МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ ІЗ РОЗПОВСЮДЖЕННЯМ У МЕРЕЖІ ІНТЕРНЕТ ЗАБОРОНЕНОГО КОНТЕНТУ

Методичні рекомендації

Київ 2014

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ ІЗ РОЗПОВСЮДЖЕННЯМ У МЕРЕЖІ ІНТЕРНЕТ ЗАБОРОНЕНОГО КОНТЕНТУ

Методичні рекомендації

За загальною редакцією Ю. Ю. Орлова

Київ 2014

УДК 343.985
ББК Х 629.4
О–648

Авторський колектив:

Стрільців О. М. – начальник наукової лабораторії з проблем кримінальної міліції навчально-наукового інституту підготовки фахівців для підрозділів слідства та кримінальної міліції Національної академії внутрішніх справ, кандидат юридичних наук, старший науковий співробітник;

Крижна В. В. – старший науковий співробітник наукової лабораторії з проблем кримінальної міліції навчально-наукового інституту підготовки фахівців для підрозділів слідства та кримінальної міліції Національної академії внутрішніх справ, кандидат юридичних наук;

Максименко О. В. – старший науковий співробітник наукової лабораторії з проблем кримінальної міліції навчально-наукового інституту підготовки фахівців для підрозділів слідства та кримінальної міліції Національної академії внутрішніх справ, кандидат юридичних наук;

Садченко М. М. – старший науковий співробітник наукової лабораторії з проблем досудового розслідування навчально-наукового інституту підготовки фахівців для підрозділів слідства та кримінальної міліції Національної академії внутрішніх справ, кандидат юридичних наук;

Арешонков В. В. – провідний науковий співробітник наукової лабораторії з проблем кримінальної міліції навчально-наукового інституту підготовки фахівців для підрозділів слідства та кримінальної міліції Національної академії внутрішніх справ, кандидат юридичних наук

Рецензенти:

Василинчук В. І. – професор кафедри спеціальної техніки та оперативно-розшукового документування навчально-наукового інституту підготовки фахівців для підрозділів слідства та кримінальної міліції Національної академії внутрішніх справ, доктор юридичних наук, професор;

Кучинська О. П. – провідний науковий співробітник наукової лабораторії з проблем кримінальної міліції навчально-наукового інституту підготовки фахівців для підрозділів слідства та кримінальної міліції Національної академії внутрішніх справ, доктор юридичних наук, професор

Рекомендовано до друку науково-методичною радою Національної академії внутрішніх справ від 17 вересня 2014 р. (протокол № 1)

Матеріали подано в авторській редакції

О–648 **Особливості** розслідування кримінальних правопорушень, пов'язаних із розповсюдженням у мережі Інтернет забороненого контенту [Текст] : метод. рек. / [Стрільців О. М., Крижна В. В., Максименко О. В. та ін.] ; за заг. ред. Ю. Ю. Орлова. – К. : Нац. акад. внутр. справ, 2014. – 80 с.

Подано кримінально-правову характеристику кримінальних правопорушень, пов'язаних із розповсюдженням у мережі Інтернет забороненого контенту. Визначено особливості виявлення та розслідування цих правопорушень, висвітлено напрями доказування на початковому етапі розслідування й проведення окремих слідчих (розшукових) дій.

Для науковців, викладачів, курсантів, а також практичних працівників органів внутрішніх справ та інших правоохоронних органів

УДК 343.985
ББК Х 629.4

ВСТУП

Правові засади протидії комп'ютерній злочинності визначено в Кримінальному кодексі (КК) України. Так, розділ XVI Особливої частини «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» містить низку статей, що передбачають кримінальну відповідальність за комп'ютерні злочини.

Водночас перелік комп'ютерних злочинів не вичерпується діяннями, зазначеними в розділі XVI КК України. Певні злочини, що існували задовго до створення комп'ютерів, також можуть бути вчинені із застосуванням інформаційних технологій.

Комп'ютерний злочин – це протиправне втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних (контенту), а також інші протиправні суспільно небезпечні дії, учинені за допомогою комп'ютерів, комп'ютерних мереж і програм.

Контент (від англ. *content* – зміст) – це будь-яке інформаційно значуще (змістове) наповнення інформаційного ресурсу (Інтернет-порталу, сайту, веб-сторінки тощо). Контентом є тексти, таблиці (систематизовані бази даних), фотографії, графічні зображення, відеофільми, інтерактивні ігри, гіперпосилання тощо.

Контент певного інформаційного ресурсу може свідчити про факт готування або вчинення кримінального правопорушення. При цьому злочини, пов'язані з розповсюдженням забороненого контенту, можна поділити на дві групи.

До першої належать кримінальні правопорушення, що полягають у незаконному придбанні та/або збуті предметів і речовин, заборонених для вільного обігу, з використанням мережі Інтернет, зокрема:

– незаконне придбання зброї, бойових припасів або вибухових речовин (ст. 263);

– придбання радіоактивних матеріалів (ст. 265);

– незаконне придбання чи збут наркотичних засобів, психотропних речовин або їх аналогів (ст. 307);

– незаконне придбання, передача чи продаж іншим особам обладнання, призначеного для виготовлення наркотичних засобів, психотропних речовин або їх аналогів (ст. 313);

– збут підроблених документів на отримання наркотичних засобів, психотропних речовин або прекурсорів (ст. 318);

– незаконне придбання або збут отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів (ст. 321);

– збут завідомо фальсифікованих лікарських засобів (ст. 321^1).

До другої групи належать кримінальні правопорушення, пов'язані з розміщенням у мережі Інтернет забороненої інформації:

– відомостей, що становлять державну або іншу таємницю, яка охороняється законом: шпигунство (ст. 114) незаконне розголошення лікарської таємниці (ст. 145), порушення таємниці голосування (ст. 159), розголошення таємниці усиновлення (удочеріння) (ст. 168), розголошення комерційної таємниці (ст. 232), розголошення державної таємниці (ст. 328), несанкціоноване розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361^2), розголошення відомостей про заходи безпеки щодо особи, взятої під захист (ст. 381), розголошення даних досудового слідства та дізнання (ст. 387), розголошення відомостей військового характеру, що становлять державну таємницю (ст. 422);

– завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (ст. 259);

– заклики до вчинення дій, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади (ст. 109), заклики до вчинення дій, що загрожують громадському порядку (ст. 295).

– увезення, виготовлення, збут і розповсюдження порнографічних предметів та зображень (ст. 301);

– увезення, виготовлення або розповсюдження творів, що пропагують культ насильства й жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 300), порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками (ст. 161).

Зважаючи на значну кількість кримінальних правопорушень, пов'язаних із розповсюдженням у комп'ютерних мережах забороненого контенту, вивчення особливостей їх розслідування слід розпочати з надання кримінально-правової характеристики цих кримінальних правопорушень.

РОЗДІЛ 1
КРИМІНАЛЬНО-ПРАВОВА ХАРАКТЕРИСТИКА ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ ІЗ РОЗПОВСЮДЖЕННЯМ У КОМП'ЮТЕРНИХ МЕРЕЖАХ ЗАБОРОНЕНОГО КОНТЕНТУ

1.1. Кримінально-правова характеристика правопорушень, що полягають у незаконному придбанні та/або збуті з використанням мережі Інтернет предметів і речовин, заборонених для вільного обігу

До кримінальних правопорушень, які полягають у незаконному придбанні та (або) збуті предметів та речовин, заборонених для вільного обігу, із використанням мережі Інтернет відносяться правопорушення, передбачені ст.ст. 263, 265, 307, 313, 318, 321, 3211 КК України.

1.1.1. Предмет кримінального правопорушення

Предметом вказаних кримінальних правопорушень є відповідно зброя, бойові припаси, вибухові речовини, радіоактивні матеріали, наркотичні засоби, психотропні речовини, їх аналоги, обладнання, призначене для виготовлення наркотичних засобів, психотропних речовин або їх аналогів, підроблені документи на отримання наркотичних засобів, психотропних речовин або прекурсорів, отруйні та сильнодіючі речовини, отруйні та сильнодіючі та фальсифіковані лікарські засоби.

Вогнепальна зброя (крім гладкоствольної мисливської) – це зброя, в якій снаряд (куля, шрот) приводиться в рух миттєвим звільненням хімічної енергії заряду (пороху або іншої пальної суміші). До зброї, яка є предметом злочину, належать всі види бойової, спортивної, нарізної мисливської зброї, а також атипічна зброя, кустарно виготовлені чи перероблені, а також історичні зразки зброї (гармати, міномети, кулемети, автомати, карабіни, гвинтівки, пістолети та револьвери тощо).

Боєприпаси – це патрони до нарізної вогнепальної зброї різних калібрів, артилерійські снаряди, бомби, міни, гранати, бойові частини ракет і торпед та інші вироби в зібраному

вигляді, споряджені вибуховою речовиною і призначені для стрільби з вогнепальної зброї чи для вчинення вибуху.

Вибухові речовини – це порох, динаміт, тротил, нітрогліцерин та інші хімічні речовини, їх сполуки або суміші, здатні вибухнути без доступу кисню.

Вибухові пристрої – це саморобні чи виготовлені промисловим способом вироби одноразового застосування, спеціально підготовлені та за певних обставин спроможні за допомоги використання хімічної, теплової, електричної енергії або фізичного впливу (вибуху, удару) створити вражаючі фактори – спричинити смерть, тілесні ушкодження чи істотну матеріальну шкоду – способом вивільнення, розсіювання або впливу токсичних хімічних речовин, біологічних агентів, токсинів, радіації, радіоактивного матеріалу, інших подібних речовин.

Радіоактивні матеріали – це речовини, здатні до самовільного радіоактивного розпаду, що супроводжується виділенням тепла, а також альфа-, бета й гама-випромінюванням, порядок обігу яких регламентовано спеціальними нормативними актами. Предметом кримінального правопорушення, передбаченого ст. 265, радіоактивні матеріали є за умови, що кількість речовини та інтенсивність випромінювання настільки великі, що здатні заподіяти шкоду здоров'ю людини. До радіоактивних матеріалів КК України відносить джерела іонізуючого випромінювання, радіоактивні речовини та ядерні матеріали.

Під радіоактивними речовинами слід розуміти ядерне паливо, яке може виділяти енергію шляхом самопідтримуваного ланцюгового процесу ядерного поділу поза ядерним реактором, радіоактивні продукти та відходи, а також речовини природного або штучного походження, що містять у своєму складі радіоактивні ізотопи, які здатні до первісного випромінювання (руда уранова або торієва, уран-233, плутоній-239, америцій-242 тощо).

Джерела іонізуючого випромінювання – це фізичні об'єкти, крім ядерних установок, що містять радіоактивну речовину, або технічні пристрої, які створюють або за певних умов можуть створювати іонізуюче випромінювання. Під іонізуючим випромінюванням розуміють потік електричне заряджених часток, тобто електромагнітні чи корпускулярні промені, які випускаються джерелами іонізуючого

випромінювання. До джерел іонізуючого випромінювання належать, зокрема, транспортні засоби, устаткування, інші предмети, що побували в зонах радіаційного забруднення і набули радіоактивності.

Ядерні матеріали – це ядерне паливо, за винятком природного урану і збідненого урану, яке може виділяти енергію шляхом самопідтримуваного ланцюгового процесу ядерного поділу поза ядерним реактором самостійно або у комбінації з будь-яким іншим матеріалом, та радіоактивні продукти і відходи, за винятком невеликої кількості радіоактивних продуктів, радіоактивних відходів та ядерного палива, що встановлюються нормами, правилами і стандартами з ядерної і радіаційної безпеки, за умови, що ця кількість не перевищує максимальні межі, встановлені Радою керуючих Міжнародного агентства з атомної енергії.

Наркотичні засоби – це речовини природні чи синтетичні, препарати, рослини, включені до Переліку наркотичних засобів, психотропних речовин і прекурсорів, затвердженого постановою Кабінету Міністрі України «Про затвердження Переліку наркотичних засобів, психотропних речовин і прекурсорів» від 6 травня 2000 р. № 770 (далі – Перелік).

Наркотичні засоби *рослинного походження* – похідні різних сортів конопель (каннабісу смола, каннабісу олія тощо), опійні препарати (опій, ацетильований опій, екстракційний опій) тощо. *Напівсинтетичні* наркотичні засоби – отримують шляхом синтезування наркотичних засобів рослинного походження (героїн, кокаїн). *Синтетичні* наркотичні засоби – отримують у хімічних лабораторіях (часто кустарних) із різних хімічних речовин (перветин, метадон, фенамін, фентаніл та ін.). До них також належать наркотичні лікарські засоби. Зловживання наркотичними засобами призводить до захворювання на наркоманію.

Психотропні речовини – речовини природні чи синтетичні, препарати, природні матеріали, включені до Переліку. До психотропних речовин відносять: амфетамін, барбітал, діазепам, ЛСД, мескалін, тетрагідроканнабінол, феназепам тощо;

Прекурсори – речовини, які використовуються для виробництва, виготовлення наркотичних засобів, психотропних речовин, включені до Переліку (наприклад, ацетон, етиловий

спирт, ефедрин, ангідрид оцтової кислоти, соляна та сірчана кислоти, толуол тощо). У Переліку прекурсори згруповано у два списки. Список № 1 містить перелік прекурсорів, обіг яких обмежено та щодо яких встановлено заходи контролю. Йдеться про хімічні речовини та їх солі, під час переробки яких можна одержати синтетичні наркотичні чи психотропні речовини: ергометрин, ефедрин, лізергінова кислота, фенілацетон та ін. У Списку № 2 Переліку перелічено прекурсори, обіг яких не обмежено, але стосовно яких установлено заходи контролю. Ці прекурсори – розчинники, окислювачі й інші хімікати промислового чи побутового призначення – використовуються в процесі виготовлення наркотичних або психотропних речовин (наприклад, ангідрид оцтової кислоти, ацетон, етиловий ефір, калію перманганат, сірчана кислота, соляна кислота).

Аналоги наркотичних засобів і психотропних речовин – заборонені до обігу на території України речовини синтетичні чи природні, що не включені до Переліку, хімічна структура та властивості яких подібні до хімічної структури та властивостей наркотичних засобів і психотропних речовин, психоактивну дію яких вони відтворюють. Зазвичай наркотики–аналоги виготовляють при створенні нового фармацевтичного препарату, під час якого визначається та вивчається низка речовин, що мають порівнювані властивості, але дещо відрізняються своєю молекулярною структурою. На даний час механізм притягнення до кримінальної відповідальності за вчинення протиправних діянь з аналогами наркотичних засобів і психотропних речовин в Україні не врегульований.

Обладнання, призначене для виготовлення наркотичних засобів, психотропних речовин або їх аналогів. Під таким обладнанням розуміють апарати, пристрої, прилади, за допомогою яких ці засоби й речовини виготовляються (наприклад, конденсаційна труба, випарник, генератор пари, прес, необхідні для виготовлення гашишу), чи окремі вузли, деталі відповідного агрегата (наприклад, насос для відсмоктування фільтрата при перегонці опію). Використані для виготовлення наркотичних засобів, психотропних речовин або їх аналогів побутові предмети (кухонний посуд, млинок для кави, м’ясорубка тощо) обладнанням, призначеним для цієї мети, не визнаються. Не належать до зазначеного обладнання й

такі предмети медичного призначення, як шприци, стандартні флакони для розфасування ліків, скляні відвідні трубки та ін.

Документи (незаконно виготовлені, підроблені чи незаконно одержані), які дають право на отримання наркотичних засобів, психотропних речовин або прекурсорів – це документи, які безпосередньо засвідчують таке право (зокрема, ліцензія, рецепт, довіреність, товарно-транспортна накладна).

Отруйні речовини – це отрути, токсини (бойові, лікарські, сільськогосподарські та інші), які, потрапляючи всередину організму людини через органи дихання, травлення або через шкіру, здатні викликати смерть людини або психоневрологічний розлад, порушення дихання чи функції серцево-судинної системи, ураження нирок (нефропатію) чи печінки (гепатопатію) тощо. Вони можуть бути мінерального (миш'як, стрихнін, ртуть, сулема, синильна кислота та інші ціаніди, пестициди тощо), рослинного (отрута, виділена із мухомора, блідої поганки тощо), тваринного (зміїна отрута та отрута, що виробляється членистоногими тваринами) або змішаного чи штучного (хімічного) походження. Обіг та перелік отруйних речовин регламентується постановою Кабінету Міністрів України від 20 червня 1995 р. № 440 «Про затвердження Порядку одержання дозволу на виробництво, зберігання, транспортування, використання, захоронення, знищення та утилізацію отруйних речовин, у тому числі продуктів біотехнології та інших біологічних агентів».

Сильнодіючі речовини – це лікарські, побутові, промислові та інші хімічні речовини, здатні своїм впливом на живий організм заподіяти йому шкоди (це, зокрема, аміназин, бісептол, гросептол, еритроміцин, ефералган, камфора, корвалол, ністатин, нітрогліцерин, новокаїн, сульфадимезин, тетрациклін, фурацилін, деякі інсуліни та вітаміни, кислота нікотинова, настойки женьшеню і прополісу, розчин йоду спиртовий). До сильнодіючих речовин належать й інші кислоти, луги, солі.

Отруйні лікарські засоби – це лікарські засоби, віднесені до отруйних Міністерством охорони здоров'я України.

Сильнодіючі лікарські засоби – лікарські засоби, віднесені до сильнодіючих Міністерством охорони здоров'я України.

Перелік отруйних та сильнодіючих лікарських засобів затверджений наказом Міністерства охорони здоров'я України

від 17 серпня 2007 р. № 490. Це, зокрема, атропін, кетамін (отруйні лікарські засоби) та буторфанол, клофелін, прометазин (сильнодіючі лікарські засоби). Кількість отруйних та сильнодіючих лікарських засобів, які знаходяться у незаконному обігу, що становить великі та особливо великі розміри, затверджено наказом Міністерства охорони здоров'я України 31 серпня 2007 р. № 511. Крім вказаних нормативних документів обіг отруйних та сильнодіючих лікарських засобів регулюється наказами Міністерства охорони здоров'я України: «Про затвердження Правил зберігання та проведення контролю якості лікарських засобів у лікувально-профілактичних закладах» від 16 грудня 2003 р. № 584; «Про затвердження Правил проведення утилізації та знищення неякісних лікарських засобів» від 8 липня 2004 р. № 349; «Про затвердження Порядку відпуску лікарських засобів і виробів медичного призначення з аптек та їх структурних підрозділів» від 19 липня 2005 р. № 360.

Фальсифіковані лікарські засоби – це лікарські засоби, які умисно промарковані неідентично (невідповідно) відомостям (одній або кільком з них) про лікарський засіб з відповідною назвою, що внесені до Державного реєстру лікарських засобів України, а так само лікарські засоби, умисно підроблені в інший спосіб, що не відповідають відомостям (одній або кільком з них), у тому числі щодо складу, про лікарський засіб з відповідною назвою, що внесені до Державного реєстру лікарських засобів України (стаття 2 Закону України «Про лікарські засоби»).

1.1.2. Об'єктивна та суб'єктивна сторони

Об'єктивна сторона кримінального правопорушення полягає вчиненні суспільно небезпечних діянь у вигляді незаконного збуту з використанням мережі Інтернет речовин та предметів, заборонених для вільного обігу: 1) радіоактивних матеріалів (радіоактивних речовин, джерел іонізуючого випромінювання, ядерних матеріалів), 2) вогнепальної зброї, вибухових речовин, вибухових пристроїв, 3) наркотичних засобів, психотропних речовин, прекурсорів, 4) обладнання, призначеного для виготовлення наркотичних засобів,

психотропних речовин або їх аналогів, 5) документів, що дають право на отримання наркотичних засобів, психотропних речовин або прекурсорів, 6) отруйних речовин, сильнодіючих речовин, 7) отруйних лікарських засобів, сильнодіючих лікарських засобів, 8) фальсифікованих лікарських засобів.

Під збутом розуміють будь-які способи оплатного чи безоплатного розповсюдження предметів та речовин, заборонених для вільного обігу, серед невизначеного кола осіб (продаж, дарування, обмін, сплата боргу, позичання тощо). Збут передбачає відчуження вищезазначених предметів, речовин іншій особі, яка може розпоряджатися ними (або їх частиною) як своїм майном. Для настання відповідальності достатньо факту збуту хоча б одного предмету чи речовини хоча б одній особі.

Збут забороненого контенту вражається ***незаконним***, якщо він здійснюється з порушенням норм, які регламентують порядок обігу предметів та речовин, заборонених для вільного обігу.

Суб'єктивна сторона цих кримінальних правопорушень характеризується прямим умислом щодо збуту заборонених до обігу речовин чи предметів, а також метою отримання вигоди. Про умисел на збут можуть свідчити як відповідна домовленість з особою, яка придбала чи виготовила ці предмети або речовини, так і сукупність інших обставин: їх упаковка та розфасовка, наявність сировини для їх виготовлення, кількість в великому або особливо великому розмірі тощо.

1.2. Кримінально-правова характеристика правопорушень, що пов'язані з розміщенням у мережі Інтернет забороненої інформації

До кримінальних правопорушень, що пов'язані з розміщенням в мережі Інтернет забороненої інформації, відносять такі:

– розповсюдження у мережі Інтернет відомостей, що становлять державну або іншу таємницю, яка охороняється законом (ст. 114, 145, 159, 168, 232, 328, 361^2, 381, 387, 422);

– розповсюдження у мережі Інтернет порнографічних предметів та зображень, творів, що пропагують культ

насильства та жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 161, 300, 301);

– завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (ст. 259);

– публічні заклики, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади (стаття 109), заклики до вчинення дій, що загрожують громадському порядку (ст. 295).

1.2.1. Предмет кримінального правопорушення

Розповсюдження в мережі Інтернет відомостей, що становлять державну або іншу таємницю, яка охороняється законом

До даної групи кримінальних правопорушень належать такі: незаконне розголошення лікарської таємниці (ст. 145), порушення таємниці голосування (ст. 159), розголошення таємниці усиновлення (удочеріння) (ст. 168), розголошення комерційної таємниці (ст. 232), розголошення державної таємниці (ст. 328), несанкціоноване розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361^2), розголошення відомостей про заходи безпеки щодо особи, взятої під захист (ст. 381), розголошення даних досудового слідства та дізнання (ст. 387), розголошення відомостей військового характеру, що становлять державну таємницю (ст. 422).

Лікарська таємниця – певним чином задокументована інформація про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя особи. Лікарську таємницю (інформацію про пацієнта) слід відрізняти від медичної таємниці (інформації для пацієнта). Остання передбачає відомості про стан здоров'я людини, історію її хвороби, про мету запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, які лікар зобов'язаний надати на вимогу пацієнта, членів його сім'ї або

законних представників, за винятком випадків, коли така повна інформація може завдати шкоди здоров'ю пацієнта.

Таємниця голосування – це конфіденційна інформація про волевиявлення особи під час голосування, що належить конкретному виборцю та щодо якої він самостійно встановлює режим доступу.

Таємниця усиновлення (удочеріння) – це конфіденційна інформація про факт та умови усиновлення, яка належить усиновителю і розголошення якої може призвести до суспільно небезпечних наслідків (тяжких особистих і сімейних трагедій та конфліктів, розриву сімейних відносин тощо).

Комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з такою інформацією, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію. Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Державна таємниця – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки і охорони правопорядку, розголошення. якої може завдати шкоди національній безпеці України і які рішенням державних експертів з питань таємниць визнано державною таємницею та включено до Зводу відомостей, що становлять державну таємницю (затверджений наказом Служби безпеки України 12.08.2005 № 440). З моменту опублікування вказаного Зводу (змін до нього) ці відомості підлягають охороні з боку держави як такі, що становлять державну таємницю, хоча б на цей час вони ще не були матеріалізовані.

Інформація з обмеженим доступом – інформація, доступ до якої має лише обмежене коло осіб і оприлюднення якої заборонено законом. Обмеження доступу до інформації здійснюється виключно в інтересах національної безпеки або охорони прав людини. До інформації з обмеженим доступом

належить *конфіденційна, службова й таємна інформація*. Будь-яка інша інформація вважається відкритою і отримати доступ до неї мають право всі громадяни України, незалежно від того, стосується їх ця інформація безпосередньо чи ні.

Конфіденційною інформацією є відомості, які перебувають у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Службова інформація – це інформація: 1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо ці документи пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень; 2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці. Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф «для службового користування».

Таємна інформація – інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю слідства та іншу передбачену законом таємницю.

Відомості про заходи безпеки щодо особи, взятої під захист – інформація про особисту охорону, охорону житла і майна особи, взятої під захист відповідно до чинного законодавства, про зміну місця роботи або навчання, про переселення в інше місце проживання, про зміну прізвища чи інших конфіденційних відомостей про цю особу тощо.

Дані досудового слідства – це такі відомості, які: а) стосуються обставин розслідуваного кримінального правопорушення, підозрюваних чи обвинувачених у ньому осіб та інших доказів у кримінальній справі; б) отримані в ході здійснення дізнання чи досудового слідства; в) закріплені або підлягають закріпленню в матеріалах кримінальної справи у встановленому законом процесуальному порядку;

г) не підлягають оголошенню без спеціального на те дозволу з боку уповноважених на це осіб.

Кримінальне правопорушення визнається закінченим з того моменту, коли дані досудового слідування, щодо яких є заборона на їх розголошення, стали надбанням будь-якої особи, яка не має права на ознайомлення з ними. Такими особами можуть бути як ті, хто бере участь у справі (наприклад, інші свідки), так і сторонні особи, які не мають відношення до справи.

Відомості військового характеру, що становлять державну таємницю – це інформація, що належить до державної таємниці у сфері оборони. Конкретні відомості можуть бути віднесені до державної таємниці за грифами (ступенями) секретності «особливої важливості», «цілком таємно» і «таємно» лише за умови, що вони належать до зазначеної категорії і їх розголошення завдаватиме шкоди інтересам національної безпеки України.

Розповсюдження у мережі Інтернет порнографічних предметів та зображень, творів, що пропагують культ насильства та жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію

Порнографія – вульгарно-натуралістична, цинічна, непристойна фіксація статевих актів, самоцільна, спеціальна демонстрація геніталій, сексуальних збочень, які не відповідають моральним критеріям, ображають честь і гідність людини, спонукаючи негідні інстинкти.

Критерії віднесення предметів та зображень до порнографії зазначені в рекомендаціях Національної експертної комісії України з питань захисту суспільної моралі «Щодо визначення ознак віднесення друкованої, аудіовізуальної, електронної та іншої продукції, а також переданих та отриманих по комунікаційних лініях повідомлень та матеріалів до продукції порнографічного характеру»[1]. До таких критеріїв належать, зокрема: натуралістична, самоцільна демонстрація статевих органів, природного та протиприродного статевого акту; демонстрація деталізації та смакування акту статевого

[1] http://www.moral.gov.ua/documents/39

насильства; демонстрація сексуальних девіацій; розбещення дітей; відсутність художньої цінності тощо.

Дитяча порнографія – зображення у будь-який спосіб дитини чи особи, яка виглядає як дитина, задіяної у реальній або змодельованій відверто сексуальній поведінці, або будь-яке зображення статевих органів дитини в сексуальних цілях.

Продукцією порнографічного характеру можуть бути визнані будь-які матеріальні або матеріалізовані об'єкти, предмети, друкована, аудіо-, відеопродукція, в тому числі реклама, повідомлення та матеріали, продукція засобів масової інформації, електронних засобів масової інформації, пов'язані із задоволенням сексуальних потреб людини.

До творів, що пропагують культ насильства та жорстокості належать твори, що відповідають ознакам, зазначеним у рекомендаціях Національної експертної комісії України з питань захисту суспільної моралі «Щодо визначення ознак віднесення друкованої, аудіовізуальної, електронної та іншої продукції, а також переданих та отриманих по комунікаційних лініях повідомлень та матеріалів до продукції, що пропагує культ насильства та жорстокості»[2]. До таких ознак належать, зокрема: прямі заклики до насильства (тобто застосування (загрози застосування) сили як вияву своєї волі відносно інших, що обмежує можливості дій на власний розсуд того, на кого спрямоване) та жорстокості (байдужості до страждань людей або ж прагнення до їх спричинення); відтворення насильства та жорстокості в натуралістичній формі й в ореолі позитивного відношення до нього; нагнітання жаху тощо.

До творів, що пропагують расову, національну, релігійну нетерпимість та дискримінацію належать твори, що відповідають ознакам, зазначеним у рекомендаціях Національної експертної комісії України з питань захисту суспільної моралі «Щодо визначення ознак віднесення друкованої, аудіовізуальної, електронної та іншої продукції, а також переданих та отриманих по комунікаційних лініях повідомлень та матеріалів до продукції, що пропагує національну та релігійну ворожнечу...»[3]. До таких ознак

[2] http://www.moral.gov.ua/documents/41
[3] http://www.moral.gov.ua/documents/40

належать, зокрема: формування почуттів, настроїв неприязні, ворожнечі, огиди до представників інших расових, етнічних груп чи релігій; публічне підбурювання до вигнання за межі України чи переселення в інші регіони представників певної расової, етнічної чи релігійної належності; перешкоджання звичаєвій поведінці представників певної національності чи релігії; наруга, заклики до знищення чи пошкодження пам'ятників, пам'яток історичної та культурної спадщини, споруд, які є релігійною чи культурною цінністю тощо.

Твори порнографічного характеру, твори, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію, що розповсюджуються в мережі Інтернет, впливають на свідомість особи, яка сприймає її зміст, шляхом:

– візуального сприйняття: 1) статичні зображення (малюнки, фотографії тощо); 2) динамічні зображення (анімації та фільми без звукового супроводу); 3) електронні тексти протиправного змісту;

– сприйняття органами слуху (мовлення у прозовій, віршованій або пісенній формі);

– аудіовізуального сприйняття (художні, документальні, мультиплікаційні фільми, телевистави тощо);

– інтерактивного сприйняття (комп'ютерні ігри).

Предметом кримінального правопорушення є інформація протиправного характеру, яка зберігається на носіях, вилучених у правопорушника (комп'ютери, переносні «вінчестери», флеш-картки пам'яті, оптичні компакт-диски, комп'ютерні дискети тощо), або ж в Інтернет-ресурсі, що його формує правопорушник на відповідному сервері.

Обов'язковою ознакою об'єктивної сторони цих кримінальних правопорушень є використання правопорушником предмета злочину не для власних потреб, а розповсюдження його через мережу Інтернет серед необмеженого кола осіб.

Завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності

Неправдиве повідомлення – це неправдива інформація, що не відповідає дійсності, про нібито існуючу підготовку вибуху, підпалу або інших подібних дій, доведена до відома будь-якої особи. Предметом кримінального правопорушення є повідомлення, що міститься на Інтернет-ресурсі у вигляді тексту, зображення, аудіо- або відеофайлів тощо, яке доведене до широкого кола осіб за допомогою мережі Інтернет чи повідомлене таким же шляхом хоча б одній особі з тим, щоб воно набуло дальшого поширення. За своїм змістом воно стосується здійснення в майбутньому загальнонебезпечних дій, які становлять об'єктивну сторону, зокрема, терористичного акту, і є безсумнівно неправдивим.

Публічні заклики, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, а також заклики до вчинення дій, що загрожують громадському порядку

Публічні заклики передбачають хоча б одне відкрите звернення з використанням мережі Інтернет у вигляді текстового, відео-, аудіо- чи іншого формату до невизначеного, але значного кола осіб, в якому висловлюються ідеї, погляди чи вимоги, спрямовані на те, щоб шляхом поширення їх серед населення чи його окремих категорій (представників влади, військовослужбовців тощо) схилити певну кількість осіб до певних дій.

Якщо такі заклики звернені до конкретної особи, вони кваліфікуються як підбурювання до вчинення дій, метою яких є насильницька зміна чи повалення конституційного ладу, захоплення державної влади або вчинення дій, що загрожують громадському порядку. Публічність є оціночною ознакою, і питання про наявність її має вирішуватися в кожному конкретному випадку з урахуванням часу, місця, обстановки здійснення закликів тощо.

Публічні заклики можуть здійснюватись у формі *розповсюдження матеріалів*, яке полягає в діях, спрямованих на доведення змісту відповідних матеріалів до відома багатьох

людей (невизначеної їх кількості або певного кола) з використанням мережі Інтернет. Закінченим злочин є з моменту початку розповсюдження, виготовлення чи зберігання відповідних матеріалів.

Конституційний лад включає встановлені Конституцією України основні засади життєдіяльності суспільства, держави і людини в Україні. Його складовими є: 1) суверенітет держави (верховенство і самостійність державної влади усередині країни та незалежність у міжнародних відносинах); 2) форма правління (спосіб організації державної влади, за яким єдиним органом законодавчої влади в Україні є Верховна Рада України, главою держави – Президент України, вищим органом виконавчої влади – Кабінет Міністрів України тощо); 3) державний устрій (унітарний з відповідним поділом владних повноважень між вищими і центральними та місцевими органами державної влади) та цілісність території; 4) державний режим (демократичний, що, зокрема, передбачає можливість здійснення народного волевиявлення через вибори, референдум та інші форми безпосередньої демократії, гарантії місцевого самоврядування, захист державою прав і свобод людини і громадянина, ґрунтування суспільного життя на засадах політичної, економічної та ідеологічної багатоманітності).

Державна влада – це система сформованих у порядку, передбаченому Конституцією та законами України, органів, які уособлюють собою владу глави держави, законодавчу, виконавчу і судову владу – Президент України, парламент, вищі, центральні та місцеві органи виконавчої влади, вищі та місцеві органи судової влади, – а також органи місцевого самоврядування, контрольно-наглядові та деякі інші органи, які, маючи певну незалежність, de jure не належать до трьох основних гілок влади (прокуратура України, Національний банк України, Рахункова палата України, Вища рада юстиції України тощо). Таким чином, існуюча в Україні державна влада має відповідати її конституційному ладу.

Громадський порядок – це урегульована правовими та іншими соціальними нормами система суспільних відносин, що забезпечує захист прав і свобод громадян, їх життя і здоров'я, повагу честі та людської гідності, дотримання норм суспільної моралі. У широкому значенні громадський порядок є системою,

порядком суспільних відносин, що складаються під впливом соціальних норм при провідній ролі правових норм. У вузькому значенні громадський порядок розуміють як систему відносин, що складаються при знаходженні громадян у громадських (доступних для населення) місцях.

1.2.2. Об'єктивна та суб'єктивна сторони

Розповсюдження в мережі Інтернет відомостей, що становлять державну або іншу таємницю, творів, зображень, предметів порнографічного характеру або творів, що пропагують культ насильства та жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію – це будь-яка дія, за допомогою якої зазначені об'єкти безпосередньо чи опосередковано пропонуються публіці, зокрема доводяться до відома невизначеного кола осіб таким чином, що особи мають можливість здійснити вільний доступ до цих об'єктів за власним вибором. Розповсюдження контенту у мережі Інтернет може проводитись у формі його опублікування, дарування, показу, відкриття доступу до свого комп'ютера, сервера чи іншого носія інформації, демонстрації та інших дій, внаслідок яких відомості сприймається іншими особами.

Під *збутом* відомостей, що становлять державну або іншу таємницю, творів, зображень або предметів порнографічного характеру тощо, розуміють їх оплатне або безоплатне відчуження (продаж, дарування, передача в якості повернення боргу тощо) хоча б одній особі.

Збут або розповсюдження забороненого контенту слід вважати *несанкціонованим,* якщо ці дії вчинені без дозволу (згоди) власника цього контенту. Несанкціоновані збут або розповсюдження містять ознаки кримінального правопорушення як в тому випадку, коли вони вчинені особою, якій в установленому порядку було надано доступ до відповідної інформації, так і у випадку вчинення їх особою, яка такого доступу не мала.

Розповсюдження творів, зображень або предметів через мережу Інтернет може відбуватися й у формі спілкування в цій мережі.

Спілкування в мережі Інтернет – процес обміну електронними повідомленнями між двома та більше комп'ютерними пристроями, що підключені до Інтернету й передають ці повідомлення у вигляді пакетів даних, створюваних та оброблюваних на основі стандартів протоколу IP. Відповідне спілкування може відбуватися як у вигляді безпосереднього обміну повідомленнями між учасниками спілкування, так і опосередковано, через публічні Інтернет-ресурси: сайти, форуми, чати, блоги, дошки повідомлень тощо. Повідомлення можуть бути у вигляді тексту, малюнків, фотозображень, в аудіо- та відеоформаті. Спілкування може бути як в режимі реального часу, так і з відстрочкою отримання повідомлення адресатом (адресатами).

Під *розміщенням* контенту треба розуміти процес публікації інформації за допомогою комп'ютерного пристрою, що підключений до мережі Інтернет. Розміщення даних, як правило відбувається на власних або публічних Інтернет-ресурсах: порталах, сайтах, веб-сторінках, форумах, чатах, блогах, дошках повідомлень тощо. Розміщені дані можуть бути у вигляді тексту, графічних об'єктів, аудіо та відеофайлів.

Реклама контенту, що містить ознаки порнографії або пропаганди культу насильства і жорстокості – це інформація про такий контент, призначена для формування або підтримання обізнаності споживачів реклами та їх інтересу щодо такого контенту. Розповсюдження цієї реклами може здійснюватись, зокрема, через мережу Інтернет.

Розголошення відомостей, що становлять державну або іншу таємницю, яка охороняється законом – розміщення цих відомостей в мережі Інтернет без згоди їх власника, внаслідок чого з цими відомостями безпосередньо чи опосередковано можуть ознайомлюватись певні особи чи невизначене коло осіб. Обсяг розголошених відомостей для кваліфікації кримінального правопорушення значення не мають.

Суб'єктивна сторона кримінальних правопорушень, що розглядаються, зазвичай характеризується прямим умислом і метою розповсюдити заборонений до обігу контент, збути заборонені до обігу предмети.

РОЗДІЛ 2
НАПРЯМИ ВСТАНОВЛЕННЯ КОМП'ЮТЕРНОЇ ТЕХНІКИ, ЩО ВИКОРИСТОВУВАЛАСЯ ДЛЯ РОЗПОВСЮДЖЕННЯ В МЕРЕЖІ ІНТЕРНЕТ ЗАБОРОНЕНОГО КОНТЕНТУ

2.1. Загальний порядок проведення слідчих (розшукових) та негласних слідчих (розшукових) дій за фактом розповсюдження в мережі Інтернет забороненого контенту

1). Отримання та реєстрація в Єдиному реєстрі досудових розслідувань (ст. 214 КПК України) заяви, повідомлення про вчинення кримінального правопорушення, пов'язаного з обігом забороненого контенту.

2). Виїзд слідчо-оперативної групи на місце події. Огляд місця події, під час якого:

а) оглядають комп'ютерне обладнання, на якому був виявлений заборонений контент, засоби комунікації, а також навколишню обстановку.

Під час огляду на комп'ютерному обладнанні та засобах комунікації виявляють заборонений контент або ознаки його перебування там, документують проведення огляду місця події.

При цьому:

– щоб зберегти сторінку з екрану, де зображено заборонений контент, робиться скріншот цього зображення. В операційній системі Windows відкривають в браузері сторінку із забороненим контентом. У подальшому, натискаючи клавішу Print Screen у правому верхньому куті клавіатури, здійснюють копіювання зображення екрану монітору в буфер обміну. Надалі слід перейти у вікно Microsoft Word і вставити скопійовану сторінку сайту із буферу обміну; зберегти документ на диску у форматі .doc, роздрукувати його (за можливістю) й додати до протоколу огляду місця події:

– також слід зафіксувати посилання на сторінку сайту (файл) у каталозі обраного в браузері, що використовується. Зокрема, для браузера Microsoft Internet Explorer необхідно вибрати з меню «Сервис» – «Панели Explorer» – «Избранное» команду «Добавить в избранное», в діалоговому вікні

«Добавление в избранное» встановити прапорець «Сделать доступно автономно», обрати місце збереження й натиснути кнопку «ОК» (Рис. 1.);

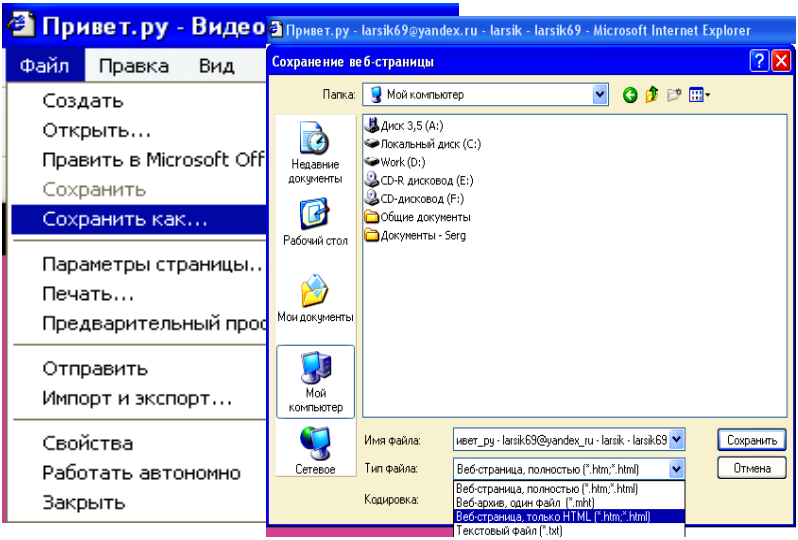

Рис. 1

– фіксується документ (файл) із забороненим контентом для перегляду сторінки сайту в режимі офф-лайн. Для створення цього документу потрібно скористатися функ-цією збереження веб-сайту, яка реалізована у Microsoft Internet Explorer. Виберіть з меню «Файл» команду «Сохранить как…». З'явиться діалогове вікно «Сохранение веб-страницы». Зі списку, що розкривається «Тип файла:» оберіть варіант для збереження сторінки: «Веб-страница, полностью (*.htm;*.html)»; «Веб-архив, один файл (*.mht)» або «Веб-страница, только HTML (*.htm;*.html)». Після цього слід натиснути кнопку «Сохранить», і сторінка почне завантажуватися й буде збережена на жорсткому диску (Рис. 2);

– далі слід створити копію сторінки сайту (файл) на жорсткому диску за допомогою спеціальної утиліти, наприклад: HTTrack Website Copier. Ця утиліта дозволяє викачувати сайти на жорсткий диск і переглядати їх в режимі офф-лайн. HTTrack рекурсивно створює всі директорії сайту і відтворює тим самим його оригінальну структуру. Після закачування користувач має можливість відкрити сайт у будь-якому браузері і переходити на сторінки по посиланнях так само, як це робиться в режимі он-лайн. Програма HTTrack автоматично відновлює розірвані з'єднання, підтримує функцію оновлення вже викачаних сайтів, містить інтегровану довідкову систему;

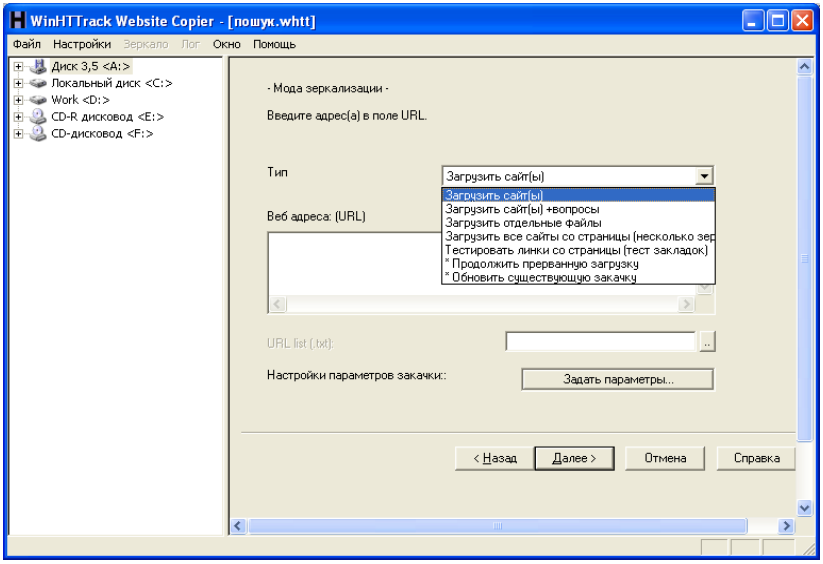

Рис. 2. Утиліта HTTrack Website Copier

– вилучають інші засоби, речовини та предмети, які засвідчують протиправну діяльність.

б) відбирають пояснення у осіб, які можуть бути свідками або очевидцями обігу забороненого контенту.

3). Внесення до Єдиного реєстру досудових розслідувань відомостей, отриманих за результатами огляду місця події, відкриття кримінального провадження, початок досудового розслідування та направлення письмового повідомлення про це прокурору (ч. 6 ст. 214 КПК України).

4). В рамках кримінального провадження здійснення таких слідчих (розшукових) та негласних слідчих (розшукових) дій:

а) направлення на експертизу вилучених з місця події предметів, речовин та слідів;

б) встановлення IP-адреси, комп'ютерної техніки та засобів комунікації, з яких здійснювалося розповсюдження забороненого контенту;

в) направлення запитів до Інтерет-провайдерів стосовно надання інформації щодо користувачів Інтернет-сайтів та власників поштових скриньок:

– про реєстрацію доменного імені та хостінгу для розміщення сайту, з якого здійснювалось розповсюдження забороненого контенту;

– про реєстрацію IP-адреси чи поштової скриньки користувача Інтернет-мережі (підозрюваного);

– про адміністрування Інтернет-форуму або чату, через який здійснювалося розповсюдження забороненого контенту;

г) направлення запитів до банківських установ щодо надання інформації про рахунки, які належать юридичним та фізичним особам, що їх використовували для отримання коштів за збут забороненого контенту, а також про рух коштів по таких рахунках;

д) проведення обшуку приміщень:

– за місцем встановлення комп'ютерної техніки та засобів комунікації, з яких здійснювалося поширення забороненого контенту;

– за місцем проживання та роботи осіб, які можуть бути причетні до поширення забороненого контенту;

– у яких здійснювались незаконні операції з виготовлення та розповсюдження забороненого контенту;

– у яких підозрюваний ймовірно перебував під час виходу у мережу Інтернет;

е) проведення виїмки комп'ютерного обладнання та засобів комунікації, на яких виготовлявся та оброблявся заборонений контент;

є) проведення виїмки комп'ютерного обладнання та засобів комунікації, через які здійснювалось Інтернет-спілкування підозрюваного (Інтернет-клуби, інші приміщення, обладнанні провідним та безпровідним Інтернет-зв'язком);

ж) забезпечення тимчасового доступу до камер спостереження та огляд записів, у яких зафіксовано перебування підозрюваного у приміщеннях чи інших місцях, де він виходив у мережу Інтернет. В разі необхідності поведення виїмки відповідних технічних засобів;

з) огляд предметів, що мають відношення до кримінального правопорушення;

и) допит свідків, які були присутні при огляді;

і) допит свідків, яким відомі обставини вчиненого кримінального правопорушення, пов'язаного з розповсюдженням забороненого контенту, а також які знають підозрюваного або мають інформацію про факти вчинення ним протиправних діянь;

к) затримання та допит підозрюваного в розповсюдженні забороненого контенту;

л) відібрання (отримання) зразків, необхідних для проведення експертизи: наприклад змиви з рук (якщо проводилась оперативна чи контрольна закупівля, контрольована поставка з використанням помічених коштів);

м) призначення судових експертиз вилученого в результаті слідчих (розшукових) дій комп'ютерного обладнання та засобів комунікації (комп'ютерно-технічна), слідів рук (дактилоскопічна) та ін.;

н) призначення експертиз щодо інших предметів, вилучених в рамках кримінального провадження;

п) самостійне проведення слідчим негласних слідчих (розшукових) дій або надання доручення на проведення таких дій уповноваженим оперативним підрозділам органів внутрішніх справ;

р) приєднання до кримінального провадження документів та протоколів з відповідними додатками, які отримані в результаті проведення негласних слідчих (розшукових) дій.

Вина осіб, причетних до розповсюдження забороненого контенту, має бути також доведена:

– результатами дослідження способів передавання контенту (електронною поштою, записами на диски або на флеш-картки пам'яті);

– результатами відстеження обміну інформацією через мережу Інтернет між підозрюваним і кінцевим споживачем забороненого контенту;

– юридичним зв'язком підозрюваного з роботою на певному комп'ютері, через який розповсюджувався заборонений контент (банківські рахунки, облікові записи електронної пошти, ліцензія на програмне забезпечення, інформація про кредитну картку, замовлення для доставки з домашньою адресою тощо);

– результатами дослідження змісту жорсткого диску з комп'ютера підозрюваного зі слідами журналів роботи в Інтернеті (закладки, пошукові запити), тимчасових файлів (кеш, Cookie-файли, буфер друку, місце зберігання інформації, записаної на комп'ютер веб-сайтом), змісту своп-файла «вільне місце», списків друзів + особистих профілів + записів чат-кімнат + інших збережень «області»; відстеженням дат збереження файлів (у файлі Windows зберігаються дати створення (коли файл був створений), останнього запису (коли файл востаннє був змінений) та останнього доступу до файлу (коли файл востаннє був відкритий);

– іншими документами, які засвідчують про протиправну діяльність особи – наприклад, результати проведеної оперативної та контрольованої закупівлі, контрольної поставки чи пояснення свідків та очевидців щодо виготовлення чи збуту матеріалів із забороненим контентом тощо.

2.2. Визначення IP-адреси Інтернет-ресурсу, а також фізичної адреси за IP-адресою та доменним ім'ям

Підставами для внесення відомостей у Єдиному реєстру досудових розслідувань та початку досудового розслідування за фактом розповсюдження в мережі Інтернет забороненого контенту є:

– отримання слідчим, прокурором заяви, повідомлення про вчиненне кримінальне правопорушення;

– виявлення особисто слідчим, прокурором з будь-яких джерел обставин, що можуть свідчити про вчинення кримінального правопорушення.

Службова особа, уповноважена на прийняття та реєстрацію заяв і повідомлень про кримінальні правопорушення, вносить відповідні відомості до Єдиного реєстру досудових розслідувань (ч. 1 ст. 214 КПК України), після чого визначений керівником органу досудового розслідування слідчий негайно розпочинає досудове розслідування та невідкладно у письмовій формі повідомляє прокурора про його початок (ч. 6 ст. 214 КПК України).

Головною умовою викриття кримінальних правопорушень, пов'язаних з обігом у мережі Інтернет забороненого контенту, є встановлення місцезнаходження комп'ютерної техніки, причетної до такого обігу.

У даному випадку встановлення місцезнаходження комп'ютерної техніки відбувається за допомогою технічних особливостей функціонування Інтернет-мережі. Отже, задача встановлення особи правопорушника напряму пов'язана із встановленням IP-адреси, під якою його комп'ютер виходив у мережу Інтернет. Встановлення IP-адреси може здійснити як безпосередньо слідчий, так і, за його дорученням, оперативний працівник підрозділу по боротьбі з кіберзлочинністю.

Кожен комп'ютер у мережі Інтернет має свою унікальну адресу, яка складається з чотирьох чисел, що знаходяться в діапазоні від 0 до 255, розділених крапками. Приклад такої адреси: 192.254.55.232. Такі адреси називаються *IP-адресами* (адресами Інтернет Протоколу).

Ця система адресації базується на мережевій програмі IP версії 4 (IP v4), що використовує 32-бітову адресацію.

Слід зауважити, що сьогодні проходить експлуатаційні випробування нова версія програми Internet Protocol Next Generation (IP v6), яка використовує 128-бітну адресацію.

IP-адреса складається з *двох частин*.

Перша частина має від одного до трьох чисел, розташованих ліворуч – вона позначає мережу, у якій знаходиться комп'ютер, і називається ідентифікатором мережі. Інтернет складається з безлічі мереж, кожна з яких має власну адресу.

Друга частина має від трьох до одного чисел, розташованих праворуч – вона позначає конкретний комп'ютер у мережі і називається ідентифікатором вузла.

Таким чином, ієрархія IP-адрес читається зліва направо, тобто ліворуч розташовуються старші біти, праворуч – молодші (як-то поштова адреса: країна, місто, вулиця, будинок).

Коли особа підключається до Інтернет, її комп'ютер стає частиною мережі, тому йому має бути привласнена унікальна IP-адреса. Отримання IP-адреси здійснюється при кожному підключенні, але ця адреса щораз має нове значення з діапазону динамічних IP-адрес провайдера, через якого здійснюється підключення.

Статичні IP-адреси, як правило, закріплені за тими вузлами Інтернет, що повинні бути присутніми у мережі постійно. Це сервери, призначення яких полягає в тому, щоб обробляти запити користувачів Інтернет.

Щоб встановити IP-адресу Інтернет-ресурсу (порталу, сайту, веб-сторінки), який містить заборонений контент, слід використовувати певні програмні продукти й утиліти (ping, Trace, Figner LookUp, тощо). Найбільш простішим є використання команди ping.

Наприклад, нам необхідно встановити IP-адресу сайту privet.ru та місцезнаходження Інтернет-провайдера, який надає послуги хостингу для цього сайту. Спочатку встановлюємо IP-адресу сайту privet.ru. З цією метою необхідно у головне меню системи Windows натиснувши кнопку «Пуск», обрати пункт меню «Выполнить». У вікні «Запуск программы», яке з'явиться набрати рядок: ping privet.ru, натиснути кнопку «ОК». Результат виконання програми зображений на Рис. 3. За результатами виконання програми отримуємо інформацію про IP-адресу сайту privet.ru 64.34.89.162.

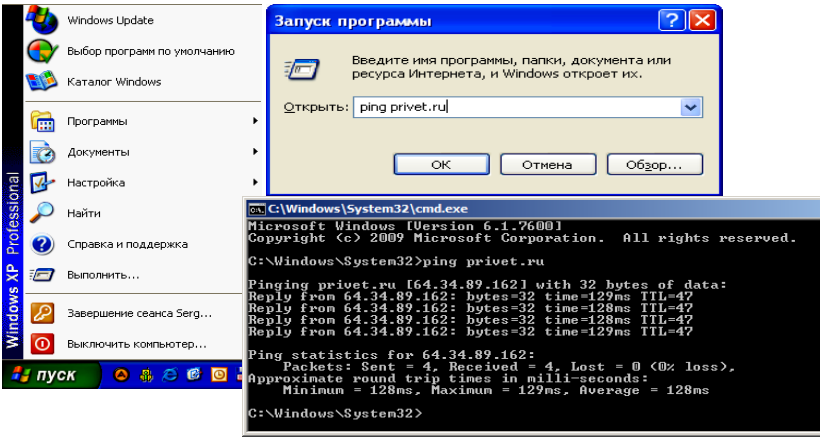

Рис. 3. Виконання команди ping у командному рядку Windows

Команда ping може бути також виконана і на інших сайтах, що надають таку можливість (як правило це сайти, що надають сервіс Whois). Для прикладу використаємо сервіс сайту DomainTools (http://dns-tools.domaintools.com/?tool=ping) з метою встановлення IP-адресу privet.ru (Рис. 4).

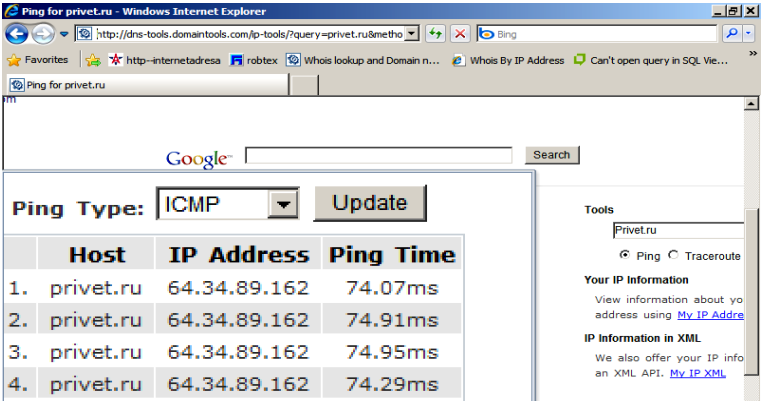

Рис. 4. Виконання команди ping на сайті DomainTools

Знаючи адресу сайту privet.ru подальшим кроком буде встановлення компанії Інтернет-провайдера (за допомогою сервісу Whois або RIPE), яка надає послуги хостингу для цього сайту і, відповідно, має технічні можливості з призупинення або закриття мережевого доступу до веб-сайту (Рис. 5).

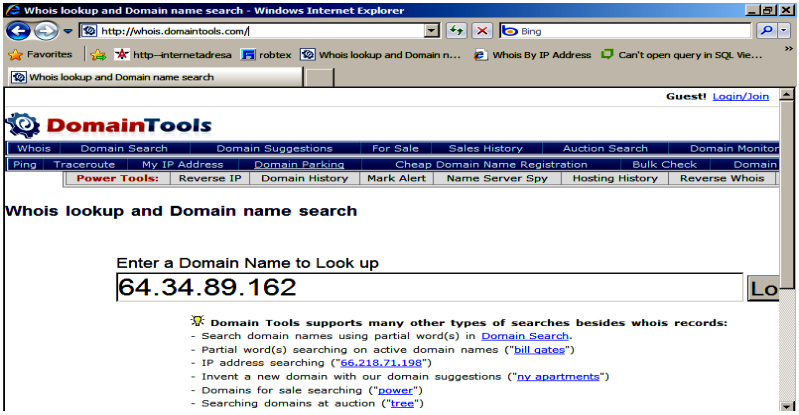

Рис. 5. Вікно сервісу Whois сайту DomainTools

Як бачимо, на запит про належність IP-адреси 64.34.89.162 отримана певна інформація (Рис. 6.1.): Інтернет-провайдером діапазону IP-адрес з 64.34.0.0. по 64.34.255.255 (куди і входить IP-адреса, якою ми цікавимося) належать компанії – Peer 1 Network Inc., її поштова адреса – 75 Broad Street, 2nd Floor, New York, 10004, USA.

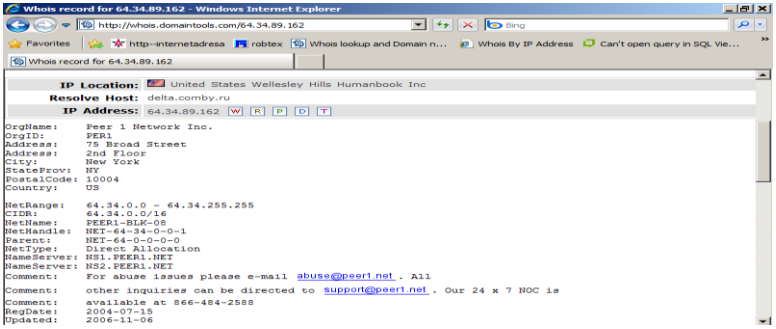

Рис. 6.1. Результат виконання запиту сервісу Whois

Рис. 6.2. Результат виконання запиту сервісу Whois

Разом з тим з вказаного діапазону IP-адрес з 64.34.89.128 по 64.34.89.191 IP-адреса, що нас цікавить (64.34.89.162), надана у користування компанії Humanbook, Inc., поштова адреса: P.O. Box 81362, Wellesley Hills, MA, 02481, US. (Рис. 6.2.).

Отже з використанням команди ping ми встановили IP-адресу сайту privet.ru, який нас цікавить, – 64.34.89.162, а також місцезнаходження Інтернет-провайдера, який надає послуги хостингу для нього: Humanbook, Inc., поштова адреса: P.O. Box 81362, Wellesley Hills, MA, 02481, US.

Система IP-адресації в комп'ютерних мережах є технічним кодом, людини нею користуватися незручно. Тому для ергономічного подання Інтернет-адрес була розроблена система *доменних імен* у вигляді літерних кодів (наприклад www.i.ua, www.google.ru, www.podrobnosti.ua).

Домен – це частина простору ієрархічних імен мережі Інтернет, що обслуговується групою серверів доменних імен (DNS-серверів) та централізовано адмініструється. Доменні імена дають можливість адресації Інтернет-вузлів і розташованих на них мережевих ресурсів (веб-сайтів, серверів електронної пошти тощо) у зручній для людини послідовності.

Домен можна розглядати як групу комп'ютерів в мережі Інтернет, логічно об'єднаних за деякою ознакою (наприклад, комп'ютери навчальних закладів, комп'ютери певної країни, комп'ютери певної організації тощо). Система доменів має ієрархічну дендритну структуру. Кожний домен (окрім доменів нижнього рівня) містить групу нижчестоящих доменів, які утворюють доменну зону. Так, доменна зона **.ua** (український сектор Інтернету) містить доменні імена другого рівня, наприклад **kiev.ua** (Інтернет-сектор Києва), **ukrtelecom.ua** (Інтернет-сектор компанії «Укртелеком») тощо. Зона **kiev.ua** містить доменні імена третього рівня, наприклад, **rock.kiev.ua** (київський клуб рок-музики)**, qs.kiev.ua** (інформаційно-розважальний портал) тощо.

Отже, повне доменне ім'я складається з безпосереднього імені локального домену й далі імен всіх доменів, до яких він входить, розділених крапками. Наприклад, повне ім'я naiau.kiev.ua означає домен третього рівня naiau, який входить до домену другого рівня kiev, який входить до домену першого (верхнього) рівня ua, який входить до безіменного домену нульового (кореневого) рівня, що позначається крапкою.

Позначення деяких доменних зон надані в таблиці:

Доменні зони деяких сфер діяльності:	**Доменні зони деяких країн:**
.com – комерційні (найпопулярніша зона Інтернету)	.au – Австралія
.net – технічні	.ca – Канада
.info – інформаційні	.de – Німеччина
.org – організації	.ru – Росія
.biz – бізнес-структури	.us – США
.gov – урядові установи	.ua – Україна
.edu – навчальні заклади	.fr– Франція
	.jp – Японія

Якщо URL певного сайту (від англ. *Uniform Resource Locator* – єдиний дороговказ ресурсів) складається лише з назви домену та імені користувача, це свідчить, що власник сайту отримує послуги хостингу з боку потужного веб-ресурсу, або ж користується персональною веб-сторінкою користувача певної соціальної мережі.

Наведемо приклад встановлення доменного імені веб-сайту http://sowa.net.ua, на якому розміщена пропозиція щодо купівлі-продажу наркотиків (Рис. 7). Натискаючи клавішу Print Screen зробимо скріншот екрану, який у подальшому збережемо у документі формату .doc.

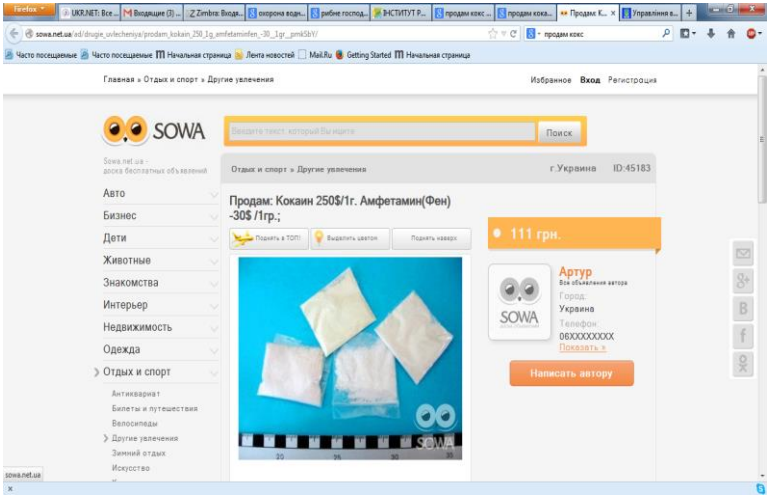

Рис. 7. Вікно сайту http:// sowa.net.ua

Встановити Інтернет-провайдера, який здійснює технічне обслуговування, технічну підтримку цього сайту та угоди з провайдером щодо надання їм послуг можливо за допомогою безоплатних сервісів Whois. Це – інформаційний сервіс, що містить інформацію про зареєстровані домени, компанії або осіб, на ім'я яких ці домени зареєстровані, і (іноді) – про системних адміністраторів, які відповідальні за системи. Окрім цього, Whois містить інформацію про власників діапазонів мережевих адрес.

Вказаний сервіс широко розповсюджений в мережі Інтернет і може бути легко знайдений за допомогою пошукових сервісів, наприклад google.com Для пошуку достатньо вказати Whois у запиті пошукової служби Google (Рис. 8).

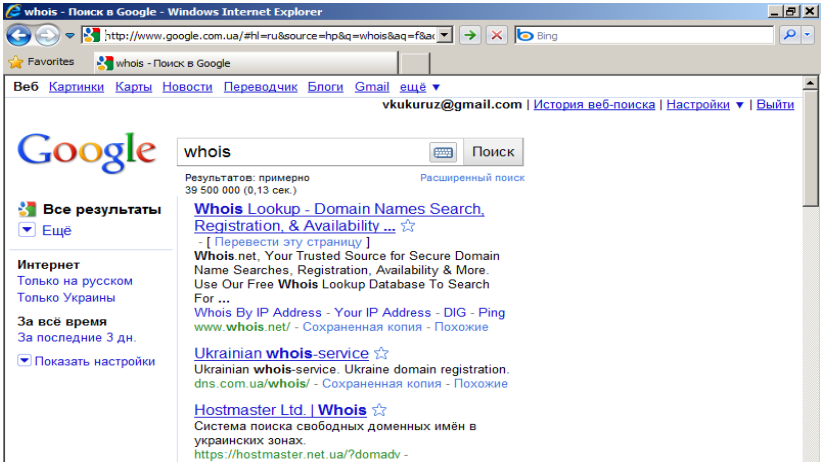

Рис. 8. Сторінка запиту пошукової служби Google

Потрапивши на сервіс Whois, слід у запиті вказати ім’я шуканого веб-сайту http://sowa.net.ua.

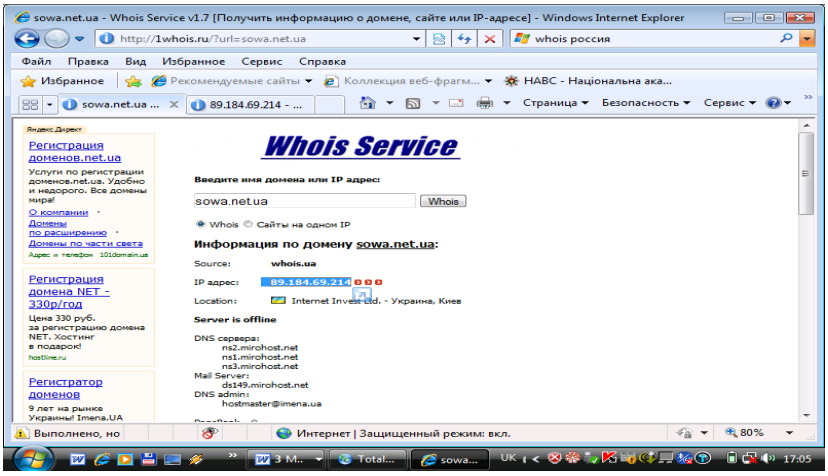

Рис. 9. Результати пошуку Інтернет-провайдера сайту http:// sowa.net.ua
(лист 1)

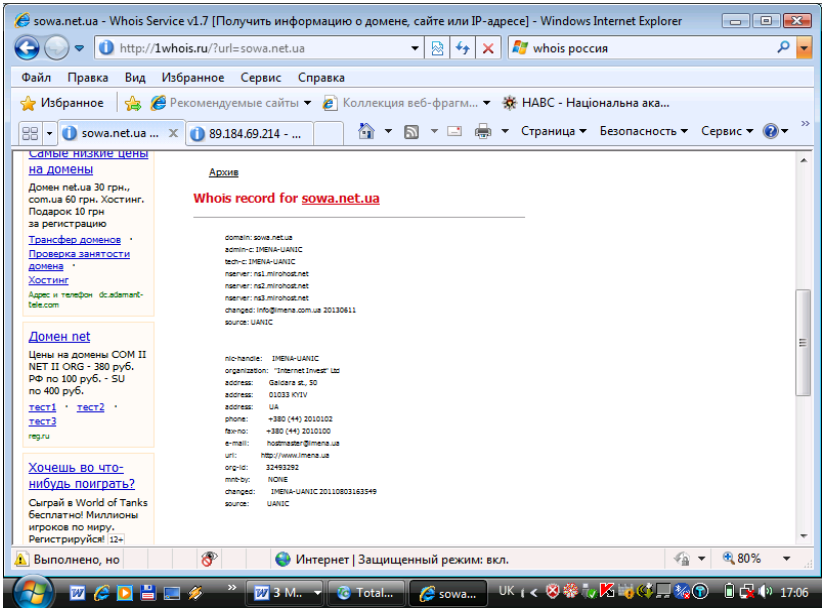

Рис. 9. Результати пошуку Інтернет-провайдера сайту http:// sowa.net.ua
(лист 2)

Таким чином, встановлено, що доменне ім'я sowa.net.ua зареєстровано у підприємства-реєстратора «Товариство з обмеженою відповідальністю Internet Invest», яке розташоване за адресою: Київ, вул. Гайдара, 50, тел.: +380 (44) 2010102, факс: +380 (44) 2010100, e-mail: hostmaster@imena.ua

Також встановлено, що зазначений Інтернет-ресурс знаходиться на серверному обладнані за IP-адресою 89.184.69.214.

Для запиту встановлення хостинг-провайдера за IP-адресою 89.184.69.214 використовувався сервіс Whois.

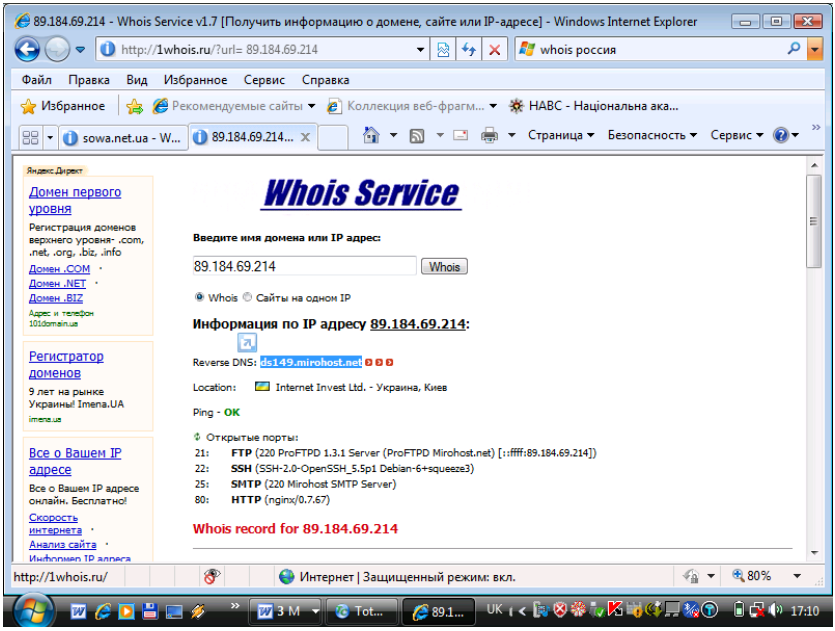

Рис. 10. Результати пошуку хостинг-провайдера за IP-адресою 89.184.69.214

З результату запиту за IP-адресою 89.184.69.214 встановилено, що дана IP-адреса надана для користування «Товариством з обмеженою відповідальністю Internet Invest», яке, зокрема, надає послуги з розміщення веб-ресурсів (хостингу). Таким чином IP-адреса сайту sowa.net.ua належить тому самому підприємству, що реєструвало його доменне ім'я.

2.3. Підготовка запитів щодо надання інформації про користувачів Інтернет-сайтів і власників поштових скриньок

Після встановлення IP-адреси користувача, причетного до розповсюдження в мережі Інтернет забороненого контенту, слідчий вживає заходів щодо ідентифікації особи користувача й встановлення місцезнаходження відповідного комп'ютерного обладнання та засобів комунікації.

З цією метою слідчий повинен отримати відповідні ухвали слідчого судді на тимчасовий доступ до комп'ютерних систем на адресу встановлених Інтернет-провайдерів, зокрема:

– у яких зареєстровано доменне ім'я сайту та які здійснюють хостінг для розміщення сайту, з якого здійснювалось розповсюдження забороненого контенту або надавалися пропозиції придбати заборонені до вільного обігу предмети або речовини.

Метою направлення ухвали є отримання інформації, що має відношення до справи, зокрема:

– коли та проміжком якого часу був створенно даний обліковий запис протиправного характеру (наприклад, «Продам наркотики»);

– з якої IP-адреси було створено обліковий запис користувача, який створив Інтернет-ресурс з протиправним контентом;

– на кого зареєстрований обліковий запис (повні анкетні дані власників сайту, інформація з панелі адміністрування, IP-адреси, номери телефонів тощо);

– деталізація всіх IP-адрес та часу виходу у даний обліковий запис користувача;

– як здійснювався перегляд даного облікового запису та його наповнення (IP-адреса, установчі дані та час входу);

– яким чином оплачуються послуги за зазначене доменне ім'я (вид платіжної системи, яка використовувалась при поповненні балансу облікового запису користувача даної системи (гаманці, ідентифікатори, види оплат), банківські установи, рахунки тощо;

– якою є зареєстрована IP-адреса чи поштова скринька правопорушника-користувача мережі Інтернет, який здійснював спілкування з невстановленого комп'ютерного обладнання:

– якими є реквізити абонента, який здійснював доступ до мережі Інтернет під певною IP-адресою у певний час доби;

– які IP-адреси використовувалися для створення певного облікового запису;

– які IP-адреси використовуються для з'єднання з цим обліковим записом;

– якими є реєстраційні дані (logs) та абонентська інформація про користувача певного облікового запису (електронної поштової адреси) (наприклад, roma_narkoman@ukr.net);

– якими є відомості про певний обліковий запис (електронну поштову адресу), на який пересилається повідомлення після його отримання;

– яким є зміст адресної книги електронної поштової скриньки;

– якими є зміст всіх вхідних та вихідних повідомлень.

– які права на адміністрування Інтернет-форумом або чатом, через який здійснювалося протиправне спілкування (з метою встановлення IP-адреси правопорушника):

– час реєстрації даної поштової скриньки і IP-адреси, якими користувався правопорушник;

– установчі дані користувача поштової скриньки;

– через який телефонний номер здійснювалась активація облікового запису;

– якими є деталі всіх сеансів входу до даного облікового запису із зазначенням IP-адрес та часу.

З метою отримання даних переписки (спілкування) в Інтернет-форумі або чаті, який здійснював продавець предметів та речовин, заборонених для вільного обігу, з їх покупцем, доцільно запросити історію повідомлень на певному Інтернет-форумі певного користувача під певним ніком (мережевим ім'ям). У цьому випадку доцільно, щоб провайдер до відповіді додав інформацію в електронному вигляді.

Для спрямування запитів закордонним хостінг-провайдерам слід використовувати можливості НЦБ Інтерполу при МВС

України з метою зв'язатися з правоохоронними органами тієї держави, де розташовано головний офіс провайдера.

Слід пам'ятати, що стаціонарний комп'ютер, підключений до мережі Інтернет, має в базі Інтернет-провайдера облікові записи імені користувача, його реквізити адресу встановлення комп'ютерної техніки та засобів комунікації й інші дані (наприклад, технічний телефонний номер). Вказане надає слідчому можливості провести подальші слідчі дії, направлені на встановлення особи користувача комп'ютерного обладнання та засобів комунікації, за допомогою яких розповсюджувався заборонений контент.

Якщо з'єднання комп'ютера з Інтернетом відбувається через провідний *модем*, слідчий має витребувати інформацію у Інтернет-провайдера про номер стаціонарного телефону, через який підтримувався зв'язок користувача з провайдером. У подальшому слідчий за визначеним телефонним номером вживає заходів щодо тимчасового доступу до встановленого модему та підключеного до нього комп'ютерного обладнання й засобів комунікації, а також відпрацьовує їх користувачів на причетність до розповсюдження забороненого контенту.

Якщо з'єднання з Інтернетом відбувається через підключення за допомогою звичайних *мережевих карт* (LAN) та мережевого кабелю, то слідчий витребовує у Інтернет-провайдера інформацію про адресу встановлення комп'ютерної техніки та засобів комунікації, а також особу, яка заключила абонентський договір з провайдером. У подальшому слідчий за визначеною адресою вживає необхідних заходів щодо тимчасового доступу до комп'ютерної технки чи засобів комунікацій, а також відпрацьовує її користувачів на причетність до розповсюдження забороненого контенту.

Якщо електронна поштова адреса створена навмисно для вчинення протиправних дій, правопорушник може користуватися нею з робочих місць в комп'ютерних Інтернет-клубах, кафе, орендованих квартирах, готелях тощо. В цьому випадку слід встановити наступне:

– конкретний комп'ютер у внутрішній локальній мережі Інтернет-клубу, кафе або іншого місця, де правопорушник анонімно здійснював свою діяльність;

– який адміністратор, офіціанти та інші працівники закладу були на зміні під час виходу правопорушника до мережі Інтернет;

– осіб з числа інших клієнтів, які в той час перебували поблизу комп'ютера правопорушника;

– інший обслуговуючий персонал Інтернет-клубу, кафе, готелю тощо, який міг запам'ятати правопорушника (охоронець, бармен, офіціант, прибиральниця та ін.).

Встановлених осіб необхідно опитати та встановити особу (або скласти фоторобот) правопорушника.

Слід особливо звертати увагу на наявність камер відеоспостереження, які могли зафіксувати правопорушника під час перебування у певному приміщенні, звідки він здійснював вихід в мережу Інтернет. У подальшому здійснюють тимчасовий доступ та перегляд відеоматеріалів, отриманих камерами стеження у місцях появи правопорушника.

Здійснення аналізу отриманих відеоматеріалів дозволить встановити певні ознаки правопорушника (стать, вік, зовнішній вигляд, одяг, атрибути, інші індивідуальні ознаки тощо), встановити транспортний засіб, яким він користується, а також інших осіб, які володіють відомостями про особу правопорушника (оскільки вони були свідками чи спільниками його протиправних дій, або бачили марку чи реєстраційні номери машини, яка його підвозила тощо).

РОЗДІЛ 3
ОСОБЛИВОСТІ ПРОВЕДЕННЯ ОКРЕМИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ, ПОВ'ЯЗАНИХ ІЗ РОЗПОВСЮДЖЕННЯМ У МЕРЕЖІ ІНТЕРНЕТ ЗАБОРОНЕНОГО КОНТЕНТУ

3.1. Допит

Однією з найбільш важливих слідчих дій є допит. З метою об'єктивного розслідування кримінального правопорушення слідчий допитує підозрюваного, потерпілого та свідків.

Допит проводиться за місцем проведення досудового розслідування або в іншому місці за погодженням із особою, яку мають намір допитати. Кожний свідок допитується окремо, за відсутності інших осіб. Дана слідча дія не може продовжуватися без перерви понад дві години, а в цілому – понад вісім годин на день.

Перед допитом встановлюється особа допитуваного, роз'яснюються його права, а також порядок проведення допиту. У разі допиту свідка він попереджається про кримінальну відповідальність за відмову давати показання і за давання завідомо неправдивих показань, а потерпілий – за давання завідомо неправдивих показань. За необхідності до участі в допиті залучається перекладач.

Під час допиту може застосовуватися фотозйомка, аудіо- та (або) відеозапис. Особа має право не відповідати на запитання з приводу тих обставин, щодо надання яких є пряма заборона у законі (таємниця сповіді, лікарська таємниця, професійна таємниця захисника тощо), або які можуть стати підставою для підозри, обвинувачення у вчиненні цією особою, її близькими родичами чи членами її сім'ї кримінального правопорушення, а також щодо службових осіб, які виконують негласні слідчі (розшукові) дії, та осіб, які конфіденційно співпрацюють із органами досудового розслідування.

Допит малолітньої або неповнолітньої особи проводиться у присутності законного представника, педагога або психолога, а за необхідності – лікаря. Дана слідча дія не може продовжуватися без перерви понад одну годину, а загалом – понад дві години на день. До початку слідчої (розшукової) дії законному представнику, педагогу, психологу або лікарю роз'яснюється їхнє право за дозволом ставити уточнюючі запитання малолітній або неповнолітній особі.

Допит учасників процесу може проходити у дистанційному досудовому провадженні та здійснюватися згідно з правилами, передбаченими статтями 224–227 КПК України.

Особливості допиту особи, яка підозрюється у незаконному придбанні предметів та речовин, заборонених для вільного обігу, із використанням мережі Інтернет

Під час допиту особи, яка незаконно придбала предмет або речовину, заборонені для вільного обігу, необхідно встановити наступні обставини:

- особу затриманого (прізвище, ім'я, по-батькові, число, місяць, рік народження);
- місце реєстрації та місце фактичного проживання;
- місце навчання та роботи;

– чи є близькі родичі або особи, які знаходяться на утриманні;

– з ким підтримує дружні стосунки за місцем проживання та навчання (їх анкетні дані);

– чи притягувався до кримінальної або адміністративної відповідальності (якщо так, то за якими статтями Кримінального кодексу України та Кодексу України про адміністративні правопорушення);

– номер домашнього, робочого телефону та телефону стільникового зв'язку;

– звідки отримав речовину або предмет, заборонені для вільного обігу;

– на протязі якого часу та які види наркотиків вживає, їх дозування;

– де та у кого, зазвичай, придбає наркотики;

– звідки дізнався про можливість придбання через мережу Інтернет речовини або предмету, заборонених для вільного обігу. Хто повідомив (установчі дані, адреса, телефон);

– з якого місця та в який час виходив у мережу Інтернет з метою ознайомлення з пропозиціями купівлі/продажу заборонених до вільного обігу речовин або предметів;

– який це був сайт або сторінка, який у них тип даного Інтернет-ресурсу (назва чату, блогу, сайту, номер ISQ, назва електронної пошти), які у них URL-адреси. Які на ній контактні дані було використано (E-mail, ICQ, skype);

– яким чином (від кого) представився особі, яка збувала заборонені до вільного обігу речовини або предмети;

– під яким ім'ям користувача (логіном) представлявся у мережі Інтернет;

– яким чином домовився з особою, яка збувала заборонені до вільного обігу речовини або предмети про їх придбання;

– які види заборонені до вільного обігу речовин або предметів були запропоновані йому через Інтернет, їхня кількість, ціна;

– який спосіб збуту заборонених до вільного обігу речовин або предметів був рекомендований їх збувальником (контактний чи безконтактний);

– які Інтернет-ресурси використовував для подальшого придбання заборонених до вільного обігу речовин або предметів (назва сайту, номер ICQ, адреса електронної пошти E-mail);

– яким чином підтримувався подальший зв'язок з особою, яка збувала заборонені до вільного обігу речовини або предмети (стільниковий мобільний телефон, ICQ, електронна пошта тощо);

– скільки разів купував заборонені до вільного обігу речовини або предмети у даного розповсюджувача;

– яким чином здійснювалась оплата за придбання заборонені до вільного обігу речовини або предмети (поповнення рахунку певного телефонного номеру; надання телефоном шляхом SMS-повідомлення секретного коду ваучера на поповнення рахунку; здійснення банківського переказу; переказу коштів з рахунку Інтернет-картки тощо);

– на який банківський рахунок чи номер телефону оператора стільникового зв'язку здійснювався переказ грошових коштів;

– чи мало місце підтвердження надходження грошових коштів; яким чином це відбувалось;

– яким чином та через який час розповсюджувач повідомив покупця про місце та час передачі заборонених до вільного обігу речовин або предметів (через телефонний дзвінок, Інтернет-повідомлення, через SMS-повідомлення чи MMS-повідомлення чи інше);

– яким чином, де та коли було отримано заборонені до вільного обігу речовини або предмети;

– якщо заборонені до вільного обігу речовини або предмети передавались через так званні тайники (закладки), описати де саме знаходився такий тайник (закладка), місце, територія, зазначити детальне розташування та засоби маскування;

– яким чином були запаковані заборонені до вільного обігу речовини або предмети (вказати матеріал пакування, спосіб пакування, вид та колір, агрегатний стан);

– що зробив покупець з отриманими забороненими до вільного обігу речовинами або предметами у подальшому;

– хто ще замовляв заборонені до вільного обігу речовини або предмети, використовуючи мережу Інтернет.

Особливості допиту особи, яка підозрюється у незаконному збуті через мережу Інтернет предметів або речовини, заборонених для вільного обігу

Під час допиту особи, яка підозрюється у незаконному збуті предметів або речовин, заборонених для вільного обігу, необхідно встановити наступні обставини:

– прізвище, ім'я, по батькові;

– число, місяць, рік народження;

– адреса місця проживання, адреса місця реєстрації;

– чи притягався до кримінальної відповідальності. Якщо так, то за які саме кримінальні правопорушення;

– чи має затриманий з числа друзів осіб, які притягалися до кримінальної відповідальності;

– чи вживає наркотики, якщо так, то які, з якого часу, їх дозування;

– протягом якого часу він займається розповсюдженням заборонених до вільного обігу предметівабо речовин;

– що призвело до розповсюдження заборонених до вільного обігу предметів аббо речовин;

– хто придумав та організував схему розповсюдження заборонених до вільного обігу речовин та предметів через мережу Інтернет;

– хто допомогав у організації створення такої схеми;

– яким чином використовувалась мережа Інтернет для збуту заборонених до вільного обігу предметів та речовин;

– де саме та за які кошти було придбане комп'ютерне обладнання та засоби комунікації, що використовувалась у злочинних цілях;

– які Інтернет-ресурси використовувались для розміщення реклами та пропозицій щодо продажу заборонених до вільного обігу предметів та речовин;

– хто створював, чи допомагав у створенні Інтернет-сайту, як, коли при яких обставинах познайомились (установчі дані, адреса, телефон);

– яким саме Інтернет-провайдером користувався та під яким ім'ям користувача («ніком»);

– яка назва Інтернет-сайту, що ним користувався для збуту заборонених до вільного обігу предметів та речовин;

– як часто змінювалися контактні дані (телефон, E-mail, ICQ, Skype та ім'я користувача);

– скільки Інтернет-сайтів було створено або використано для організації збуту заборонених до вільного обігу предметів та речовин;

– у яких місцях та в який час виходив у мережу Інтернет з метою ознайомлення з пропозиціями купівлі/продажу заборонені до вільного обігу предметів та речовин;

– який це був сайт або сторінка, тип даного Інтернет-ресурсу (назва чату, блогу, сайту, номер ISQ, назва електронної пошти e-mail), які у них URL-адреси? Які на ній контактні дані було використано: E-mail, ICQ, Skype;

– яким чином (від кого) представився підозрюваний;

– під яким ім'ям (логіном) представлявся;

– яким чином домовлявся з покупцем про придбання заборонених до вільного обігу предметів та речовин;

– який спосіб збуту заборонених до вільного обігу предметів та речовин був рекомендований підозрюваним (контактний чи безконтактний);

– які Інтернет-ресурси використовувались для подальшого збуту заборонених до вільного обігу предметів та речовин (назва чату, сайту, номер ICQ, назва електронної пошти e-mail);

– яким чином підтримувався подальший зв'язок з покупцем заборонених до вільного обігу предметів та речовин (стільниковий мобільний телефон, ICQ, електронна пошта);

– звідки у підозрюваного заборонені до вільного обігу предмети та речовини, де, при яких обставинах, за яку ціну та у кого він їх придбав (установчі дані, адреса, телефон), при яких обставинах підозрюваний з ним познайомився;

– яким чином здійснювалася доставка заборонених до вільного обігу предметів та речовин, де (у кого) вони зберігалися перед їх збутом;

– скільки фактів незаконного збуту заборонених до вільного обігу предметів та речовин за допомогою мережі Інтернет було вчинено (по кожному факту окремо допитати зі з'ясуванням усіх необхідних обставин);

– за якою ціною збувались заборонені до вільного обігу предмети та речовини;

– в якій упаковці розповсюджувались заборонені до вільного обігу предмети та речовини;

– розкрити зміст одерження коштів від продажу заборонених до вільного обігу предметів та речовин;

– на кого, коли та при яких обставинах відкривались банківські рахунки;

– яким чином проводилась конвертація та легалізація коштів, отриманих від збуту заборонених до вільного обігу предметів та речовин;

– яким чином проводилась перевірка надходження грошових коштів, отриманих від незаконного збуту заборонених до вільного обігу предметів та речовин;

– через які банківські термінали так коли знімались кошти, отримані від незаконного збуту заборонених до вільного обігу предметів та речовин;

– яким чином проводився розподіл грошей між учасниками незаконного збуту заборонених до вільного обігу предметів та речовин та яка саме частка залишалась підозрюваному;

– на які потреби витрачались кошти, здобуті від незаконного розповсюдження заборонених до вільного обігу предметів та речовин;

– яким чином повідомлялись замовники про надходження від них грошових коштів на придбання заборонених до вільного обігу предметів та речовин;

– хто був задіяний у якості співучасників (детально описати функції кожного з них).

Особливості допиту особи, яка є свідком незаконного придбання та (або) збуту предметів та речовин, заборонених для вільного обігу, із використанням мережі Інтернет

Під час допиту особи, яка є свідком незаконного придбання та (або) збуту предметів та речовин, заборонених для вільного обігу, із використанням мережі Інтернет, необхідно встановити наступні обставини:

– прізвище, ім’я, по батькові свідка;

– число, місяць, рік народження;

– адреса місця проживання, адреса місця реєстрації;

– чи притягався до кримінальної відповідальності. Якщо так, то за які саме кримінальні правопорушення;

– в яких стосунках перебуває з особою, причетною до придбання або збуту заборонених до вільного обігу предметів або речовин;

– за яких обставин йому стало відомо про незаконні дії підозрюваного;

– протягом якого часу він помічав протиправні дії підозрюваного;

– що конкретно може пояснити по суті справи.

Особливості допиту особи, яка підозрюється у розповсюдженні в мережі Інтернет порнографічних предметів або творів, що пропагують культ насильства та жорстокості

Під час допиту особи, яка підозрюється у розповсюдженні в мережі Інтернет порнографічних предметів або творів, що пропагують культ насильства та жорстокості, необхідно встановити наступні обставини:

– прізвище, ім'я, по батькові;

– число, місяць, рік народження;

– адресу місця проживання, адреса місця реєстрації;

– чи притягувалась раніше до кримінальної відповідальності особа, у т.ч. за розповсюдження порнографічних предметів або творів, що пропагують культ насильства та жорстокості, якщо так, то коли та за які саме кримінальні правопорушення;

– чи має з числа друзів осіб, які притягалися до кримінальної відповідальності;

– протягом якого часу вона займається протиправною діяльністю, пов'язаною з розповсюдженням порнографічних предметів або творів, що пропагують культ насильства та жорстокості;

– що спонукало до зайняття такою протиправною діяльністю;

– хто придумав та організував протиправну схему виготовлення та розповсюдження порнографічних предметів або творів, що пропагують культ насильства та жорстокості через мережу Інтернет;

– хто, як, коли, де, при яких обставинах, від кого отримав порнографічні предмети або твори, що пропагують культ насильства та жорстокості;

– на якому обладнанні створював порнографічні предмети або твори, що пропагують культ насильства та жорстокості, хто брав участь у цьому процесі (їх установчі дані, адреси, телефон);

– як давно особа розповсюджує порнографічні предмети або твори, що пропагують культ насильства та жорстокості;

– чи усвідомлювала особа, що предмети та твори містять порнографічний характер або пропагують культ насильства та жорстокості;

– де саме та за які кошти була придбана техніка, яка використовувалась для виготовлення та розповсюдження порнографічних предметів або творів, що пропагують культ насильства та жорстокості через мережу Інтернет;

– звідки у підозрюваного заборонений контент, де, при яких обставинах та у кого він його отримав, хто постачальник забороненого контенту (установчі дані, адреса, телефони), при яких обставинах підозрюваний з ним познайомився;

– яким чином використовувалась мережа Інтернет у протиправній діяльності;

– які Інтернет-ресурси використовувались для розміщення та подальшого розповсюдження порнографічних предметів або творів, що пропагують культ насильства та жорстокості;

– что створював Інтернет-сайт, чи допомагав у його створенні, як познайомились (установчі дані, адреса, телефон);

– яким саме Інтернет-провайдером користувався та під яким ім’ям («ніком»);

– яка назва Інтернет-сайту, яким користувався для розповсюдження порнографічних предметів або творів, що пропагують культ насильства та жорстокості;

– як часто змінювався Інтернет-провайдер та «нік»;

– скільки Інтернет-сайтів було створено для організації розповсюдження порнографічних предметів або творів, що пропагують культ насильства та жорстокості;

– на яких типах Інтернет-сайтів він зареєстрований (сайти для знайомств, моделей, підлітків);

– з якого місця та в якій годині здійснювався доступ до облікового запису у мережі Інтернет з метою розміщення там порнографічних предметів або творів, що пропагують культ насильства та жорстокості;

– під яким ім'ям (логіном) представлявся під час спілкування з провайдерами Інтернет сервісів;

– яким чином домовлявся з користувачами про надання їм забороненого контенту;

– який спосіб оплати за продаж порнографії був рекомендований підозрюваним (контактний чи безконтактний);

– які Інтернет-ресурси використовував для подальшого відтворення протиправної діяльності (назва чату, сайту, номера ICQ, адреси електронної пошти e-mail);

– яким чином підтримувався подальший зв'язок зі співучасниками (мобільний телефон, ICQ, електронна пошта);

– скільки фактів розповсюдження порнографії з використанням мережі Інтернет було вчинено (по кожному факту окремо допитати зі з'ясуванням усіх необхідних обставин);

– які типи порнографічного контенту розповсюджувались (фото, відео, текст, їх формат);

– чи збувались і розповсюджувались порнографічні предмети неповнолітнім;

– за якою схемою надавалися послуги користування порнографічним контентом;

– яким чином одержувались гроші від надання послуг;

– з якою фінансовою установою мав договір про переказ коштів, отриманих від розповсюдження порнографії;

– яким чином відбувалось спілкування з клієнтами – отримувачами порнографічних предметів або творів, що пропагують культ насильства та жорстокості;

– як створювалась юридична особа, яка укладала договір про перерахування грошових коштів, на кого вона була оформлена;

– на чиє ім'я, коли та при яких обставинах відкривався банківський рахунок;

– яким чином проводилась конвертація та легалізація коштів, отриманих від збуту порнографією;

– яким чином проводилась перевірка надходження грошових коштів, отриманих від торгівлі порнографічними предметами;

– яким чином проводився розподіл грошей між учасниками схеми по створенню та розповсюдженню порнографічних предметів в мережі Інтернет та яка саме частка залишалась підозрюваному;

– на які потреби витрачались кошти, здобуті від збуту порнографічних предметів;

– хто був задіяний у якості спільників (детально описати функції кожного з них);

– які методи конспірації використовував підозрюваний з метою непритягнення до кримінальної відповідальності;

– яким чином використовувались пристрої мобільного зв'язку в протиправній діяльності;

– причини, які спонукали до виготовлення (розповсюдження) контенту, що містить порнографічні предмети або твори, що пропагують культ насильства та жорстокості;

– скільки часу підозрюваний користується комп'ютером;

– хто ним ще користується;

– скільки комп'ютерів він має і де вони встановлені;

– де і яке комп'ютерне обладнання зберігається;

– яким чином зберігається в комп'ютерній пам'яті заборонений контент, чи використовується для цього який-небудь метод шифрування даних, його назва та хто має до них доступ, пароль;

– як зазвичай підозрюваний зберігає файли, що відбувається під час запуску комп'ютера, чи вміє він створювати файли та папки, якими програмами користується та чи має бездротову мережу (для формування загального уявлення про рівень знань комп'ютера підозрюваним).

Особливості допиту особи, яка підозрюється у розповсюдженні в мережі Інтернет відомостей, що становлять державну або іншу таємницю, яка охороняється законом

Під час допиту особи, яка підозрюється у розповсюдженні в мережі Інтернет відомостей, що становлять державну або іншу таємницю, яка охороняється законом, необхідно встановити наступні обставини:

– прізвище, ім'я, по батькові;

– число, місяць, рік народження;

– адресу місця проживання, адреса місця реєстрації;

– чи притягувалась раніше до кримінальної відповідальності особа, якщо так, то коли та за які саме кримінальні правопорушення;

– чи має з числа друзів осіб, які притягалися до кримінальної відповідальності;

– де працює та яку посаду займає;

– протягом якого часу він займається протиправною діяльністю, пов'язаною з розповсюдженням державної та іншої таємниці;

– що спонукало до зайняття такою протиправною діяльністю;

– хто придумав та організував протиправну схему отримання та розповсюдження таємниці через мережу Інтернет;

– хто, як, коли, де, при яких обставинах, від кого отримав інформацію, що містить державну або іншу таємницю;

– які засоби використовувались для отримання інформації, що містить державну або іншу таємницю (фотографування, сканування, крадіжка документів тощо);

– чи усвідомлювала особа, що інформація, яку вона розповсюджує в мережі Інтернет, містить державну або іншу таємницю;

– яким чином використовувалась мережа Інтернет у протиправній діяльності;

– які Інтернет-ресурси використовувались для розміщення та подальшого розповсюдження державної та іншої таємниці;

– хто створював Інтернет-сайт, чи допомагав у його створенні, як познайомились (установчі дані, адреса, телефон);

– яким саме Інтернет-провайдером користувався та під яким ім'ям (нікнеймом);

– яка назва Інтернет-сайту, яким користувався;

– як часто змінювався Інтернет-провайдер та «нік»;

– скільки Інтернет-сайтів було створено для організації розповсюдження державної та іншої таємниці в мережі Інтернет;

– на яких типах Інтернет-сайтів він зареєстрований;

– з якого місця та в якій годині здійснювався доступ до облікового запису у мережі Інтернет з метою розповсюдження державної та іншої таємниці;

– під яким ім'ям (логіном) представлявся під час спілкування з провайдерами Інтернет сервісів;

– яким чином домовлявся з користувачами про надання їм забороненого контенту;

– який спосіб оплати за розповсюдження державної та іншої таємниці був рекомендований підозрюваним (контактний чи безконтактний);

– які Інтернет-ресурси використовував для подальшого відтворення протиправної діяльності (назва чату, сайту, номера ICQ, адреси електронної пошти e-mail);

– яким чином підтримувався подальший зв'язок зі співучасниками (мобільний телефон, ICQ, електронна пошта);

– скільки фактів розповсюдження державної та іншої таємниці з використанням мережі Інтернет було вчинено (по кожному факту окремо допитати зі з'ясуванням усіх необхідних обставин);

– які типи забороненого контенту розповсюджувались (фото, відео, текст, їх формат);

– яким чином одержувались гроші від надання послуг;

– на чиє ім'я, коли та при яких обставинах відкривався банківський рахунок;

– яким чином проводилась перевірка надходження грошових коштів, отриманих від розповсюдження державної та іншої таємниці;

– яким чином проводився розподіл грошей між учасниками схеми по розповсюдженню розповсюдження державної та іншої таємниці в мережі Інтернет та яка саме частка залишалась підозрюваному;

– на які потреби витрачались кошти, здобуті від розповсюдження державної та іншої таємниці;

– хто був задіяний у якості спільників (детально описати функції кожного з них);

– які методи конспірації використовував підозрюваний з метою не притягнення до кримінальної відповідальності;

– скільки комп'ютерів він має і де вони розміщені;

– яким чином зберігається в комп'ютерній пам'яті заборонений контент, чи використовується для цього який-небудь метод шифрування даних, його назва та хто має до них доступ, пароль;

– як зазвичай підозрюваний зберігає файли, що відбувається під час запуску комп'ютера, чи вміє він створювати файли та папки, якими програмами користується та чи має бездротову мережу (для формування загального уявлення про рівень знань комп'ютера підозрюваним).

Особливості допиту особи, яка підозрюється у розповсюдженні в мережі Інтернет завідомо неправдивого повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності

Під час допиту особи, яка підозрюється у розповсюдженні в мережі Інтернет завідомо неправдивого повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності, необхідно встановити наступні обставини:

– прізвище, ім'я, по батькові;

– число, місяць, рік народження;

– адреса місця проживання, адреса місця реєстрації;

– чи притягувалась раніше до кримінальної відповідальності особа, якщо так, то коли та за які саме кримінальні правопорушення;

– чи має з числа друзів осіб, які притягалися до кримінальної відповідальності;

– де працює та яку посаду займає;

– наскільки часто він займається протиправною діяльністю, пов'язаною з розповсюдженням неправдивих повідомлень про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності;

– що спонукало до зайняття такою протиправною діяльністю;

– чи усвідомлював підозрюваний, що своїми діями може породити паніку в суспільстві та порушує безпеку суспільства;

– хто придумав та організував протиправну схему розповсюдження неправдивих повідомлень про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності шляхом повідомлення про це через мережу Інтернет;

– яке саме завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності здійснив підозрюваний;

– на чию адресу через мережу Інтернет було направлено повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності;

– яким чином використовувалась мережа Інтернет у протиправній діяльності;

– які Інтернет-ресурси використовувались для передачі завідомо неправдивого повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності;

– хто створював Інтернет-сайт, чи допомагав у його створенні, як познайомились (установчі дані, адреса, телефон);

– яким саме Інтернет-провайдером користувався та під яким ім'ям («ніком»);

– як часто змінювався Інтернет-провайдер та «нік»;

– з якого місця та в якій годині здійснювався доступ до облікового запису у мережі Інтернет з метою завідомо неправдивого повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності;

– під яким ім'ям (логіном) представлявся під час спілкування з провайдерами Інтернет сервісів;

– які Інтернет-ресурси використовував для подальшого відтворення протиправної діяльності (назва чату, сайту, номера ICQ, адреси електронної пошти e-mail);

– які наслідки передбачав підозрюваний при завідомо неправдивому повідомленні про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності;

– скільки фактів завідомо неправдивого повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності з використанням мережі Інтернет було

вчинено (по кожному факту окремо допитати зі з'ясуванням усіх необхідних обставин);

– хто був задіяний у якості спільників (детально описати функції кожного з них);

– які методи конспірації використовував підозрюваний з метою непритягнення до кримінальної відповідальності;

– яким чином використовувались пристрої мобільного зв'язку в протиправній діяльності;

– скільки часу підозрюваний користується комп'ютером;

– хто ним ще користується;

– скільки комп'ютерів він має і де вони розміщені;

– де і яке комп'ютерне обладнання зберігається з яких здійснювалось відправлення через мережу Інтернет повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності;

– яким чином зберігається в комп'ютерній пам'яті заборонений контент, чи використовується для цього який-небудь метод шифрування даних, його назва та хто має до них доступ, пароль;

– як зазвичай підозрюваний зберігає файли, що відбувається під час запуску комп'ютера, чи вміє він створювати файли та папки, якими програмами користується та чи має бездротову мережу (для формування загального уявлення про рівень знань комп'ютера підозрюваним).

Особливості допиту особи, яка підозрюється у розповсюдженні в мережі Інтернет публічних закликів, спрямованих на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, або до вчинення дій, що загрожують громадському порядку

Під час допиту особи, яка підозрюється у розповсюдженні в мережі Інтернет публічних закликів, спрямованих на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, або до вчинення дій, що загрожують громадському порядку, необхідно встановити наступні обставини:

– прізвище, ім'я, по батькові;

– число, місяць, рік народження;

– адреса місця проживання, адреса місця реєстрації;

– чи притягувалась раніше до кримінальної відповідальності особа, якщо так, то коли та за які саме кримінальні правопорушення;

– чи має з числа друзів осіб, які притягалися до кримінальної відповідальності;

– де працює та яку посаду займає;

– з якою метою вона здійснювала публічні заклики, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, або до вчинення дій, що загрожують громадському порядку, що спонукало до зайняття такою протиправною діяльністю;

– чи усвідомлював підозрюваний, що своїми діями він сприяє насильницькій зміні та поваленню конституційного ладу, захопленню державної влади, або вчиняє дії, що загрожують громадському порядку;

– які саме публічні заклики спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, або до вчинення дій, що загрожують громадському порядку, здійснив підозрюваний;

– на чию адресу через мережу Інтернет були направлені повідомлення, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, або вчинення дій, що загрожують громадському порядку;

– яким чином використовувалась мережа Інтернет у протиправній діяльності;

– які Інтернет-ресурси використовувались для передачі публічних закликів, спрямованих на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, або вчинення дій, що загрожують громадському порядку;

– хто створював Інтернет-сайт, чи допомагав у його створенні, як познайомились (установчі дані, адреса, телефон);

– яким саме Інтернет-провайдером користувався та під яким ім’ям («ніком»);

– як часто змінювався Інтернет-провайдер та «нік»;

– з якого місця та в якій годині здійснювався доступ до облікового запису у мережі Інтернет з метою поміщення публічних закликів, спрямованих на насильницьку зміну чи

повалення конституційного ладу або на захоплення державної влади, або вчинення дій, що загрожують громадському порядку;

– під яким ім'ям (логіном) представлявся під час спілкування з провайдерами Інтернет сервісів;

– які Інтернет-ресурси використовував для подальшого відтворення протиправної діяльності (назва чату, сайту, номера ICQ, адреси електронної пошти e-mail);

– чи передбачав наслідки підозрюваний при поміщенні в мережі Інтернет публічних закликів, спрямованих на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, або вчинення дій, що загрожують громадському порядку;

– скільки фактів поміщенні в мережі Інтернет публічних закликів, спрямованих на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, або вчинення дій, що загрожують громадському порядку було вчинено (по кожному факту окремо допитати зі з'ясуванням усіх необхідних обставин);

– хто був задіяний у якості спільників (детально описати функції кожного з них);

– які методи конспірації використовував підозрюваний з метою не притягнення його до кримінальної відповідальності;

– яким чином використовувались пристрої мобільного зв'язку в протиправній діяльності;

– скільки часу підозрюваний користується комп'ютером;

– хто ним ще користується;

– скільки комп'ютерів він має і де вони розташований;

– де і яке комп'ютерне обладнання зберігається з яких здійснювалось поміщенні в мережі Інтернет публічних закликів, спрямованих на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, або вчинення дій, що загрожують громадському порядку;

– яким чином зберігається в комп'ютерній пам'яті заборонений контент, чи використовується для цього який-небудь метод шифрування даних, його назва та хто має до них доступ, пароль;

– як зазвичай підозрюваний зберігає файли, що відбувається під час запуску комп'ютера, чи вміє він створювати файли та папки, якими програмами користується та

чи має бездротову мережу (для формування загального уявлення про рівень знань комп'ютера підозрюваним).

3.2. Обшук

Обшук у кримінальних провадженнях, пов'язаних із розповсюдженням у мережі Інтеренет забороненого контенту, здійснюється за наступними напрямами:

– виявлення предметів та речовин, заборонених для вільного обігу;

– виявлення комп'ютерного обладнання та засобів комунікації, яке використовувалося для розповсюдження в мережі Інтернет забороненого контенту;

– встановлення способів оплати за вчиненні протиправні дії.

3.2.1. Виявлення предметів і речовин, заборонених для вільного обігу

Під час обшуку у кримінальних провадженнях, пов'язаних з розповсюдженням заборонених до вільного обігу предметів та речовин із використанням мережі Інтернет, вилучають (залежно від складу кримінального правопорушення):

– усі види бойової, спортивної, нарізної мисливської зброї, атипічну зброю, кустарно виготовлену чи перероблену, а також зразки історичної зброї (гармати, міномети, кулемети, автомати, карабіни, гвинтівки, пістолети та револьвери тощо);

– частини зброї: глушник, запобіжник, ствол, затворна рамка, затворна затримка, кобура, ремінь, приклад, лазерний цільовий указник, оптичний приціл, полум'ягасник, зворотна, бойова та інші види пружин, ствольна коробка, ударник, рейка Пікатінні, рефлекторний приціл тощо;

– боєприпаси: патрони до нарізної вогнепальної зброї різних калібрів, артилерійські снаряди, бомби, міни, гранати, бойові частини ракет і торпед та інші вироби в зібраному чи у розібраному вигляді;

– вибухові речовини: порох різних марок, тверді суміші та ракетні палива, динаміт, нітросполуки (тротил, гексоген, ксиліл, пікринова кислота октоген), азотнокислі ефіри, нітроефіри,

нітрогліцерин та інші хімічні речовини, їх сполуки або суміші, здатні вибухнути без доступу кисню;

– ініціюючі (первинні) вибухові речовини – гримуча ртуть (фульмінат ртуті), азид свинцю, ТНРС (тринітрорезорцинат свинцю), тетразен;

– піротехнічні суміші;

– вибухові пристрої (промислові, саморобні);

– засоби вибуху: засоби запалювання (капсулі запалювання та електрозапалювання); засоби детонації (капсуль-детонатор, електродетонатор, вогнепровідний шнур, детонуючий шнур); засоби передачі ініціюючого імпульсу (годинникові, радіокеровані, ударної дії тощо);

– радіоактивні речовини: ядерне паливо, яке може виділяти енергію шляхом самопідтримуваного ланцюгового процесу ядерного поділу поза ядерним реактором, радіоактивні продукти та відходи, а також речовини природного або штучного походження, що містять у своєму складі радіоактивні ізотопи, здатні до первісного випромінювання (руда уранова або торієва, уран-233, плутоній-239, америцій-242 тощо).

– обладнання для зберігання та транспортування радіоактивних речовин (спеціалізовані контейнери, транспортні засоби);

– речі, що набули радіоактивності внаслідок впливу радіоактивних матеріалів (проби грунту, обладнання, техніка, одяг тощо);

– джерела іонізуючого випромінювання: різноманітні речовини та предмети, що містять радіоактивну речовину, технічні пристрої, що створюють або за певних умов можуть створювати іонізуюче випромінювання;

– отруйні та сильнодіючі речовини й лікарські засоби;

– фальсифіковані лікарські засоби;

– наркотичні засоби, психотропні речовини, їх аналоги та прекурсори;

– початкову сировину для виготовлення наркотичних засобів, психотропних речовин, їх аналогів, прекурсорів, сильнодіючих та отруйних речовин, сильнодіючих, отруйних та фальсифікованих лікарських засобів;

– предмети, в яких зберігалась початкова сировина, яка була основою для виготовлення зазначених засобів та речовин (бочки, каністри, бутлі, упаковки медичних препаратів);

– вторинні прекурсори та залишки від виготовлення наркотичних засобів, психотропних речовин, їх аналогів, прекурсорів, сильнодіючих та отруйних речовин, сильнодіючих, отруйних та фальсифікованих лікарських засобів, які знаходяться усередині обладнання (зокрема, мікросліди, нашарування на обладнанні, залишки речовини або сухий осад);

– допоміжні хімічні реактиви, речовини та предмети, що використовувались для виготовлення зазначених засобів та речовин (кислоти, луги, дистильована вода);

– відходи технологічного процесу (синтезу (екстрагування) виготовлення наркотичних засобів, психотропних речовин, їх аналогів, прекурсорів, сильнодіючих та отруйних речовин, сильнодіючих, отруйних та фальсифікованих лікарських засобів;;

– обладнання та устаткування, яке використовується на будь-якій стадії виготовлення зазначених засобів та речовин ;

– обладнання та устаткування, що використовувалося при інших операціях, пов’язаних із сушінням, подрібненням, зважуванням, розфасовкою наркотичних засобів, психотропних речовин, їх аналогів, прекурсорів, сильнодіючих та отруйних речовин, сильнодіючих, отруйних та фальсифікованих лікарських засобів;

– матеріали для упаковки зазначених засобів та речовин (харчовий папір, металева фольга, поліетиленові пакетики, спеціально виготовлені паперові згортки тощо);

– матеріали, які залишаються після різноманітних операцій, пов’язаних з виготовленням або вживанням зазначених засобів та речовин (залишки марлі, ватні тампони, шприци, «кальяни» тощо);

– речовини, які є домішками для вже готових наркотичних засобів, психотропних речовин, їх аналогів, прекурсорів, сильнодіючих та отруйних речовин, сильнодіючих, отруйних та фальсифікованих лікарських засобів;

– зразки та проби речовин зі стелі, стін, засобів вентиляції, систем водопостачання та каналізації тощо;

– використані експрес–тести, якими перевірялись дійсність наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів;

– літературу з фармакології та фармацевтики, записи з хімічними формулами щодо виготовлення наркотичних засобів, психотропних речовин, їх аналогів, прекурсорів, сильнодіючих та отруйних речовин, сильнодіючих, отруйних та фальсифікованих лікарських засобів;

– записи, які свідчать про виготовлення та збут зазначених засобів та речовин (на електронних номіях, у зошитах, на окремих аркушах, обривки паперу тощо);

– записники, листи, кореспонденцію, фотографії, відео- та аудіозаписи, комп'ютерне обладнання, засоби комунікації, з яких можна встановити зв'язки затриманого та його причетність до виготовлення та збуту наркотичних засобів, психотропних речовин, їх аналогів, прекурсорів, сильнодіючих та отруйних речовин, сильнодіючих, отруйних та фальсифікованих лікарських засобів;

– чисті бланки рецептів, кліше печаток, які свідчать про виготовлення рецептів на право придбання медичних препаратів, що містять наркотичні засоби та психотропні речовини;

– захисний одяг, протигази, респіратори, рукавички;

– інші предмети, що містять сліди кримінального правопорушення.

Обов'язково відбирають зразки волосся, змиви з пальців рук, а також одежу та взуття, в якій знаходились затримані під час виготовлення наркотичних засобів, психотропних речовин, їх аналогів, прекурсорів, сильнодіючих та отруйних речовин, сильнодіючих, отруйних та фальсифікованих лікарських засобів (для встановлення та виявлення мікрослідів).

Залучення спеціалістів для проведення обшуку в разі виявлення радіоактивних матеріалів. Якщо обшук спрямований на виявлення радіоактивних матеріалів, які є предметом їх збуту через мережу Інтернет, слідчий, відповідно до положень ст.236 КПК України, має залучити для участі в проведенні слідчої дії спеціалістів, які мають фахові знання в галузі поводження з радіоактивними речовинами. Про участь спеціаліста у проведенні слідчої дії він обов'язково зазначає у протоколі обшуку.

Спеціаліст вживає заходів із забезпечення безпеки осіб, які залучаються до участі в обшуку, мінімізації будь-якого ризику радіоактивного опромінювання. Він проводить вимірювання потужності радіоактивного випромінювання, встановлює наявність та особливості радіоактивного забруднення із застосуванням спеціалізованих вимірювальних засобів. Результати вимірювань слідчий заносить до протоколу обшуку з обов'язковим зазначенням марки, серійного номера та відомостей про сертифікацію вимірювального обладнання.

В окремих випадках спеціаліст може встановити вид радіоактивного матеріалу на місці проведення обшуку (наприклад, за наявним заводським маркуванням). У разі неможливості ідентифікації джерела радіоактивного випромінювання на місці події, речові докази слід направити до Інституту ядерних досліджень Національної академії наук України (03680, м. Київ, проспект Науки, 47; тел. +380 (44) 525-23-49) чи іншої експертної організації для визначення фізичних характеристик радіоактивних матеріалів, які можуть мати криміналістичне значення. В разі відсутності відповідної експертної організації у певній адміністративно-територіальній одиниці, законодавство допускає залучення до дослідження радіоактивних матеріалів спеціалістів з інших установ, які мають фахові знання та допуск до поводження з такими матеріалами. Це можуть бути фахівці з системи МНС України, працівники відповідних навчальних та наукових закладів.

Після зазначення в протоколі обшуку всіх необхідних відомостей щодо джерела радіоактивного випромінювання слідчий чи інша повноважна особа, яка проводить обшук, приймає рішення про подальше транспортування радіоактивних матеріалів до відповідної установи (підприємства) для зберігання. При транспортуванні радіоактивних речових доказів спеціаліст, що бере участь в проведенні обшуку, вживає всіх необхідних заходів для забезпечення безпеки людей та недопущення зараження оточуючого середовища, використовуючи для цього спеціально призначені контейнери.

Слід мати на увазі, що реалізація робіт з транспортування та утилізації радіоактивних матеріалів проводиться спеціалізованими підприємствами. В Україні головною організацією, що виконує збирання, транспортування,

кондиціювання та тимчасове зберігання радіоактивних відходів, є Державна корпорація «Українське державне об'єднання «Радон» (03083, м. Київ, вул. Червонопрапорна, 50; тел. +38 (044) 525-48-35).

В подальшому слідчий за необхідності приймає рішення про проведення ядерно-фізичної судової експертизи радіоактивних матеріалів з метою визначення їх ізотопного складу, параметрів ядерного випромінювання та подальшого встановлення на цій основі джерела їх походження, місця й часу виробництва.

Під час обшуку у кримінальних провадженнях, пов'язаних з розповсюдженням у мережі Інтеренет порнографічних предметів або творів, що пропагують культ насильства та жорстокості, вилучають:

– порнографічні предмети та твори, а також твори, що пропагують культ насильства та жорстокості, які були використані як оригінал для серійного копіювання;

– обладнання, за допомогою якого здійснювалось виготовлення порнографічних предметів та творів, а також творів, що пропагують культ насильства та жорстокості;

– матеріали, використані для виготовлення порнографічних предметів та творів, а також творів, що пропагують культ насильства та жорстокості;

– виготовлені порнографічні предмети та твори, а також твори, що пропагують культ насильства та жорстокості, готові до розповсюдження, а також напівфабрикати (об'єкти виготовлення яких не закінчене);

– предмети зі слідами, що утворилися у процесі виготовлення порнографічних предметів та творів, а також творів, що пропагують культ насильства та жорстокості (аркуші паперу з пробними відбитками, ганчірка для витирання рук, забруднена друкарською фарбою, посудини з-під фарби, туби від тонера, використані картриджі та ін. Доказове значення таких предметів визначається обставинами справи. Так, якщо правопорушник встиг знищити чи винести з квартири всі матеріали, що безпосередньо застосовувалися для виготовлення порнографічних предметів та творів, а також творів, що пропагують культ насильства та жорстокості, то виявлення вищезазначених об'єктів буде непрямим доказом у справі);

– література та записи, які свідчать про вчинення кримінального правопорушення;

– одяг та інші аксесуари, які могли використовуватися під час виготовлення порнографічної продукції та творів, а також творів, що пропагують культ насильства та жорстокості.

До обладнання, яке може бути виявлено при обшуку в особи, що виготовляє порнографічні предмети та твори, а також твори, що пропагують культ насильства та жорстокості, поліграфічним способом, належать:

– засоби друку (принтери, сканери, поліграфічне обладнання);

– витратні матеріали й допоміжне пристосування (друкарські форми, картриджі, туби з тонером, поліграфічна плівка, пензлики, тампони, пульверизатори тощо);

– пристосування для подальшого оброблення напівфабрикатів (біндери, швидкозшивачі, сушки для паперу та ін.).

Під час обшуку варто шукати папір, аналогічний за своїми властивостями тому, на якому віддруковані порнографічні зображення. Іноді можна навіть знайти папір, нарізаний за форматом порнографічних творів, або творів, що пропагують культ насильства та жорстокості (журналів, книг, газет та ін.).

При обшуку в правопорушників, які спеціально вивчали технологію поліграфічних процесів, нерідко можна виявляти книги з цієї галузі (інструкції до поліграфічного обладнання, керівництва з використання відповідного спеціалізованого програмного забезпечення – графічних редакторів, посібники для якісного сканування тощо), а також записи: рецепти, описи технологічних процесів тощо. Такі тексти іноді шифрують, тому в процесі обшуку всі зошити, записні книжки, блокноти мають бути ретельно переглянуті та проаналізовані, а всі підозрілі записи – вилучені. Якщо запис зроблений не обвинувачуваним, а іншою, невідомою слідству особою, то розшук за почерком серед зв'язків виготівельника порнографічних предметів та творів, а також творів, що пропагують культ насильства та жорстокості, дасть можливість виявити співучасників, зокрема осіб, які розповсюджують такі предмети чи твори.

Предмети, які викривають правопорушника при виготовленні порнографічних предметів та творів, а також творів, що пропагують культ насильства та жорстокості, за

допомогою фотографічної репродукції, частково вже були названі вище. Однак, зазначимо, що при виготовленні таки предметів або творів за допомогою фоторепродукційного способу, предмети, видрукувані з одного негатива, мають те саме зображення, а також непомітні ідентифікаційні ознаки. Тож виявлення при обшуку, наприклад, порнографічного предмета (зображення), що був оригіналом для репродукції, має істотне значення. Іноді виготівельник порнографічної продукції або творів, що пропагують культ насильства та жорстокості, друкує зображення не з одного, а з декількох негативів. Можливо, до моменту проведення обшуку у розповсюджувачів будуть вилучені ще не всі копії порнографічних предметів і творів, а також творів, що пропагують культ насильства та жорстокості, виготовлені конкретною особою. Тож, виявлені в нього оригінали з тими ж зображеннями, мають бути вилучені та збережені до закінчення кримінального провадження. У разі затримання розповсюджувачів порнографічних предметів і творів, а також творів, що пропагують культ насильства та жорстокості, з тими ж ознаками, що й у вилучених при обшукові оригіналів, останні будуть викривати правопорушника у виготовленні таких предметів чи творів.

Варто зважати на те, що можуть бути виявлені зіпсовані чи пробні предмети з порнографічним змістом. Їх, зазвичай, слід шукати у смітті.

Під час обшуку у кримінальних провадженнях, пов'язаних з розповсюдженням у мережі Інтеренет відомостей, що становлять державну або іншу таємницю, яка охороняється законом вилучають:

– матеріали та предмети, які містять державну або іншу таємницю, яка охороняється законом;

– побутові та професійні засоби отримання інформації: диктофони, фотоапарати та їх частини, відеокамери, засоби сканування та копіювання, комунікатори (смартфони, айфони, айпеди тощо), інші пристрої з функціями отримання та фіксації аудіо-, фото- та відеоінформації;

– засоби зберігання інформації: аудіо- та відеокасети, дискети, оптичні компакт-диски, флеш-картки пам'яті тощо;

– спеціальні технічні засоби негласного отримання інформації: засоби негласного візуального спостереження та

документування, негласного прослуховування телефонних переговорів, негласного перехоплення та реєстрації інформації з технічних каналів зв'язку, негласного контролю поштових повідомлень і відправлень, негласного обстеження предметів і документів, негласного проникнення у приміщення, транспортні засоби, інші об'єкти та їх обстеження, негласного контролю за переміщенням транспортних засобів та інших об'єктів, негласного отримання (зміни, знищення) інформації з технічних засобів її зберігання, обробки та передачі;

– засоби друку: принтери, поліграфічне обладнання;

– витратні матеріали й допоміжне пристосування: друкарські форми, картриджі, туби з тонером, поліграфічна плівка, пензлики, тампони, пульверизатори тощо;

– пристосування для оброблення напівфабрикатів: біндери, швидкозшивачі, сушки для паперу тощо;

– матеріали, які підтверджують доступ особи до державної чи іншої таємниці (паперові документи та електронні носії інформації);

– тайники та сховища;

– засоби для проникнення у приміщення та сховища: ключі, відмички, засоби подолання сигналізації тощо.

Під час обшуку у кримінальних провадженнях, пов'язаних з розповсюдженням у мережі Інтеренет завідомо неправдивого повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності, вилучають, зокрема:

– матеріали, які містять повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності;

– телефонні довідники, карти міста, де здійснювалось завідомо неправдивого повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності тощо.

Під час обшуку у кримінальних провадженнях, пов'язаних з розповсюдженням у мережі Інтеренет публічних закликів, спрямованих на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, або до вчинення дій, що загрожують громадському порядку, вилучають, зокрема:

– матеріали, які містять публічні заклики, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, або до вчинення дій, що загрожують громадському порядку.

3.2.2. Виявлення комп'ютерного обладнання та засобів комунікації, що використовувалися для розповсюдження в мережі Інтернет забороненого контенту

В ході обшуку підлягають вилученню наступні предмети:

– комп'ютерне обладнання та засоби комунікації (системні блоки комп'ютерів, ноутбуки, айпеди, сервери тощо) з відповідним програмним забезпеченням;

– комплектуючі деталі до комп'ютерного обладнання та засобів комунікації;

– модеми та інші пристрої провідного та безпровідного Інтернет-зв'язку;

– засоби відео- та аудіозв'язку (веб-камери, мікрофони тощо);

– фото-, відеотехніка (якщо повідомлення про наявність предметів та речовин, заборонених до вільного обігу, надходило в форматі відео- або фотофайлів);

– телефонні апарати стільникового зв'язку (в протоколі обшуку вказують їхні номери IMEI);

– інструкції по користуванню до вилучених пристроїв;

– використані ваучери (картки поповнення рахунку) операторів Інтернет-зв'язку та стільникового телефонного зв'язку;

– телефонні SIM-картки операторів стільникового телефонного зв'язку;

– використані пластикові пакування ваучерів (карток поповнення рахунку) операторів Інтернет-зв'язку та SIM-карток операторів стільникового телефонного зв'язку (з метою виявлення відбитків пальців рук);

– аркуші з нотатками правопорушника (імена, паролі, адреси тощо), які можуть бути прикріплені до монітору, на столі, під клавіатурою, у смітті тощо;

– ділові щоденники з записами;

– поштові листівки та інша кореспонденція.

Під час вилучення комп'ютерного обладнання та засобів комунікації необхідно внести до протоколу їх модель, певні технічні параметри, серійні номери, мобільні та серійні номери SIM-карток операторів мобільного зв'язку, IMEI-код мобільного телефону (отримується шляхом вводу на телефоні комбінації клавіш *#06#) тощо. У пристроях мобільного зв'язку потрібно

обов’язково вилучити електронну телефонну книжку, відправлені та отримані sms-повідомлення.

Під час досудового розслідування розповсюдження через мережу Інтернет забороненого контенту, доказовою базою можуть бути зафіксовані на вилученій комп’ютерній техніці та відповідних серверах в мережі Інтернет:

– переписка електронною поштою (e-mail), через службу обміну повідомленнями (ICQ) або в інший спосіб;

– відомості стосовно використання Інтернет-ресурсів (сайтів, веб-сторінок, чатів, дощок об’яв тощо), через які здійснювалось розповсюдження забороненого контенту або реклами продажу предметів і речовин, заборонених до вільного обігу.

Крім того, доказову базу становить зафіксована в телефонних апаратах мобільного зв’язку:

– електронна телефонна книжка, яка містить інформацію про факти, час і тривалість переговорів з абонентами;

– масив відісланих та прийнятих SMS-повідомлень.

3.2.3. Встановлення способів оплати за вчиненні протиправні дії

Під час обшуку вилученню підлягають наступні предмети:

– кошти, цінності, інші предмети, які могли бути отримані в результаті вчинення протиправної діяльності;

– пластикові магнітні картки банківських установ;

– паперові чеки банківських установ про отримання грошових коштів;

– договори з банком чи банківськими установами про відкриття банківського рахунку;

– установчі документи про створення підприємства, установи, організації чи фізичної особи;

– інші документи, які підтверджують здійснення грошових оборудок (накладні, розписки, чеки, декларації, договори тощо);

– кошти, які були отримані підозрюваним в ході контрольованої поставки або оперативної закупівлі заборонених до вільного обігу предметів та речовин.

З приводу вилучених під час обшуку речей, документів та грошових коштів слідчий допитує підозрюваного (підозрюваних) та приймає рішення щодо визнання їх у якості речових доказів у кримінальному провадженні.

3.3. Призначення експертиз

Порядок надання об'єктів для експертного дослідження, а також проведення їх експертизи регламентовано наказом Міністерства юстиції України 53/5 від 08.10.1998 «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» зі змінами та доповненнями.

У постанові про призначення експертизи слідчий має вказати серійний номер комп'ютера та його індивідуальні ознаки (конфігурація, колір, написи на корпусі тощо). Він повинен детально описати знаряддя, засоби, спосіб та обставини вчинення кримінального правопорушення, зокрема, використане обладнання та програмне забезпечення, особливості комп'ютерної техніки, що надається на експертизу, її програмного забезпечення та захисних систем (логінів, паролів тощо).

Експертиза комп'ютерної техніки і програмних продуктів (комп'ютерно-технічна експертиза)

До основних завдань експертизи комп'ютерної техніки і програмних продуктів належать:

– установлення робочого стану комп'ютерно-технічних засобів;

– установлення обставин, пов'язаних із використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення;

– виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях;

– установлення відповідності програмних продуктів певним версіям чи вимогам на його розробку.

Об’єктами комп’ютерно-технічної експертизи є:

– комп’ютерна техніка (системні блоки комп’ютерів, ноутбуки, сервери тощо та їх комплектуючі);

– периферійні пристрої (принтери, сканери, дисководи, модеми, тощо), комунікаційні пристрої комп’ютерів і обчислювальних мереж;

– носії інформації (накопичувачі на жорстких магнітних дисках, комп’ютерні дискети, оптичні компакт-диски, флеш-картки пам’яті тощо);

– електронні записні книжки, айпеди, смартфони, мобільні телефони та інші електронні носії текстової або цифрової інформації.

Для дослідження робочого стану комп’ютерно-технічних засобів експерту надають ці засоби, а також технічну документацію до них; для встановлення відповідності програмних продуктів певним параметрам –надають носій з копією досліджуваного програмного продукту або програмного коду.

Для дослідження інформації, що міститься на комп’ютерному носієві, експерту надається цей носій, а за потреби – комплекс комп’ютерних засобів, до складу якого входить досліджуваний носій інформації.

З метою визначення, які саме об’єкти слід надати експерту в кожному конкретному випадку, а також як їх відбирати для дослідження, доцільно отримати консультацію експерта або спеціаліста в галузі комп’ютерної техніки.

До об’єктів, які направляються на комп’ютерно-технічну експертизу, встановлені такі вимоги:

– для збереження наданих на дослідження носіїв інформації в робочому стані вони надаються в окремих пакуваннях;

– системний блок комп’ютера та інші пристрої мають бути упаковані й опечатані в такий спосіб, що унеможливлює їхнє пошкодження, безпосередній доступ до носіїв інформації та підключення системного блока до мережі електроживлення;

– у постанові про призначення експертизи повинні бути точно вказані місце, час вилучення, а також зовнішній вигляд пристроїв та програмних продуктів, які направляються на експертизу;

– при вилученні комп'ютерів та електронних носіїв інформації їх варто упаковувати в поліетиленовий (або полотняний) пакет, який опечатують. Носії інформації можна упакувати в картонну чи пластмасову коробку та опечатати її. Варто зробити на окремому аркуші паперу докладний опис упакованих носіїв (тип кожного з них, їхня кількість). Коробку з носіями та опис поміщають до поліетиленового пакету, який заклеюють;

– під час перевезення комп'ютерних засобів вживають заходів щодо запобігання їх механічного пошкодження і взаємодії з хімічно активними речовинами.

Орієнтовний перелік вирішуваних комп'ютерно-технічною експертизою питань:

Чи міститься на даному носії інформація стосовно (зазначити, яка інформація цікавить) і у якому вигляді?

Чи містить носій досліджуваного комп'ютера інформацію про певні (зазначити, які саме) дії користувача?

Чи піддавався досліджуваний накопичувач певним процедурам з метою знищення інформації?

Чи могла бути створена зазначена інформація на цьому комп'ютері чи вона перенесена з іншого носія?

Яким чином інформація (зазначити, яка саме) перенесена до досліджуваного комп'ютера (носія)?

Яка технологія та хронологія створення електронного документа (зазначити електронний документ та певний зміст)?

Які атрибути (час друку, редагування, створення, видалення тощо) файлів, що містять інформацію стосовно... (зазначити зміст)?

Чи містить накопичувач інформації досліджуваного комп'ютера певне (зазначити, яке саме – встановлене, не встановлене) програмне забезпечення?

Які функціональні несправності мають дане комп'ютерне обладнання або його окремі складові та пристрої і як ці несправності впливають на роботу обладнання в цілому?

Чи можливо виконання певних дій за допомогою даного програмного продукту?

Чи можливе вирішення певного завдання за допомогою даного програмного продукту?

Чи реалізовані у даному програмному продукті (програмному коді) функції, передбачені технічним завданням на його розробку?

Експертиза телекомунікаційних систем та засобів

Об'єктами експертизи телекомунікаційних систем та засобів є телекомунікаційні системи, засоби, мережі і їх складові частини та інформація, що ними передається, приймається та обробляється.

Основними завданнями експертизи телекомунікаційних систем та засобів є:

– визначення характеристик та параметрів телекомунікаційних систем та засобів;

– встановлення фактів та способів передачі (отримання) інформації в телекомунікаційних системах;

– встановлення фактів та способів доступу до систем, ресурсів та інформації у сфері телекомунікацій;

– визначення якості надання телекомунікаційних послуг на рівні їх споживання;

– встановлення конфігурації та робочого стану телекомунікаційних систем та засобів;

– встановлення типу, марки, моделі та інших класифікаційних категорій телекомунікаційних систем та засобів;

– дослідження алгоритмів обробки інформації та її захисту у сфері телекомунікацій.

Орієнтовний перелік вирішуваних експертизою телекомунікаційних систем та засобів питань:

Які тип, марка, модель телекомунікаційного засобу (системи)?

Чи в робочому стані знаходиться телекомунікаційний засіб (об'єкт)?

Які характеристики підключень до мережі має телекомунікаційний засіб?

Чи змінювались користувачем телекомунікаційної мережі налаштування окремих пристроїв, у який час, які їх значення?

Який загальний характер підключень до телекомунікаційної мережі виконував об'єкт (телекомунікаційна система, засіб)?

За допомогою яких програмних засобів здійснювалось підключення до телекомунікаційної мережі?

Яка топологія апаратних засобів, об'єднаних у телекомунікаційну систему?

Чи відповідає функціонування телекомунікаційного засобу (системи) технічній документації?

Які технічні характеристики (параметри) має телекомунікаційний засіб (система)?

Чи мав місце факт доступу до телекомунікаційної системи та в який спосіб?

Чи мало місце використання ресурсів та інформації в телекомунікаційній системі та в який спосіб?

Чи мав місце факт передачі (отримання) інформації в телекомунікаційній системі та в який спосіб?

Чи є ознаки втручання в роботу телекомунікаційної системи?

Чи могли апаратні засоби об'єднуватись у телекомунікаційну мережу та за якими ознаками?

Які шляхи маршрутизації даних у телекомунікаційній системі?

Чи можливо використання телекомунікаційного засобу (обладнання) для вказаних цілей?

Експертиза слідів рук (дактилоскопічна експертиза)

Головним завданням дактилоскопічної експертизи є ідентифікація особи за слідами її рук, що залишені на місці події на комп'ютерному обладнанні, засобах комунікації, предметах, заборонених для вільного обігу, та інших предметах, яких могли торкатися підозрювані. Якщо версія про особу, що залишила слід, ще не висунута, а також якщо слідчий вважає за потрібне встановити, чи є на предметах обстановки місця події невидимі або слабовидимі сліди, перед експертом слід поставити питання про наявність такого роду слідів і їх придатність для ідентифікації особи.

Об'єктами дактилоскопічної експертизи є речові докази, на яких знайдено сліди рук або припускається їх наявність. Експертиза може бути проведена також шляхом дослідження

копії сліду на слідокопіювальній плівці, зліпка об'ємного сліду або масштабного фотознімка сліду.

Як порівняльні зразки надаються відбитки нігтьових фаланг пальців або відбитки долонь осіб, які підлягають перевірці.

Орієнтовний перелік вирішуваних дактилоскопічною експертизою питань:

Чи є на об'єкті сліди рук?

Чи придатні дані сліди для ідентифікації особи?

Чи залишені сліди рук конкретною (однією) особою?

Чи залишені однією особою сліди рук, вилучені в різних місцях?

Чи є на даному предметі сліди рук і якщо так, то чи придатні вони для ідентифікації?

Якою рукою і якими пальцями руки залишено сліди?

Які особливості мають руки людини, що залишила сліди (відсутність пальців, наявність шрамів тощо)?

Якими ділянками поверхні долоні залишено сліди?

У результаті якої дії залишено слід (захват, торкання тощо)?

Чи були сліди до вилучення на поверхні конкретного об'єкта?

Чи є ознаки переносу вилучених слідів з однієї поверхні на іншу?

Об'єкти дактилоскопічної експертизи мають надсилатися експерту в якомога коротші строки.

До кола осіб, що перевіряються, слід включати і тих, що не причетні до вчинення кримінального правопорушення, якщо вони могли залишити сліди на місці події. Установлення того факту, що слід залишила певна особа, виключить пошук нових підозрюваних і призначення зайвих експертиз.

Якщо в процесі слідчого огляду не було встановлено, якою частиною руки залишено слід, слідчий направляє експерту як порівняльні зразки відбитки всіх трьох фаланг пальців рук підозрюваної особи, а також відбитки долонь.

Якщо сліди рук після проведення дактилоскопічної експертизи мають бути направлені на судово-медичну експертизу (для встановлення групи крові тощо), слідчий зазначає про це в постанові про призначення дактилоскопічної експертизи з метою забезпечення збереження біологічної ідентичності слідів.

ВИСНОВКИ

Мережа Інтернет представляючи собою глобальну систему обміну інформаційними потоками, що об'єднала величезну кількість людей, стала не тільки предметом прогресу людства, а й дуже ефективним засобом вчинення злочинів.

Використовуючи Інтернет як середовище для протиправної діяльності, злочинці дуже часто роблять акцент на можливості, які їм дає мережа обміну інформацією: у будь-якому місці та будь-який час виходити на зв'язок, оперувати практично без обмежень за обсягом текстовою та графічною інформацією забороненого змісту, при цьому зберігаючи анонімність абонента-користувача мережі Інтернет.

Іншою відмінною рисою мережі Інтернет, як специфічного середовища, що приваблює злочинців, є можливість здійснювати в глобальних масштабах інформаційно-психологічний вплив на людей з метою поширення забороненого контенту.

Проблема документування злочинних дій, пов'язаних з розповсюдженням забороненого контенту через мережу Інтернет та організація дієвої протидії цим злочинам в україномовному сегменті мережі Інтернет для діяльності правоохоронних органів України не є новою, разом з тим ще існують певні труднощі у даному напрямку. Цьому сприяють й прогалини у законодавчому забезпеченні правоохоронних органів з протидії використанню Інтернет-мережі у протиправних цілях, недостатня організація міжвідомчої взаємодії зі встановлення конкретних користувачів, брак відповідних методик розкриття і розслідування даного виду злочинів, відсутність достатньої кількості в ОВС відповідних фахівців та високотехнологічного програмно-пошукового забезпечення в Мережі, висока латентність злочинності в Інтернет тощо.

Враховуючи складність викриття та розслідування кримінальних правопорушень вказаної категорії у запропонованих методичних рекомендаціях надається класифікація діянь, пов'язаних із розповсюдженням забороненого контенту за допомогою мережі Інтернет, алгоритм виявлення та документування дій злочинців, які використовують мережу Інтернет з метою вчинення таких злочинів та особливості проведення окремих слідчих дій у таких кримінальних провадженнях.

ЗМІСТ

Навчальне видання

СТРІЛЬЦІВ Олександр Михайлович,
КРИЖНА Валентина Володимирівна,
МАКСИМЕНКО Олена Василівна та ін.

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ ІЗ РОЗПОВСЮДЖЕННЯМ У МЕРЕЖІ ІНТЕРНЕТ ЗАБОРОНЕНОГО КОНТЕНТУ

Методичні рекомендації

Комп'ютерна верстка *Я. В. Шумко*

Підписано до друку 20.11.2014. Формат 60х84/16. Папір офсетний.
Обл.-вид. арк. 5,0. Ум. друк. арк. 4,65. Вид. № 49/ІІІ.
Тираж 20 прим. Зам. № 216

Редакційно-видавничий центр
Національної академії внутрішніх справ
03035, Київ-35, пл. Солом'янська, 1