігійної нетерпимості у кримінальному праві України : автореф. дис. … канд. юрид. наук : 12.00.08. Київ, 2014. 20 с.

20.Матусовський Г. А. Загальні положення методики розслідування злочинів. *Криміналістика :* підручник / за ред. В. Ю. Шепітька. Київ : Ін Юре, 2001. 684 с.

21.Одерій О. В. Теорія і практика розслідування злочинів проти довкілля : монографія. Харків, 2015. 528 с.

22.Пчеліна О. В. Теоретичні засади формування та реалізації методики розслідування злочинів у сфері службової діяльності : автореф. … дис. д-ра юрид. наук : 12.00.09. Харків, 2017. 40 с

23.Розслідування злочинів, пов’язаних з незаконним розповсюдженням у мережі Інтернет недійного контенту провайдерами програмних послуг та Інтернет-провайдерами : метод. рек. / [О. М. Стрільців, О. С. Тарасенко, І. Р. Курилін та ін.]. Київ, 2017. 44 с.

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

25.Федотов Н. Н. Форензика – компютерная криминалистика. М. : Юрид. мир, 2007. 360 с.

26.Хараберюш І. Ф., Мацюк В. Я., Некрасов В. А., Хараберюш О. І., Хараберюш І. Ф. Використання оперативно-технічних засобів у протидії злочинам, що вчиняються у сфері нових інформаційних технологій : монографія. Київ : КНТ, 2007. 196 с.

27.Шилан Н. Н., Кривонос Ю. М., Бирюков Г. М. Компьютерные преступления и проблемы защиты информации. Луганск : РИО ЛИВД, 1999. 64 с.

28.Шилін М. Національна безпека: проблеми правового забезпечення діяльності суб’єктів сектору безпеки та можливі шляхи вирішення. *Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку :* матеріали Міжнар. наук.-практ. конф. (Острог, 1 груд. 2017 р.) / за заг. ред. М. С. Романова. Острог : Нац. ун-т «Острозька академія», 2017. 180 с.

Питання заняття

1. Сутність та криміналістична класифікація кіберзлочинів, вчинених з антидержавно-політичних мотивів.
2. Криміналістична характеристика злочининів, що пов’язані з антидержавницькими діями у кіберпросторі.

3. Характеристика початкового етапу і програми (алгоритми) розслідування злочинінів, що пов'язані з антидержавницькими діями у кіберпросторі.

4. Охарактеризувати інцидент кібертероризму.

5. Особливості розслідування інцидентів кібертероризму: ситуації та програми (алгоритми) розслідування на початковому етапі.

Завдання для поточного контролю знань і вмінь здобувачів вищої освіти

1. **Завдання.** Розробити розгорнутий конспект для відповіді на питання за варіантами:

1.1. Місце кібертероризму серед різновидів тероризму.

1.2. Характеристика особи-кібертерориста.

1.3. Сучасний стан протидії кібертероризму в Україні.

1.3. Розслідування фінансування тероризму.

1.4. Розслідування кіберзлочинів, що пов'язані з отриманням неправомірної вигоди.

1.5. Розслідування службових злочинів, пов'язаних із втручанням у роботу автоматизованих систем.

Методична порада: підчас оформлення письмового завдання враховувати, що питання може мати дискусійні аспекти, студенти можуть дотримуватися будь-якої позиції, але зобов'язані посилатися на джерело інформації. Для розуміння та кращого запам'ятовування того, що вивчається, корисно проводити порівняння 2-3 точок зору, викладених у підручниках, монографічних працях, а також звертатись до практики (користуючись прикладами з вироків суду, що містяться в Реєстрі судових рішень).

2. **Тестові завдання**. Метою проведення тестування є визначення рівня засвоєння викладеного матеріалу та перевірка вміння щодо практичного використання отриманих знань здобувачами вищої освіти.

Тест 1. Оцініть обґрунтованість наведених тверджень і оберіть правильне: «Типова початкова слідча ситуація, що характеризується наявністю досить повної інформації, що міститься в документах, про факт підготовки до злочину проти основ національної безпеки України, складається у випадку відкриття кримінального провадження про такий злочин за:

а) заявою осіб»;

б) явкою з повинною»;

в) повідомленням підприємства, організації, установи, що базуються на даних внутрішньої перевірки»;

г) повідомленням представників влади про затримання підозрюваних на місці злочину»;

д) за матеріалами оперативно-розшукової діяльності (справи)».

Тест 2. Порівняйте наведені твердження і оберіть логічно обґрунтоване: «Тактична операція встановлення технології злочинної діяльності з використанням кіберпростору» НЕ характерна при розслідуванні кіберзлочинів, вчинених з антидержавно-політичних мотивів в умовах типової слідчої ситуації, коли:

а) кримінальне провадження розпочато в результаті отримання заяви/повідомлення особи про кримінальне правопорушення, в матеріалах відсутні будь-які відомості про особу злочинця»;

б) кримінальне провадження розпочато в результаті перевірки оперативної інформації, в матеріалах відсутні будь-які відомості про особу злочинця» ;

в) кримінальне провадження розпочато в результаті перевірки оперативної інформації, матеріали первинної перевірки містять неперсоналізовані відомості про особу злочинця»;

г) кримінальне провадження розпочато в рамках реалізації матеріалів ОРС; у ініціативному рапорті оперативного співробітника відсутність відомостей про особу злочинця є формальною»;

д) наявні всі вище наведені ситуації.

Тест 3. Визначте, що з наведеного не належить до криміналістичної характеристики злочинів проти основ національної безпеки України, вчинених у кіберпросторі:

а) дані про злочинців, які вчиняють ці злочини;

б) дані про потерпілих;

в) слідова картина злочинів;

г) спосіб вчинення злочинів;

д) спосіб підготовки.

Тест 4. Поясніть, що розуміється під кібератакою:

а) будь-який кіберінцидент;

б) вид терористичної діяльності, орієнтований на використання різних форм і методів тимчасового або незворотного виведення з ладу інформаційної інфраструктури держави або її елементів, а також за допомогою протиправного використання інформаційної структури для створення умов, що тягнуть за собою тяжкі наслідки для різних сторін життєдіяльності особистості, суспільства і держави (узагальнене визначення;

в) це сукупність узгоджених щодо мети, змісту та часу дій або заходів (так званих кібераакцій, спрямованих на певний об’єкт впливу з метою порушення конфіденційності, цілісності, доступності, спостережуваності або авторства інформації, що циркулює в ньому, з урахуванням її уразливості, а також порушення роботи ІТ-систем і мереж зазначеного об’єкта);

г) акт технологічного тероризму;

д) спосіб вчинення акту кібертероризму.

Тест 4. Оцінка масштабів результату кібератаки, усунення цих наслідків, налагодження міжвідомчих зв'язків з метою забезпечення розслідування входить до :

а) програми (алгоритму) розслідування злочину в ситуації відсутності будь-яких відомостей про особу імовірного злочинця;

б) програми (алгоритму) розслідування злочину в ситуації наявності персоналізованої інформації про особу злочинця;

в) Тактичної операції «Затримання злочинця на гарячому»;

г) Тактичної операції «Збирання електронних (цифрових) носіїв інформації»;

д) переліку тактичних завдань початкового етапу розслідування.

3. **Кейс**. Використовуючи Реєстр судових рішень або матеріали практики самостійно обрати конкретний факт злочинної діяльності в межах Теми заняття та здійснити аналіз процесу його розслідування. Обрати, керуючись рішенням і умовами конкретної фабули події злочину, що випливає зі змісту вироку або матеріалів практики, програму (алгоритм) дій слідчого.

Критерії оцінювання підчас поточного контролю

У відповідності до визначених критеріїв поточний контроль здійснюється за визначеною силабусом (робочою навчальною програмою) системою.

Схема нарахування балів (складові оцінювання результатів навчання)		
Пункт оцінки	% підсумкової оцінки або максимальна оцінка в балах	Групове чи індивідуальне оцінювання
Поточний контроль, разом, у т.ч.:		
• опитування	20	інд
• вирішення практичних завдань	15	інд
• самостійна робота	15	груп
Підсумковий контроль, разом, у т.ч.:	50	
• письмова компонента	25	інд
• усна компонента	25	інд
Разом за дисципліну	100	

Методичні вказівки (рекомендації) для викладачів, які проводять практичні заняття

Проведення практичних занять дозволяє вирішувати такі дидактичні цілі:

- оптимально поєднувати лекційні заняття із систематичною самостійною навчально-пізнавальною діяльністю здобувачів освіти, їх теоретичну підготовку з практичною;

- розвивати уміння, навички розумової праці, творчого мислення, уміння використовувати теоретичні знання для вирішення практичних завдань;

- формувати у здобувачів совіти інтерес до науково-дослідної роботи і залучення їх до наукових досліджень, які здійснює кафедра;

- забезпечувати системне повторення, поглиблення і закріплення знань здобувачів вищої освіти за певною темою;

- формувати уміння і навички здійснення різних видів майбутньої професійної діяльності;

- здійснювати діагностику і контроль знань здобувачів вищої освіти з окремих розділів і тем програми, формувати уміння і навички виконання різних видів майбутньої професійної діяльності.

Практичні (семінарські) заняття проводяться в об’ємі, не меншому, ніж зазначений у цьому комплексі для таких занять.

При проведенні практичних занять викладач заздалегідь формує порядок проведення практичного заняття, у якому визначає порядок і послідовність заслуховування підготовлених відповідно до теми заняття доповідей, обговорення їх, опитування здобувачів, проведення захисту рефератів, у разі наявності таких та проведення дискусії з теми практичного заняття.

Оцінка доповідей, відповідей на запитання оцінюються за національною шкалою, про що ставиться відмітка у журналі академгрупи.

При проведенні занять, крім відповідей на питання (відповідно до рекомендованих планів), студентами розв’язуються тести, ситуативні завдання (кейси), відповідно до змісту практичного заняття. Оцінювання вирішення сутаутивних завдань проводиться також за національною шкалою, про що робиться відміта в журналі академгрупи.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ

Завдання № 1
(денна форма навчання)

Завдання №1
(заочна форма навчання)

Тема 1. Методичні основи розслідування кіберзлочинів

Мета самостійної роботи

Закріпити систему знань про сучасні методологічні основи розслідування кіберзлочинів, визначити основні проблеми правозастосовної практики в цій сфері, а також шляхи їх подолання.

Результати навчання

Після виконання завдання для самостійної роботи здобувач вищої освіти буде (спроможний):

1) здійснювати пошук, вивчення та аналіз інформаційних ресурсів щодо розроблення методик боротьби з кіберзлочинами;

2) використовувати в правозастосовній діяльності нормативно-правові акти, що регулюють відносини, що виникають підчас виявлення та розслідування фактів вчинення злочинів у кіберпросторі.

План самостійної роботи

1. Опрацювання лекційного матеріалу та інших джерел з переліку літератури за темою.
2. Підготовка до практичних занять.
3. Відповісти на питання : Сучасний стан дисертаційних розробок в сфері протидії кіберзлочинам та методик їх розслідування.
4. Підготовка реферату на одну з таких тем: «Англосаксонська доктрина визначення сутності кіберзлочинів», «Європейська доктрина визначення сутності кіберзлочинів», «Результати діяльності СБ України у протидії кіберзлочинності в Україні».

Завдання № 2
(денна форма навчання)

Завдання №2
(заочна форма навчання)

Тема 2. Організаційні та правові основи діяльності осіб у мережі Інтернет в Україні та за її межами

Мета вивчення

Закріпити систему знань щодо особливостей реалізації та застосування норм матеріального і процесуального права стосовно відносин у традиційних сферах суспільного життя суб'єктів кіберпростору,

Результати навчання

Після виконання завдання для самостійної роботи здобувач вищої освіти буде (спроможний):

1) здійснювати пошук, вивчення та аналіз нормативно-правових актів, що регулюють конкретні відносини між суб"єктами кіберпростору, що пов'язані із процесом розслідування фактів вчинення злочинів у кіберпросторі;

2) розвивати здатність до критичного та системного аналізу правових явищ у кіберпросторі;

3) розуміти міжнародні стандарти прав людини як користувача кіберпростору, перспективи розвитку кіберпростору.

План самостійної роботи

1. Опрацювання лекційного матеріалу та інших джерел з переліку літератури за темою.
2. Підготовка до практичних занять.
3. Відповісти на питання: Законодавчо закріплені основні напрямки розвитку Інтернет-управління на міжнародному рівні.
4. Підготовка реферату на одну з таких тем: «Правові основи діяльності осіб у кіберпросторі в США»; «Правові основи діяльності осіб у кіберпросторі в країнах Європейського Союзу»; «Правові основи діяльності осіб у кіберпросторі в країнах Арабського світу»; «Правові основи діяльності осіб у кіберпросторі в країнах Азії».

Завдання № 3
(денна форма навчання)

Завдання №3
(заочна форма навчання)

Тема 3. Організаційні засади виявлення та початку кримінального провадження щодо кіберзлочинів

Мета вивчення

Закріпити систему знань щодо організаційних засад виявлення кіберзлочинів та відкриття кримінального провадження щодо такої категорії злочинів.

Результати навчання

Після виконання завдання для самостійної роботи здобувач вищої освіти буде (спроможний):

1) визначати належні та прийнятні для юридичного аналізу факти щодо сфери боротьби з кіберзлочинами;

2) використовувати криміналістичні рекомендації підчас відкриття кримінального провадження щодо кіберзлочинів.

План самостійної роботи

1. Опрацювання лекційного матеріалу та інших джерел з переліку літератури за темою.
2. Підготовка до практичних занять.
3. Відповісти на питання: Особливості початку кримінального провадження щодо несанкціонованого втручання в роботу ЕОМ, АС, мереж чи систем; Особливості початку кримінального провадження щодо шахрайства в мережі Інтернет.
4. Підготовка реферату на одну з таких тем: «Встановлення шкідливих наслідків неправомірного доступу до комп'ютерних систем чи мереж», «Встановлення надійності засобів захисту комп'ютерної інформації».

Завдання № 4
(денна форма навчання)

Завдання № 4
(заочна форма навчання)

Тема 4. Використання спеціальних знань під час розслідування кіберзлочинів

Мета вивчення

Закріпити систему знань щодо організаційних засад виявлення та розслідування кіберзлочинів.

Результати навчання

Після виконання завдання для самостійної роботи здобувач вищої освіти буде (спроможний):

1) використовувати в правозастосовній діяльності нормативно-правові акти, що регулюють відносини, що виникають підчас використання спеціальних знань;

2) призначати судові експертизи в процесі розслудвання злочинів у кіберпросторі;

3) застосовувати криміналістичні рекомендації підчас збирання матеріалів попередньої перевірки за такими фактами.

План самостійної роботи

1. Опрацювання лекційного матеріалу та інших джерел з переліку літератури за темою.
2. Підготовка до практичних занять.
3. Відповісти на питання: Специфіка використання допомоги спеціаліста підчас проведення НС(Р)Д.
4. Підготовка реферату на одну з таких тем: «Експертні дослідження електронного документа», «Проблемні питання організації та проведення комплексних експертиз підчас розслідування кіберзлочинів».

Завдання № 5
(денна форма навчання)

Завдання № 5
(заочна форма навчання)

Тема 5. Організаційно-тактичні основи розслідування кіберзлочинів

Мета вивчення

Закріпити систему знань щодо організаційно-тактичні засад розслідування кіберзлочинів.

Результати навчання

Після виконання завдання для самостійної роботи здобувач вищої освіти буде (спроможний):

1) проводити слідчі (розшукові) дії, тактичні операції, взаємодіяти з працівниками оперативних підрозділів підчас розслідування кіберзлочинів;

2) аналізувати правові та правозастосовчі проблеми, формувати та обґрунтовувати власну правозастосовну та практичну позицію підчас здійснення або участі в слідчих (розшукових) діях в ході розслідування злочинів, вчинених у кіберпросторі.

План самостійної роботи

1. Опрацювання лекційного матеріалу та інших джерел з переліку літератури за темою.
2. Підготовка до практичних занять.
3. Відповісти на питання: 1) тактика проведення затримання злочинця, що вчинив кіберзлочин; 2) особливості тактики проведення обшуку в юридичній особі.
4. Підготовка реферату на одну з таких тем: «Дотримання режиму секретності під час проведення негласних слідчих (розшукових) дій», «Форми взаємодії слідчого із працівниками оперативних підрозділів підчас розслідування кіберзлочинів», «Слідчий огляд веб-сторінки»

Завдання № 6
(денна форма навчання)

Завдання №6
(заочна форма навчання)

Тема 6. Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов'язаних з фінансово-економічною сферою відносин у кіберпросторі

Мета вивчення

Закріпити систему знань щодо методики розслідування кіберзлочинів вчинених з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі

Результати навчання

Після виконання завдання для самостійної роботи здобувач вищої освіти буде (спроможний):

1) використовувати в професійній юридичній діяльності основні техніко-криміналістичні засоби, прийоми і методи розслідування;

2) розробляти з використанням криміналістичних рекомендацій план підготовки і проведення слідчої дії, тактичної операції, використання спеціальних знань під час розслідування кіберзлочинів, вчинених з корисливих мотивів;

3) проводити слідчу дію, призначати судову експертизу, організовувати взаємодію слідчого з працівниками оперативних підрозділів й іншими суб'єктами під час розслідування кіберзлочинів, вчинених з корисливих мотивів.

Додаткова література

1. Генеральна прокуратура України. URL: http://www.gp.gov.ua
2. Департамент Кіберполіції Національної поліції України. URL: https://www.cybercrime.gov.ua
3. Офіційний сайт Лізі протидії кібертероризму та інформаційним війнам. URL: http://ligabezinfo.org/contacts
4. Єдиний державний реєстр судових рішень. URL: http://reyestr.court.gov.ua/
5. Електронний каталог національної бібліотеки України імені В.І. Венадскього - http://www.irbis-nbuv.gov.ua.

План самостійної роботи

1. Опрацювання лекційного матеріалу та інших джерел з переліку літератури за темою.
2. Підготовка до практичних занять.
3. Підготовка реферату на одну з таких тем: «Розслідування вчиненого в кіберпросторі незаконного використання знака для товарів і послуг, фірмового

найменування, кваліфікованого зазначення походження товару», «Розслідування розголошення комерційної або банківської таємниці, вчиненого через мережу Інтернет».

4. Аналіз процесу розслідування факту злочинної діяльності, вчиненої з корисливих мотивів у кіберпросторі (в основу покласти матеріали фактичного кримінального провадження, використовуючи Реєстр судових рішень або матеріали практики).

Завдання № 7
(денна форма навчання)

Завдання №7
(заочна форма навчання

Тема 7. Розслідування кіберзлочинів, вчинених з антидержавно-політичних мотивів, пов'язаних з державно-політичною сферою відносин суб'єктів у кіберпросторі

Мета вивчення

Закріпити систему знань щодо методики розслідування кіберзлочинів вчинених з антидержавно-політичних мотивів, що пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі

Результати навчання

Після виконання завдання для самостійної роботи здобувач вищої освіти буде (спроможний):

1) використовувати в професійній юридичній діяльності основні техніко-криміналістичні засоби, прийоми і методи розслідування;

2) розробляти з використанням криміналістичних рекомендацій план підготовки і проведення слідчої дії, тактичної операції, використання спеціальних знань під час розслідування кіберзлочинів, вчинених з антидержавно-політичних мотивів;

3) проводити відповідну слідчу дію, призначати судову експертизу, організовувати взаємодію слідчого з працівниками оперативних підрозділів й іншими суб'єктами під час розслідування кіберзлочинів, вчинених з антидержавно-політичних мотивів.

Додаткова література

1. Генеральна прокуратура України. URL: http://www.gp.gov.ua
2. Департамент Кіберполіції Національної поліції України. URL: https://www.cybercrime.gov.ua
3. Офіційний сайт Лізі протидії кібертероризму та інформаційним війнам. URL: http://ligabezinfo.org/contacts
4. Єдиний державний реєстр судових рішень. URL: http://reyestr.court.gov.ua/
5. Електронний каталог національної бібліотеки України імені В.І. Венадскього - http://www.irbis-nbuv.gov.ua.

План самостійної роботи

1. Опрацювання лекційного матеріалу та інших джерел з переліку літератури за темою.

2. Підготовка до практичних занять.

3. Підготовка реферату на одну з таких тем: «Проблемні питання протидії кібертероризму в Україні», «Розслідування злочини проти виборчих прав і свобод, вчинених із використанням кіберпростору».

4. Аналіз процесу розслідування конкретного факту злочинної діяльності**,** вчиненої з антидержавно-політичних мотивів у кіберпросторі (в основу покласти матеріали фактичного кримінального провадження, використовуючи Реєстр судових рішень або матеріали практики).

ПИТАННЯ, ЗАВДАННЯ ТА КЕЙСИ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ І ВМІНЬ ЗДОБУВАЧА

(денна та заочна форма навчання)

Питання

1. Сутність поняття «кіберпростір».
2. Особливості кіберпростору, що привертають увагу злочинців до використання його середовища з метою досягнення злочинного результату.
3. Визначення основних технічних термінів, пов'язаних із кіберпростором: телекомунікаційна мережа, комп'ютерна мережа, інформаційні технології, електричний зв'язок, мережа зв'язку, мережа Інтернет.
4. Оцінки загроз кіберзлочинності національній безпеці держав та міжнародному порядку.
5. Класифікація кіберзлочинів в Європейської конвенції по боротьбі з кіберзлочинністю.
6. Криміналістичні класифікації кіберзлочинів.
7. Класифікація кіберзлочинів за кримінально-правовим критерієм, що визначає нормативну суть класифікації, передбаченої законом України.
8. Сучасний стан дисертаційних розробок в сфері боротьби з кіберзлочинами.
9. Розроблені окремі криміналістичні методики розслідування кіберзлочинів.
10. Традиційна структура окремих криміналістичних методик розслідування кіберзлочинів.
11. Міжнародні організації, що здійснюють регулювання Інтернет та особливості їх діяльності.
12. Особливості організації національного сегменту кіберпростору.
13. Ключові суб'єкти ринку та організації телекомунікаційних послуг в Україні (суб'єкти взаємодії слідчого підчас розслідування кіберзлочинів).
14. Особливості правового регулювання відносин в кіберпросторі.
15. Кримінально-правова охорона суспільних відносин у кіберпросторі в України. Конвенція Ради Європи про кіберзлочинність.
16. Характеристика інших міжнародних правових актів, які є частиною національного законодавства України, що регулюють правила та принципи охорони суб'єктів відносин у кіберпросторі.
17. Виявлення кіберзлочинів як напрямок правоохоронної діяльності. Типові джерела оперативної інформації про кіберзлочини.
18. Теоретичний аспект організації слідчим початку провадження та джерела обставин, що можуть свідчити про вчинення певного виду кіберзлочинів.
19. Форми початку кримінального провадження щодо кіберзлочинів.
20. Особливості перевірки інформації про кіберзлочини, що вчинені або готуються.

21.Зміст (наповнення) матеріалів первинної перевірки, які підлягають передачі керівникові органу досудового розслідування для внесення до ЄРДР інформації про кіберзлочин.

22. Відкриття кримінального провадження за заявою та повідомленням особи про кіберзлочин.

23.Організаційні заходи слідчого для перевірки отриманої первинної від заявника інформації.

24.Спеціальні знання під час розслідування кіберзлочинів.

25.Організаційні і тактичні особливості залучення спеціаліста для надання письмової та усної консультації підчас розслідування кіберзлочинів.

26.Назвіть організаційні і тактичні особливості залучення спеціаліста для надання безпосередньої техніко-криміналістичної та іншої технічної допомоги підчас слідчих (розшукових) та негласних слідчих (розшукових) дій.

27.Залучення експерта підчас розслідування кіберзлочинів для проведення судової комп'ютерно-технічної експертизи.

28.Залучення підчас розслідування кіберзлочинів експерта для проведення експертиза телекомунікаційних систем (обладнання) та засобів.

29.Залучення експерта для комплексних судових експертиз підчас розслідування кіберзлочинів (КТЕ та експертизи відео звукозапису; КТЕ і ТЕД).

30.Типові слідчі ситуації початкового та наступного етапів розслідування кіберзлочинів.

31.Типові тактичні операції розслідування кіберзлочинів та їх зв'язок із типовими слідчими ситуаціями, внутрішня структура кожної операції.

32.Ознаки інформації в електронній формі (електронних даних або документів (виходячи зі змісту положень КПК України), що мають значення для тактики провадження окремих слідчих (розшукових) дій у справах про кіберзлочини.

33.Загальні положення тактики підготовки до проведення слідчих дій, спрямованих на збирання інформації в електронній формі.

34.Тактичні правила та рекомендації, спрямовані на пошук інформації в електронній формі підчас слідчого огляду, обшуку.

35.Тактичні правила та рекомендації, спрямовані на фіксацію та вилучення інформації в електронній формі підчас слідчого огляду, обшуку або тимчасового доступу до речей та документів.

36.Тактичні рекомендації, спрямовані на вилучення інформації в електронній формі підчас слідчого огляду, обшуку або тимчасового доступу до речей та документів.

37.Особливості вилучення мобільних пристроїв.

38.Особливості допиту свідка, потерпілого, підозрюваного у справах про кіберзлочин.

39.Загальні тактичні особливості проведення зняття інформації з транспортних телекомунікаційних мереж, зняття інформації з електронних інформаційних систем; установлення місцезнаходження радіоелектронного засобу підчас розслідування кіберзлочинів.

40.Загальні тактичні особливості проведення контролю за вчиненням злочину підчас розслідування кіберзлочинів.

41.Сутність та криміналістична класифікація кіберзлочинів, вчинених з корисливих мотивів.

42.Криміналістична характеристика злочинів, що спрямовані на заволодіння чужим майном, та пов'язані з ними злочини у сфері функціонування електронних розрахунків.

43.Слідчі ситуації початкового етапу і програми (алгоритми) розслідування злочинів, що спрямовані на заволодіння чужим майном, та пов'язані з ними злочини у сфері функціонування електронних розрахунків.

44. Криміфналістична характеристика кіберзлочини що порушують встановлений порядок обігу певних речей.

45.Типові слідчі ситуації початкового етапу і програми (алгоритми) розслідування кіберзлочини що порушують встановлений порядок обігу певних речей.

46. Сутність та криміналістична класифікація кіберзлочинів, вчинених з антидержавно-політичних мотивів.

47.Криміналістична характеристика злочининів, що пов'язані з антидержавницькими діями у кіберпросторі.

48.Характеристика початкового етапу і програми (алгоритми) розслідування злочининів, що пов'язані з антидержавницькими діями у кіберпросторі.

49.Охарактеризувати інцидент кібертероризму.

50.Особливості розслідування інцидентів кібертероризму: ситуації та програми (алгоритми) розслідування на початковому етапі.

Кейси

Визначити відповідно до наведеної в задачі ситуації особливості початку провадження (аргументувати джерело інформації про кримінальне правопорушення.

Обрати, керуючись рішенням і умовами конкретної слідчої ситуації (яку необхідно охарактеризувати), що випливає зі змісту задачі, програму дій слідчого, скласти план розслідування.

Визначити також необхідність проведення тактичної операції одразу після внесення інформації в ЄРДР (якої саме). Визначає діяльність щодо її організації та проведення.

1.

1. блок інформації: До підрозділу ДКП НП України надійшло електронне повідомлення про кримінальне правопорушення (як звернення до органу поліції) від гр. О., який повідомляв про те, що 23 жовтня 01.04 години, користуючись можливостями сервісної служби «Арбітраж WebMoney» він отримав sms-повідомлення про нібито переказу ним грошових коштів зі свого електронного гаманця коштів в сумі 1 тис. грн. на інший додатковий гаманець.

О. встиг, накласти на переказ «арешт», що унеможливило їх відчуження невстановленій йому особі.

2 блок інформації: В ході перевірки інформації співробітниками ДКП було встановлено гр. К., який мешкає у м. Черкаси. К., 23 жовтня о 00.59 годині К., реалізуючи свій злочинний умисел, направлений на несанкціоноване втручання в роботу комп'ютера гр. О., діючи умисно, за місцем своєї реєстрації та проживання, використовуючи свій комп'ютер, через мережу Інтернет, за допомогою паролю, який він незаконно отримав внаслідок роботи розповсюдженого ним в мережі програмного засобу, здійснив несанкціоноване проникнення до електронної поштової скриньки гр.О. в результаті чого отримав доступ до відомостей про електронний гаманець гр.О. та його особисту переписку. З метою таємного викрадення, належних О. грошових коштів К. створив в електронній грошовій системі додатковий електронний гаманець, зареєстрував його на своїй електронній поштовій скоринці, після чого, використовуючи свій комп'ютер, через мережу Інтернет здійснив без відома О., незаконний переказ грошових коштів з електронного гаманця О. на свій додатковий електронний гаманець**.**

При цьому він використовуючи свій комп'ютер, розповсюдив шкідливий програмний засіб, що призначений для нейтралізації паролів та інших засобів захисту комп'ютерних програм чи комп'ютерної інформації, шляхом прихованого перехоплення натискань клавіш на клавіатурі, моніторингу буферу обміну, запису знімків екрану монітору (скріншотів), моніторингу відвідуваних веб-сайтів з послідуючим відправленням такої інформації на конкретну електронну скриньку. К. налаштував його таким чином, щоб за його допомогою можна було здійснити несанкціоноване втручання в роботу комп'ютерів інших користувачів мережі «Інтернет». вказаний програмний засіб шляхом розміщення в мережі Інтернет під виглядом комп'ютерної програми для викрадення ігрових грошей в он-лайн грі «FG» на спеціально створеному інтернет-сайті домену «.ru».

2.

1. блок інформації. В ходы перевірки оперативної інформації було вснаовлено, що невстановлені особи несанкціоновано втручалися в роботу комп'ютерів юридичних осіб, на яких було встановлено програмне забезпечення дистанційного доступу до рахунків, відкритих у банківських установах (система «Клієнт-Банк»). Отримавши доступ до інформації, яка на них зберігається й обробляється, злочинці здійснювали перерахування коштів загальною сумою 357 303,44 грн на рахунок фіктивно створеного підприємства.

2 блок інформації. У ході слідства в результаті контролю за вчиненням злочину було встановлено лише особу, на яку було відкрито з її відома фіктивне підприємство з метою переведення коштів у готівкову форму.

3.

1 блок інформації. 7 січня о 09.00 до чергової частини райвідділу

міського управління внутрішніх справ із явкою звернувся гр І., який повідомив про вчинення відносно нього шахрайських дій особою під нік-неймом «Скутер», який зfволодів грошима І який як замовник товару на сайти «Olx» здійснив переказ коштів на визначений покупцем картковий рахунок з призначенням «предоплата».

2 блок інформації. В результаті виконання доручення слідчого підрозділ ДКП в Дніпровській області встановив, що протягом 2014-2017 років гр. М. з використанням комп'ютера, підключеного до глобальної мережі Інтернет, маючи на сайті http://skuters.hol.es/index.php власний Інтернет-магазин, зареєстрований на його ім'я, офіційно займаючись перепродажем двоколісних скутерів за завищеними цінами, реєстрував, використовуючи різні номери мобільних телефонів, оголошення на Інтернет-ресурсі компанії ТОВ «Ємаркет Україна» «Olx.ua» щодо продажу двоколісних скутерів без наміру поставляти останні замовникові. Для заволодіння передплатою замовників М. використовував карткові рахунки малознайомих осіб та електронні гаманці.

4.

1 блок інформації. 12 січня о 10.00 до чергової частини міського управління внутрішніх справ із повідомленням про вчинення злочину звернувся ПАТ «Приватбанк». В повідомленні йшлося про те, що невстановлена особа розробила та внесла під час запланованого робочим графіком обслуговування двох банкоматів до їх програмного забезпечення код, призначений для несанкціонованого отримання інформації про номери банківських платіжних карток і пін-кодів їх власників та запису цієї інформації у файл на жорсткий диск банкомата. Пізніше вилучила цей файл із незаконно одержаною інформацією про пластикові картки. Після цього було знов розроблено іншу программу (що розміщена в банкоматі), яка дозволяла записувати інформацію про номер банківської картки на магнітну стрічку будь-яких пластикових засобів на тих же банкоматах та мала функцію он-лайн. Таким чином, використовуючи вилучені з банкомату програми, технічні можливості банкомата, пластикові картки та інформацію про банківські картки, підозрюваний через банкомати різних банків м. Києва викрав грошові кошти власників банківських карток загальною сумою 200 000 грн. (вчинив 120 епізодів за два місяці діяльності).

2 блок інформації В ході роботи ДКП встановлено, що у вчиненні цього злочину (за не процесуальними матеріалами) підозрюється гр. Я., котрий працював спеціалістом з обслуговування банкоматів в м. Києва в ТОВ „Біт". Я. характеризується як неординальна, талановита в галузі обчислювальних систем людина, при цьому має вольовий характер, який склався під час навчання у Харківському авіаційному інституті. Я. мешкає разом із батьками похилого віку, які на запланований час проведення обшуку в його квартирі пішли до магазину.

КРИТЕРІЇ ОЦІНЮВАННЯ УСПІШНОСТІ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Національна шкала

Оцінка виставляється за національною чотирибальною шка-лою: «відмінно», «добре», «задовільно», «незадовільно». При оцінці за основу слід брати повноту і правильність виконання завдань.

1. Оцінка «5» (відмінно) ставиться в тому разі, коли відповідь здобувача вищої освіти правильна, повна, послідовна, логічна; здобувач вищої освіти впевнено володіє фактичним матеріалом з усього курсу, вміє застосовувати його щодо конкретно поставле-них завдань.

2. Оцінка «4» (добре) ставиться в тому разі, коли відповідь правильна, послідовна, логічна, але здобувач вищої освіти допускає у викладі окремі незначні пропуски фактичного матеріалу, вміє застосовувати його щодо конкретно поставлених завдань.

3. Оцінка «3» (задовільно) ставиться в тому разі, коли здобу-вач вищої освіти володіє більшою частиною фактичного матеріа-лу, але викладає його не досить послідовно і логічно, допускає істотні пропуски у відповіді, невірно формулює основні теоретич-ні положення та причинно-наслідкові зв’язки.

4. Оцінка «2» (незадовільно) ставиться в тому разі, коли здо-бувач вищої освіти виявляє незнання більшої частини фактично-го матеріалу або здобувач вищої освіти відмовляється відповідати на поставлені питання.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0 – 34	F	незадовільно з обов’язковим повторним вивчен-ням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

Навчально-методичне видання

Самойленко Олена Анатоліївна

Виявлення та розслідування кіберзлочинів

Навчально-методичний посібник

Підписано до друку _____ р.
Формат 60х84/16 Папір офсетний. Ум. друк. арк. _____
Наклад __ прим. Замовлення
Видавництво та друкарня "ТЕС"
(Свідоцтво ДК № 771) Одеса, Канатна 81/2.
Тел.:(0482) 42-90-98, (0482) 42-89-72