Д.О. Максимус, О.О. Юхно

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРАЦІВНИКАМИ ОВС УКРАЇНИ ПРИ ПРОВЕДЕННІ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

Олександр Олександрович Юхно - начальник кафедри кримінального процесу факультету підготовки фахівців для підрозділів слідства ХНУВС, доктор юридичних наук, професор, полковник міліції.

Даліант Олександрович Максимус - старший слідчий слідчого відділу Красногвардійського РВ ДМУ ГУМВС України в Дніпропетровській області, старший лейтенант міліції.

Д. О. Максимус, О. О. Юхно

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРАЦІВНИКАМИ ОРГАНІВ ВНУТРІШНІХ СПРАВ ПРИ ПРОВЕДЕННІ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

УДК 343.98
ББК 67.52+67.408(4УКР)
М17

Рекомендовано до друку науково-методичною радою Харківського національного університету внутрішніх справ від 17 червня 2013 р., протокол № 6

Колектив авторів:

Максимус Д.О. – старший слідчий слідчого відділу Красногвардійського РВ ДМУ ГУМВС України в Дніпропетровській області – підрозділи –

Юхно О.О. – начальник кафедри кримінального процесу Харківського національного університету внутрішніх справ, доктор юридичних наук, професор – підрозділи –

Рецензенти:

Степанюк Р.Л. – доктор юридичних наук, доцент

Деревянкін С.Л – кандидат юридичних наук, доцент

Максимус Д.О.

Використання сучасних інформаційних технологій працівниками органів внутрішніх справ при проведенні негласних слідчих (розшукових) дій : навч. посіб. / Д.О. Максимус, О.О. Юхно. – Харків : НікаНова, 2013. – 102 с.

ISBN 976-966-2526-73-4

Навчальний посібник підготовлено по питанням актуальних проблем протидії кіберзлочинам працівниками ОВС при проведенні негласних слідчих (розшукових) дій, оперативно-розшукових заходів і наявним можливостям використання мережі Інтернету щодо виявлення таких видів злочинів з використанням пошукових сервісів, пошукових операторів у пошукових сервісах, протоколу передачі даних – File Transfer Protocol (FTP), соціальних мереж, ідентифікатора мережевого рівня (по IP адресі), а також методиці фіксації слідів злочинного спрямування у цій сфері. Посібник розрахований на курсантів, студентів, слухачів, ад'юнктів, аспірантів, викладачів, працівників правоохоронних органів та всіх, хто цікавиться розглянутими питаннями.

ЗМІСТ

ВСТУП

Стрімкий та динамічний розвиток інформаційних технологій кожен день все більше змінює аспекти економічного, політичного і соціального життя у всіх країнах світу. В середині п'ятдесятих років минулого століття телевізор був рідкістю, а тепер він є майже в кожній родині. В середині сімдесятих років того ж століття персональний комп'ютер був рідкістю, а на сьогоднішній день комп'ютером навряд чи кого здивуєш. За даними «Nua Internet Surveys» кількість користувачів глобальної мережі Інтернет із 80 тисяч у 1988 році зросла до 2,7 мільярдів у 2013 році. З моменту набрання Кримінальним процесуальним кодексом України чинної сили, кожен службовий персональний комп'ютер слідчого, з якого здійснюється доступ до Єдиного реєстру досудового розслідування (ЄРДР) має підключення до глобальної мережі Інтернет, що надає працівникам правоохоронних органів низку сучасних інформаційних інструментів для проведення слідчих (розшукових) дій і негласних слідчих (розшукових) дій. Зростання кількості персональних комп'ютерів та користувачів мережі Інтернет впливає на кількість злочинів, що все більше вчиняються з використанням інформаційних технологій. Так, в Україні у 2002 році було зареєстровано всього 30, в 2009 році вже 217 таких видів злочинів, а щорічне їх зростання складає 27 відсотків, враховуючи велику латентність, недосконаліть чинного законодавства тощо. У зв'язку з цим в системі МВС України створено спеціальні підрозділи щодо протидії викраденню людей та кіберзлочинам, що напрацьовують практику з цього напряму організаційної, слідчої, оперативно-розшукової та іншої діяльності.

Невипадково такі види злочинів ще у 1992 році були внесені ООН до списку 14 видів транснаціональних організованих злочинів, поставивши їх в один ряд із «незаконним відмиванням» грошей, терористичною діяльністю, організованим наркобізнесом, крадіжками витворів мистецтв, інтелектуальної власності, незаконною торгівлею зброєю, захватом повітряних суден, морським піратством, заволодінням наземного транспорту, ша-

хрaйством, екологічними злочинами, торгівлею людьми і людськими органами. Крім цього в Європі ще у 2001 році було підписано Конвенцію Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185, яка в нашій країні більш відома під назвою «Конвенція про кіберзлочинність», що була ратифікована Україною у 2005 році. Якщо в соціальній сфері використання новітніх технологій, особливо мережі Інтернет невпинно зростає і використовується населенням різного, починаючи з дошкільного віку, то в діяльності правоохоронних органів і, зокрема органів внутрішніх справ, у зв'язку з обмеженням фінансування, їх застосування та вирішення питань ліцензування, здійснюється досить повільно. В той же час автори навчального посібника, вивчивши наявну систему новітніх інформаційних технологій і, зокрема мережі Інтернет, прийшли до висновку, що в ній є невикористані можливості, у тому числі технічні, які нададуть допомогу працівникам підрозділів досудового розслідування та оперативних підрозділів ОВС, без використання додаткових матеріальних витрат удосконалити діяльність направлену на запобігання й протидію злочинності у сфері сучасних інформаційних технологій та мережі Інтернет, значно підвищити ефективність такої діяльності у протидії кіберзлочинності та викраденні людей. Вказане дозволить продовжити дослідження не тільки по технічним, але й правовим питанням, по розширенню можливостей, напрацюванню пропозицій та рекомендацій щодо удосконалення кримінального процесуального і кримінального законодавства України та ін. Нагальність вказаних проблем сьогодні досить гостро відчувають як вчені, так і слідчі, оперативні працівники, фахівці органів прокуратури та інших правоохоронних органів.

Навчальний посібник розрахований на курсантів, студентів, слухачів, ад'юнктів, аспірантів, викладачів, працівників правоохоронних органів, а також всіх тих, хто цікавиться вказаною проблематикою. АВТОРИ.

РОЗДІЛ 1
ОСНОВНІ КРИМІНАЛЬНО-ПРАВОВІ АСПЕКТИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

1.1 ВИМОГИ КОНВЕНЦІЇ РАДИ ЄВРОПИ ПРО ПРОТИДІЮ ЗЛОЧИННОСТІ У СФЕРІ КОМПЬЮТЕРНОЇ ІНФОРМАЦІЇ ETS № 185

Злочини у сфері сучасних інформаційних технологій приймають міжнародний та транснаціональний характер, у зв'язку с чим потерпілі від таких злочинів можуть знаходитись в різних країнах світу. Тому для протидії таким видам злочинів особливе значення має посилення і удосконалення міжнародного співробітництва в даній сфері, підвищення його ефективності.

На теперішній час вказані проблеми мають тенденцію до того, що міжнародні організації та органи влади багатьох країн вживають організаційні та правові заходи щодо запобігання та протидії злочинам у сфері сучасних інформаційних технологій. Для підтримки такої позиції, на базі використання системи криміналістичної класифікації способів вчинення правопорушень у сфері інформаційних технологій був розроблений кодифікатор Генерального Секретаріату Інтерполу, де окремо передбачені комп'ютерні злочини [1]. З метою запобігання злочинам вчиненим у сфері інформаційних технологій, 23 листопада 2001 року в Будапешті була підписана Конвенція Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185 [2], більш відома в Україні під назвою «Конвенція про кіберзлочинність». Вона відкрита для підписання як державами – членами Ради Європи, так і тими державами, які не є її членами та брали участь у її розробці. Зокрема, її підписали США і Японія. Крім того, Європейським комітетом з проблем злочинності Ради Європи в 1990 році, з метою підвищення ефективності протидії таким видам злочинів та правового визначення в Європі такої групи злочинів, пов'язаних з комп'ютерами і інформаційними технологіями, були підготовлені рекомендації про

включення в законодавство європейських країн кримінальних норм «Мінімального списку» і «необов'язкового списку» комп'ютерних злочинів.

Додатково, на початку 2002 р. був прийнятий Протокол № 1 до Конвенції про кіберзлочинність [2], який додає до вказаного переліку злочини відносно поширення інформації расистського, ксенофобного, та іншого характеру, яка підбурює до насильницьких дій, ненависті чи дискримінації окремої особи або групи осіб, що ґрунтується на расовій, національній, релігійної або етнічної приналежності. Вказаний Протокол також ратифіковано Верховною Радою України.

Згідно Конвенції Ради Європи ETS № 185 [2], яка в нашій країні має неофіційну назву про кіберзлочинність, злочини в кіберпросторі класифіковано на чотири групи, зокрема:

1) злочини, спрямовані проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, до яких входять: незаконний доступ (ст. 2), незаконне перехоплення (ст. 3), вплив на комп'ютерні дані (протиправне навмисне пошкодження, знищення, погіршення якості, зміна або блокування комп'ютерних даних) (ст. 4) або системи (ст. 5). Також в цю групу злочинів входить протизаконне використання спеціальних технічних пристроїв (ст. 6) і комп'ютерних програм, розроблених або адаптованих на вчинення злочинів, передбачених у ст. ст. 2-5, а також комп'ютерних паролів, кодів доступу, їх аналогів, за допомогою яких може бути отриманий доступ до комп'ютерної системи в цілому або будь-якої її частини. Норми ст. 6 можуть бути застосовані тільки в тому випадку, якщо використання (поширення) спеціальних технічних пристроїв спрямовано на вчинення протиправних діянь;

2) злочини, пов'язані з використанням комп'ютерних засобів. До них відносяться підроблення та шахрайство з використанням комп'ютерних технологій (ст. ст. 7; 8). Підробка з використанням комп'ютерних технологій включає в себе зловмисні і протиправні введення, зміна, видалення або блокування комп'ютерних даних, що тягнуть за собою порушення автентичності

даних, з наміром, щоб вони розглядалися або використовувалися в юридичних цілях в якості автентичних;

3) злочини, що здійснюються засобом виробництва (з метою розповсюдження через комп'ютерну систему), надання пропозицій для користування, поширення та придбання різних видів дитячої порнографії, а також володіння дитячою порнографією, що знаходиться в пам'яті комп'ютера певної особи (ст. 9);

4) злочини, пов'язані з порушенням авторського права і суміжних прав, щодо програмного забезпечення (в законодавстві України – це ст. 176 КК України [5]).

Питання для самоперевірки та контролю засвоєння знань:

1. Чи є актуальним питання приєднання України до міжнародних угод щодо протидії і запобіганню кіберзлочинності ?

2. Чи імплементовані вимоги Конвенція Ради Європи ETS № 185 «Про кіберзлочинність» у національне законодавство ?

3. Якими є зміст та основні вимоги Конвенції Ради Європи ETS № 185 «Про кіберзлочинність»?

Список рекомендованої літератури:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

2. Кримінальний процесуальний кодекс України. – К.: Юрінком Інтер, 2013. – 608 с.

3. Конвенція Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185, ратифіковано Верховною Радою України із застереженнями і заявами Законом N 2824-IV (2824-15) від 07.09.2005, ВВР, 2006, N 5-6, ст.71.

4. Класифікація комп'ютерних злочинів по кодифікатору Генерального Секретаріату Інтерполу [Електронний ресурс]. – Режим доступу: http://www.cyberpol.ru/cybercrime.shtml

5. Гуславский В. С., Задорожний Ю. А., Розовский В. Г. Информационно-аналитическое обеспечение раскрытия и расследования преступления // Монография – Луганск, ТОВ «Елтон-2», 2008. – 133 с.

1.2 КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА ЗЛОЧИНИ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ В УКРАЇНІ

Родовим об'єктом злочинів, відповідальність за які передбачена розділом XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального Кодексу України є сукупність суспільних відносин, що виникають щодо обробки (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), захисту комп'ютерної інформації та експлуатації засобів, що їх забезпечують (ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку).

Предметом злочинів, відповідальність за які передбачена ст. ст. 361–363-1 КК України можуть бути:

1) електронно-обчислювальні машини (комп'ютери);
2) автоматизовані системи;
3) комп'ютерні мережі;
4) мережі електрозв'язку;
5) інформація;
6) шкідливі програмні чи технічні засоби;
7) повідомлення електрозв'язку.

Спираючись на перелік безпосередніх предметів кримінальних правопорушень, відповідальність за які передбачена ст. ст. 361–363-1 КК України, доцільним є детальне розкриття сутності предмету вказаних видів злочинів:

1) електронно-обчислювальна машина (комп'ютер) – це будь-який пристрій або група взаємно поєднаних пристроїв, один чи більш з яких, у відповідності до певної програми, виконує автоматичну обробку інформації і обладнаний допоміжним устаткуванням (пристосуванням), що дозволяє будь-яким чином змінювати або перезаписувати керуючі

програми й (або) дані, необхідні для реалізації процесором його цільових функцій.

Слід додати, що Розділ XVI КК України характеризується неузгодженістю термінів, як в самому розділі, так і щодо інших нормативно-правових актів.

Крім того, і термін ЕОМ, на сьогодні вже є архаїчним. Вже розроблюються і є прототипи біокомп'ютерів, оптичних, квантових комп'ютерів, тобто комп'ютерів, що використовують відмінну від електронної технологію, тому, термін «електронно-обчислювальні машини» – це тимчасова дефініція і її використання у недалекому майбутньому при застосуванні комп'ютерними злочинцями нових нейрокомп'ютерів вже не дозволить криміналізувати їх протиправні діяння.

2) Автоматизована (інформаційна) система, згідно із ст. 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» – це організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

3) Комп'ютерна мережа це комплекс (сукупність) з'єднаних лініями зв'язку комп'ютерів. В залежності від швидкості обміну даними між робочими комп'ютерами й розмірів охопленої території розрізняють локальні, регіональні та глобальні комп'ютерні мережі.

4) Виходячи з положень ст. 1 Закону України «Про телекомунікації» можна зробити висновок, що мережі електрозв'язку (як синонім до телекомунікаційних мереж) – це комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням.

5) Інформація – розуміє документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі (ст. 1 Закону України «Про інформацію»). Згідно із ст. 28 вказаного Закону, за режимом доступу інформація поділяється на відкриту

інформацію та інформацію з обмеженим доступом. Предметом злочину відповідальність за який передбачено ст. 362 КК України є саме інформація з обмеженим доступом. Така інформація за своїм правовим режимом поділяється на конфіденційну і таємну. **Конфіденційна інформація** – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. **До таємної інформації** належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі. **Інформація, що є предметом аналізованих злочинів,** повинна зберігатися чи оброблюватися в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах, мережах електрозв'язку або на носіях такої інформації. Обробка інформації в системі - це виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, що здійснюються в системі за допомогою технічних і програмних засобів. Комп'ютерні програми також відносяться до інформації.

6) Шкідливі програмні чи технічні засоби – це комп'ютерні програми та пристрої (устаткування) призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, тобто для вчинення злочину відповідальність за який передбачено у ст. 361 КК України. Технічні засоби в більшості випадків реалізовані як апаратно-програмні пристрої. До таких шкідливих програмних засобів можна віднести комп'ютерні віруси. Слід вказати, що програмні чи технічні засоби призначені для інших цілей, наприклад, для відновлення роботи автоматизованої системи, не є предметом даних злочинів.

7) Повідомлення електрозв'язку це .- повідомлення, що передаються по радіо, проводових, оптичних або інших електромагнітних системах. Наприклад, це можуть бути листи електронної пошти, SMS, MMS.

Об'єктивна сторона цих злочинів може виражатися як в активних діях (наприклад, в несанкціонованому втручанні в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України), так і в злочинній бездіяльності, наприклад, при порушенні правил експлуатації автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж (ст. 363 КК України).

Склади злочинів, що розглядаються сформульовані в законі як матеріальні (ст. ст. 361, 362, 363, 363-1 КК України) та деякі формальні.

Суб'єкт (загальний) цих злочинів це будь-яка особа, що досягла віку 16 років, а у деяких випадках суб'єкт спеціальний: особа, яка має право доступу до інформації, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації (ст. 362 КК), особа, яка відповідає за експлуатацію ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж, мереж електрозв'язку (ст. 363 КК).

Суб'єктивна сторона цих злочинів передбачає, як правило, умисну вину. Хоча можлива й необережність – при порушенні правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України).

У всіх складах злочинів передбачених розділом XVI КК України (у ст. 363 КК України – ознака основного складу злочину) однією із кваліфікуючих (особливо кваліфікуючих) ознак є спричинення злочином значної шкоди. Згідно примітки до ст. 361 КК України, у всіх складах злочинів ХУ1 розділу КК України шкода визнається значною, якщо вона полягає у заподіянні матеріальних збитків, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України): безпосереднім об'єктом даного злочину є

суспільні відносини щодо обробки інформації в комп'ютерах, автоматизованих системах, комп'ютерних мережах, мережах електрозв'язку та забезпечення їх нормальної роботи.

Об'єктивна сторона злочину характеризується вчиненням діяння у вигляді несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що потягло наслідки у вигляді витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації.

Несанкціоноване втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – це будь який вплив (у тому числі й механічний) на їх роботу (процес обробки інформації) особою, яка не мала ні реального, ні уявного права на зміну, блокування інформації, спотворення процесу обробки інформації або на зміну порядку її маршрутизації.

Виток інформації – це результат дій (копіювання, зняття з каналів зв'язку, фотографування з дисплея), внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї.

Підробка інформації – це зміна її змісту шляхом внесення неправдивих відомостей.

Втрата інформації полягає в такій її зміні, коли використання чи відновлення інформації неможливе.

Блокування інформації – це дії, внаслідок яких унеможливлюється доступ до інформації в системі. Обов'язковою ознакою блокування є повернення можливості доступу користувачів до інформації, яка повертається автоматично, або після втручання людини.

Під порушенням установленого порядку маршрутизації інформації слід розуміти зміну режиму роботи телекомунікаційної мережі (мережі електрозв'язку), внаслідок якої інформація, що передається в цій мережі, не потрапляє до тієї особи, до якої вона повинна дійти, тобто вона блокується для цієї особи.

Суб'єктивна сторона – прямий або непрямий умисел. Мотив та мета злочину на кваліфікацію не впливають.

Суб'єкт злочину – загальний: фізична, осудна особа, яка досягла 16-річного віку.

Кваліфікуючі ознаки злочину – за ч. 2 – 1) вчинення злочину повторно або 2) за попередньою змовою групою осіб, або 3) якщо було заподіяно значну шкоду.

Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1 КК України): безпосереднім об'єктом даного злочину є суспільні відносини, щодо обробки інформації в комп'ютерах, автоматизованих системах, комп'ютерних мережах, мережах електрозв'язку та забезпечення їх нормальної роботи.

Предметом злочину є шкідливі програмні чи технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Об'єктивна сторона злочину може полягати у вчиненні таких альтернативних дій: 1) створення, 2) розповсюдження або 3) збут вказаних шкідливих програмних чи технічних засобів.

Створення шкідливих програмних засобів – це написання її алгоритму, тобто послідовності логічних команд, з подальшим перетворенням його в машинну мову ЕОМ, а також внесення змін у існуючі програмні засоби в результаті чого основним їх призначенням стає несанкціоноване втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Створення шкідливих технічних засобів – це виготовлення таких засобів будь-яким способом, а також переробка пристроїв (устаткування) в результаті чого основним їх призначенням стає несанкціоноване втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Розповсюдження шкідливих програмних засобів – це надання доступу до відтвореної в будь-якій матеріальній формі програми

для ЕОМ, у тому числі мережними й іншими способами (програмою може скористатися невизначене або певне коло осіб).

Розповсюдження шкідливих технічних засобів – розуміється їх передача на яких би то не було умовах третім особам.

Збутом, шкідливих програмних чи технічних засобів є їх умисне відчуження як сплатне, так і безоплатне (використання як засобу платежу, продаж, розмін, обмін, дарування, передача в борг або в рахунок покриття боргу, програш в азартних іграх тощо).

Суб'єктивна сторони злочину характеризується виною у формі прямого умислу. Для створення вказаних засобів – обов'язково встановлення мети їх використання, розповсюдження або збуту.

Суб'єкт злочину – загальний: фізична, осудна особа, яка досягла 16-річного віку.

Кваліфікуючими ознаками злочину, за ч. 2 є вчинення злочину 1) повторно або 2) за попередньою змовою групою осіб, або 3) якщо було заподіяно значну шкоду.

Несанкціоновані збут або 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 КК України): предметом злочину є інформація з обмеженим доступом, яка зберігається в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації.

Об'єктивна сторона злочину полягає у вчиненні однієї з альтернативних дій: 1) несанкціонований збут або 2) несанкціоноване розповсюдження інформації з обмеженим доступом, що є предметом злочину. Збут або розповсюдження є несанкціонованими у випадку коли винна особа не мала ні реального, ні уявного права на ознайомлення з такою інформацією невизначеного або певного кола осіб, а також на передачу будь-яким способом даної інформації третім особам.

Суб'єктивна сторона – вина у формі умислу, як прямого так і непрямого. Мотив та мета на кваліфікацію не впливають.

Суб'єкт злочину – загальний: фізична, осудна особа, яка досягла 16-річного віку.

Кваліфікуючими ознаками злочину, за ч. 2 є вчинення злочину: 1) повторно або 2) за попередньою змовою групою осіб, або 3) якщо було заподіяно значну шкоду.

Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України): предмет злочину – інформація, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації.

Об'єктивна сторона злочину полягає у несанкціонованих: 1) зміні, 2) знищенні або 3) блокуванні зазначеної інформації. У ст. 362 КК України поняття зміна, знищення та блокування використовуються для позначення одночасно і суспільне небезпечного діяння, і суспільно небезпечних наслідків.

Зміна інформації – це зміна змісту або форми інформації, закладеної в носії.

Знищення інформації полягає в такій її зміні, коли використання чи відновлення інформації неможливе. Знищенням інформації треба вважати й такі дії, внаслідок яких перестають існувати лише копії тих чи інших даних, а оригінали або інші примірники залишаються непошкодженими. Власник інформації може створювати будь-яку кількість копій, зберігати інформацію у будь-якому вигляді.

Блокування інформації було розглянуто при аналізі злочину передбаченого ст. 361 КК України.

Суб'єктивна сторона – вина у формі умисли, як прямого так і непрямого.

Суб'єкт злочину – спеціальний: особа, яка має право доступу до інформації, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації.

Кваліфікуючі ознаки злочину:

• за ч. 2 – несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації;

• за ч. 3 – вчинення злочину 1) повторно або 2) за попередньою змовою групою осіб, або 3) якщо було заподіяно значну шкоду.

Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України): безпосередній об'єкт злочину – встановлений порядок експлуатації комп'ютерів (ЕОМ), автоматизованих систем, комп'ютерних мереж, мереж електрозв'язку або порядок захисту інформації, яка в них оброблюється.

Об'єктивна сторона злочину полягає в порушенні правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, що потягло настання наслідків у вигляді значної шкоди.

Диспозиція ст. 363 КК України має бланкетний характер – для притягнення особи до відповідальності слід установити, які конкретно правила нею було порушено та яким нормативним актом ці правила встановлено.

Під правилами експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, слід розуміти будь-які технічні правила, які регламентують користування цими машинами, системами чи мережами, проведення робіт з їх використанням, захисту таких машин, систем та мереж або інформації, яка в них знаходиться, тощо.

Це можуть бути правила: установлені виробниками комп'ютерного устаткування; встановлені розроблювачами програмного забезпечення; внутрішнього розпорядку, встановлені власниками комп'ютерної системи чи мережі та інші.

Захист інформації (у т.ч. комп'ютерної), що є власністю держави, або захист якої гарантується державою, здійснюється з дотриманням правил, що встановлюються спеціально вповноваженим державним органом. На даний час таким органом є Департамент спеціальних телекомунікаційних систем та захисту інформації СБУ.

Суб'єктивна сторона – щодо порушення правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж, мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, можлива будь-яка форма вини, як умисел, так і необережність, а щодо суспільно небезпечних наслідків можлива тільки необережна форма вини.

Суб'єкт – особа, яка відповідає за експлуатацію ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж, мереж електрозв'язку. Підтверджується відповідальність особи за дотримання правил відповідними нормативними актами й документами.

Якщо зазначені в ст. 363 КК України дії вчинені службовою особою, то за наявності в її діях ознак службових злочинів, передбачених статтею 364 або 365 КК України, вчинене слід кваліфікувати за сукупністю злочинів.

Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1 КК):

Предмет – повідомлення електрозв'язку.

Об'єктивна сторона злочину передбачає вчинення діяння у вигляді масового розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів; що потягло наслідки у вигляді порушення або припинення роботи ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Суб'єктивна сторона – умисна форма вини.

Суб'єкт – загальний: фізична, осудна особа, яка досягла 16-річного віку.

Кваліфікуючі ознаки – за ч. 2: вчинення злочину 1) повторно або 2) за попередньою змовою групою осіб, або 3) якщо було заподіяно значну шкоду.

Питання для самоперевірки та контролю засвоєння знань:

1. Який розділ Кримінального кодексу України передбачає кримінальну відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку ?

2. Назвіть статті Кримінального кодексу України які передбачають кримінальну відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку ?

3. Які склади злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку передбачені розділом XVI Кримінального кодексу України?

Список рекомендованої літератури:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

2. Кримінальний кодекс України. Кримінальний процесуальний кодекс України. – К.: Юрінком Інтер, 2013. – 608 с.

3. Закон України «Про основи національної безпеки України» зі змінами та доповненнями – Відомості Верховної Ради України (ВВР), 2003, N 39, ст. 351.

4. Уголовный кодекс Российской Федерации / Авт.-сост. Коммент. Д. А. Гайдуков, С. А. Перчаткина. – М. : Эксмо, 2009. – 336 с.

5. Уголовный кодекс Федеративной Республики Германии / Науч. ред. и вступ. статья Д. А. Шестакова; предисл. доктора права Г. Г. Йешека; перевод с нем. Н. С. Рачковой. – СПб. : Юридический центр Пресс, 2003. – 524 с.

1.3 ВІДПОВІДНІСТЬ СТАТЕЙ КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ ДО КЛАСИФІКАЦІЇ КОМПЬЮТЕРНИХ ЗЛОЧИНІВ ПО КОДИФІКАТОРУ ГЕНЕРАЛЬНОГО СЕКРЕТАРІАТУ ІНТЕРПОЛУ

Згідно до Конвенції Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185 [2], кожна країна учасниця зобов'язана створити необхідні правові умови для запобігання таким видам злочинів компетентними органам у протидії кіберзлочинності, зокрема: виїмку системних блоків комп'ютерів чи комп'ютерної системи, її частини або носіїв; виготовлення та вилучення копій комп'ютерних даних; забезпечення збереження комп'ютерних даних у повному та цілісному стані; знищення або блокування комп'ютерних даних, які знаходяться в комп'ютерній системі. Але між законодавством Євросоюзу та законодавством окремих країн Європи і Азії, країн СНД, існує чимало розбіжностей, які унеможливлюють, чи суттєво ускладнюють виконання зобов'язань, які встановлює Конвенція Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185 [2]. У зв'язку з вказаним, країни що підтримали ці міжнародні акти, повинні привести національне законодавство до міжнародних правових стандартів.

Для більш повного розуміння сутності проблеми розбіжності національних законодавств країн світу з Класифікацією комп'ютерних злочинів по кодифікатору Генерального Секретаріату Інтерполу [1], доцільним буде цей кодифікатор навести в даному навчальному посібнику. Всі коди, що характеризують комп'ютерні злочини, мають ідентифікатор, що починається на букву Q. Для опису злочину використовуються до п'яти кодів, розташованих у порядку зменшення значимості вчиненого виду злочину [1], зокрема:

1) QA - несанкціонований доступ і перехоплення (QAH-комп'ютерний абордаж, QAI - перехоплення, QAT - крадіжка часу, QAZ-інші види несанкціонованого доступу і перехоплення);

2) QD-зміна комп'ютерних даних (QUL - логічна бомба, QDT-троянський кінь, QDV - комп'ютерний вірус, QDW - комп'ютерний черв'як, QDZ - інші види зміни даних);

3) QF - комп'ютерне шахрайство (QFC - шахрайство з банкоматами, QFF-комп'ютерна підробка, QFG - шахрайство з ігровими автоматами, QFM - маніпуляції з програмами введення-виведення, QFP-шахрайство з платіжними засобами, QFT - телефонне шахрайство, QFZ - інші комп'ютерні шахрайства);

4) QR-незаконне копіювання (QRG - комп'ютерні ігри, QRS - інше програмне забезпечення, QRT - топографія напівпровідникових виробів, QRZ - інше незаконне копіювання);

5) QS - комп'ютерний саботаж (QSH - з апаратним забезпеченням, QSS - із програмним забезпеченням, QSZ - інші види саботажу);

6) QZ - інші комп'ютерні злочини (QZB - з використанням комп'ютерних дошок оголошень, QZE - розкрадання інформації, що становить комерційну таємницю, QZS - передача інформації конфіденційного характеру, QZZ - інші комп'ютерні злочини).

Спираючись на національні джерела, а так само і на саму науку кримінального права, в даній роботі слід навести умовну відповідність статей Кримінального кодексу України в редакції 2001 року (з внесеними змінами), до класифікації комп'ютерних злочинів по кодифікатору Генерального Секретаріату Інтерполу:

1) QA - несанкціонований доступ і перехоплення:

1.1) QAH-комп'ютерний абордаж, або «Незаконний доступ до комп'ютерної системи або мережі» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст. 363 КК «Порушення роботи автоматизованих систем».

1.2) QAI - перехоплення, «Незаконне перехоплення за допомогою будь-яких технічних пристроїв та засобів зв'язку даних, які знаходяться в комп'ютерній системі або мережі, чи прямують до (або) з неї» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст. 163 КК «Порушення таємниці листування, телефонних розмов, телеграфних та інших повідомлень, що передаються засобами зв'язку», або ст. 231 КК «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю».

1.3) QAT - крадіжка часу, «Неправомірне використання комп'ютера або комп'ютерної мережі з наміром уникнути

оплати за користування» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст. 163 КК «Порушення таємниці листування, телефонних розмов, телеграфних та інших повідомлень, що передаються засобами зв'язку».

2) QD-зміна комп'ютерних даних:

2.1) QUL - логічна бомба, «Незаконна заміна комп'ютерних даних або програм шляхом впровадження Логічної Бомби» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст.ст. 361-363 КК «Порушення роботи автоматизованих систем».

2.2) QDT-троянський кінь, «Незаконна зміна комп'ютерних даних або програм шляхом впровадження «Троянського Коня» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст.ст. 361-363 КК «Порушення роботи автоматизованих систем».

2.3) QDV - комп'ютерний вірус, «Незаконна зміна комп'ютерних даних або програм шляхом впровадження або розповсюдження комп'ютерних вірусів» [3]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст. 361, 362 КК «Порушення роботи автоматизованих систем».

2.4) QDW - комп'ютерний черв'як, «Незаконна зміна комп'ютерних даних або програм пересилкою, впровадженням або розповсюдженням комп'ютерних черв'яків по комп'ютерних мережах» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст.ст. 361, 362 КК «Порушення роботи автоматизованих систем».

3) QF - комп'ютерне шахрайство:

3.1) QFC - шахрайство з банкоматами, «Шахрайство та крадіжки з використанням автоматів по видачі готівки» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** потребує детального вивчення матеріалів кожної окремо взятої справи.

3.2) QFF-комп'ютерна підробка, «Шахрайство та крадіжки пов'язані з виготовленням підроблених засобів з застосуванням комп'ютерних технологій» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст.ст.199, 200 КК «Виготовлення, зберігання, придбання, перевезення, пересилання, збут підроблених грошей, державних цінних паперів».

3.3) QFG - шахрайство з ігровими автоматами, «Шахрайство та крадіжки з використанням ігрових автоматів» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст.ст. 361-363 КК «Порушення роботи автоматизованих систем».

3.4) QFM - маніпуляції з програмами введення-виведення, «Шахрайство та крадіжка шляхом неправильного вводу/виводу з комп'ютерної системи або маніпуляції програмами» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст.ст. 361-363 КК «Порушення роботи автоматизованих систем».

3.5) QFP-шахрайство з платіжними засобами, «Шахрайство та крадіжка, пов'язані з платіжними засобами та системами реєстрації платежів» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст.ст. 361-363 КК «Порушення роботи автоматизованих систем».

3.6) QFT - телефонне шахрайство, «Несанкціонований доступ до (теле-) комунікаційних послуг з порушенням загальноприйнятих протоколів та процедур» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст. 163 КК «Порушення таємниці листування, телефонних розмов, телеграфних та інших повідомлень, що передаються засобами зв'язку».

4) QR-незаконне копіювання:

4.1) QRG - комп'ютерні ігри, «Несанкціоноване копіювання, незаконне втручання в роботу комп'ютерних мереж, розповсюдження або публікація комп'ютерних ігор» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст. 176 КК «Порушення авторського права», та ст. 361 КК «Порушення роботи автоматизованих систем».

4.2) QRS - інше програмне забезпечення, «Несанкціоноване копіювання, викрадення чи привласнення, вимагання комп'ютерної інформації, розповсюдження або публікація програмного забезпечення, захищеного авторським правом» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст. 176 «Порушення авторського права», та ст. 362 КК «Порушення роботи автоматизованих систем».

4.3) QRT - топографія напівпровідникових виробів, «Виробництво без дозволу копій топології інтегральних мікросхем, які

захищені законом, або їх недозволене тиражування, комерційне використання чи імпорт» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст. 176 КК «Порушення авторського права».

5) QS - комп'ютерний саботаж:

5.1) QSH - з апаратним забезпеченням, «Внесення, зміна, пошкодження або знищення комп'ютерних даних або програм, а також втручання до комп'ютерної системи, з наміром перешкоджати функціонуванню комп'ютера або телекомунікаційної системи» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст.ст. 361-363 «Порушення роботи автоматизованих систем».

5.2) QSS - із програмним забезпеченням, «Незаконне пошкодження, порушення, викривлення та знищення комп'ютерних даних або програм» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст.ст. 361-363 «Порушення роботи автоматизованих систем».

6) QZ - інші комп'ютерні злочини:

6.1) QZB - з використанням комп'ютерних дошок оголошень, «Використання Bulletin Board System (BBS) для приховування, обміну та розповсюдження матеріалів, пов'язаних з кримінальними злочинами» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст. 176 «Порушення авторського права».

6.2) QZE - розкрадання інформації, що становить комерційну таємницю, «Незаконне привласнення або розголошення, передавання або використання комерційної таємниці з наміром спричинити економічні збитки або отримати незаконні економічні вигоди» [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст.ст. 361-363 «Порушення роботи автоматизованих систем».

6.3) QZS - передача інформації конфіденційного характеру, «Використання комп'ютерних систем або мереж для зберігання або пересилки матеріалів, які є об'єктом судового переслідування». [1]. **Кваліфікація згідно до КК України в редакції 2001 року:** ст.ст. 361-363 КК «Порушення роботи автоматизованих систем».

Враховуючи наведене, можна дійти до висновку, що чинні норми кримінального законодавства які використовуються для протидії комп'ютерним злочинам в країнах Європи і ряді інших країн, вимагають проведення порівняльного аналізу на предмет сумісності й можливості адекватного застосування у правозастосовній діяльності їх правоохоронних органів. Саме узгодженність норм кримінального законодавства країн Європи, а так само та інших країн є однією із вимог Конвенції про кіберзлочинність [2], реалізація якої направлена на підвищення ефективності протидії кіберзлочинності на міждержавному рівні та співпраці країн учасників.

Питання для самоперевірки та контролю засвоєння знань:

1. На які групи поділено коди комп'ютерних злочинів згідно до кодифікатору генерального секретаріату Інтерполу ?

2. Статті якого розділу Кримінального кодексу України умовно відповідають кодам кодифікатору генерального секретаріату Інтерполу?

3. Які конкретні статті Кримінального кодексу України умовно відповідають кодам кодифікатору генерального секретаріату Інтерполу ?

Список рекомендованої літератури:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

2. Кримінальний кодекс України. Кримінальний процесуальний кодекс України. – К.: Юрінком Інтер, 2012. – 608 с.

3. Конвенція Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185, ратифіковано Верховною Радою України із застереженнями і заявами Законом N 2824-IV (2824-15) від 07.09.2005, ВВР, 2006, N 5-6, ст.71.

4. Класифікація комп'ютерних злочинів по кодифікатору Генерального Секретаріату Інтерполу [Електронний ресурс]. – Режим доступу: http://www.cyberpol.ru/cybercrime.shtml

1.4 ОСНОВНІ АСПЕКТИ ЗАГАЛЬНОЇ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ НАЙБІЛЬШ ПОШИРЕННИХ ЗЛОЧИНІВ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УКРАЇНІ

На сьогоднішній день проблема вчинення, виявлення та розслідування злочинів у сфері інформаційних технологій має глобальний, міжнародний та міжнаціональний характер. За даними Nua Internet Surveys кількість користувачів глобальної мережі Інтернет з 80 тисяч у 1988 році зросла до 2,4 мільярдів на кінець 2012 року [8]. Зростання кількості користувачів мережі Інтернет не може не відобразитись на кількості злочинів, вчинених у сфері інформаційних технологій. Слід також зазначити, що у зв'язку з існуванням у світі значної загрози з боку комп'ютерного тероризму, дане питання актуальне на сьогодні і для України. Задачі протидії цьому закріплено в Законі України «Про основи національної безпеки України» [9], в статті 7 якого «комп'ютерний тероризм» та «комп'ютерна злочинність» визначені серед основних потенційних та реальних загроз національній безпеці України в інформаційній сфері.

За дослідженням в Україні, на сьогоднішній день, механізми виявлення та розслідування злочинів у сфері новітніх інформаційних технологій потребують подальшого удосконалення та наукових вивчень, а також напрацювання нових методик їх викриття та розслідування. Слід надати визначення цій категорії злочинів.

На нашу думку, визначення поняття цієї категорії злочинів може бути наступним: злочини у сфері інформаційних технологій – це злочини корисливої направленості, що здійснюються особами з використанням сучасних інформаційних технологій, та зокрема Інтернету для досягнення злочинних цілей.

За останній час в Україні та країнах СНД, прийнято називати такі злочини кіберзлочинністю, тобто злочинами у сфері інформаційних технологій, які можна класифікувати на три групи: перша група злочинів у сфері інформаційних технологій включає в себе: «злом» паролів і крадіжку номерів кредитних карток

та інших банківських реквізитів, тобто так званий «фішинг», який більше пов'язаний з використанням існуючих інформаційних технологій, що використовуються у сфері обслуговування громадян, без використання мережі Інтернет; друга група включає в себе такі види злочинів у сфері інформаційних технологій, які тісно зв’язані з використанням мережі Інтернет: поширення шкідливих вірусів; поширення через мережу Інтернет протиправної інформації, яка збуджує міжнаціональну та міжрелігійну ворожнечу, ксенофобію і релігійний фанатизм; матеріали порнографічного характеру чи наклепу; третю групу об’єднує найбільш небезпечні та поширені злочини проти власності, зокрема шахрайства, вчинені з використанням інформаційних технологій та мережі Інтернет. Такі шахрайства, вчиняються з використанням мережі Інтернет в якості засобу спілкування і входження в довіру до потерпілої особи, що відрізняє від входження в довіру до особи при вчиненні звичайного «побутового» шахрайства без використання мережі Інтернет. До цієї групи шахрайств слід віднести інші види шахрайств, що вчиняються із використанням Інтернет – аукціонів, в яких непомітно для покупця самі продавці роблять ставки, штучно створюючи уяву про ніби то участь багатьох покупців у аукціоні, щоб підняти ціну виставленого на аукціон товару. Крім цього у цій групі слід виділити такі види шахрайств, коли умовний продавець виставляє на огляд в мережі Інтернет лише фотографії товару, пропонує здійснити оплату за нього, а після отримання грошей, фактичну пересилку товару покупцеві не здійснює.

У зарубіжних країнах, зокрема США, набули поширення факти шахрайств, пов'язані із продажем доменних імен Інтернет–сайтів. Для вчинення таких злочинів проводиться масова розсилка електронних повідомлень, в яких, наприклад, повідомляється про спроби невідомих осіб зареєструвати доменні імена, схожі на адреси, котрі вже належать адресатам сайтів, і власникам сайтів пропонується зареєструвати непотрібне їм доменне ім'я, щоб випередити цих осіб. Враховуючи значне і швидке розповсюдження новітніх інформаційних технологій,

появи вказаних видів злочинів слід очікувати і в Україні. У зв'язку з цим методику виявлення, розкриття та розслідування таких видів злочинів слід удосконалювати за рахунок продовження досліджень та наукових вивчень і напрацювання рекомендацій для практичних працівників правоохоронних органів.

Питання для самоперевірки та контролю засвоєння знань:

1. Які основні положення закріплено у Законі України «Про основи національної безпеки України»?

2. Які види злочинів у сфері інформаційних технологій найбільше всього поширені в Україні?

Список рекомендованої літератури:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

2. Кримінальний процесуальний кодекс України. – К.: Юрінком Інтер, 2012. – 608 с.

3. Закон України «Про основи національної безпеки України» зі змінами та доповненнями – Відомості Верховної Ради України (ВВР), 2003, N 39, ст.351.

4. І.О. Борозенний, О. О. Юхно Особливості використання мережі Інтернет та автоматизованих інформаційно-пошукових систем для забезпечення проведення негласних слідчих (розшукових) дій // Право і Безпека : науковий журнал, № 4 (46) за 2012 рік, - Харківський національний університет внутрішніх справ : видавництво ХНУВС, 2012. – 360 с.

5. Захарченко В.Ю., Лазуренко В. И., Олифиров А. В . , Рогозин С.Н. Компьютерные преступления: их выявление и предотвращение: Учебное пособие / Под общ. редакцией В. И. Лазуренко. – К.: Центр учебной литературы, 2007. – 170 с.

6. Словарь криминологических и статистических терминов / А. Г. Кальман, И. А. Христич. – Х. : Гимназия : Ин-т изучения проблем преступности АПрН Украины, 2001. – 94 с.

7. Двенадцатый Конгресс ООН по предупреждению преступности и уголовному правосудию [Электронный ресурс]. – Режим доступа: http://www.un.org/ru/conf/crimecongress2010.

РОЗДІЛ 2.
ОСОБЛИВОСТІ ВИКОРИСТАННЯ АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНО-ПОШУКОВИХ СИСТЕМ МВС УКРАЇНИ ТА МЕРЕЖІ ІНТЕРНЕТ ЩОДО ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

2.1 ОКРЕМІ МОЖЛИВОСТІ АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНО-ПОШУКОВИХ СИСТЕМ МВС ДЛЯ ПРОВЕДЕННЯ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

Тенденції розвитку оперативно-розшукової діяльності у сфері використання інформаційних технологій спираються на застосування спеціальних технічних засобів контролю, фіксації та обробки інформації. Слід зазначити, що працівники органів внутрішніх справ (далі – ОВС) відстають від вимог часу, залишаючись технічно недостатньо озброєними в сучасному стані, від чого ефективність запобігання, виявлення та розкриття кримінальних правопорушень з використанням оперативно-розшукових заходів є низькими, і це важко приховати. Згідно із статистичними даними правоохоронних органів, біля 35–40% традиційних злочинів щорічно вчиняється з використанням сучасних телекомунікаційних, комп'ютерних та інших технологій, а у майбутньому цей відсоток може суттєво збільшитись. Необхідно зазначити, що після створення в МВС України автоматизованих інформаційно-пошукових, інформаційно-аналітичних та біометричних систем, інформаційно-аналітичне забезпечення працівників ОВС стало набагато якісним і кращим. Початком формування та створення зазначених систем стало створення в 2001 році Інтегрованого банку даних, що об'єднав в єдиний логічно позв'язаний інформаційний масив усі обліки МВС України, а також першої версії програмного забезпечення «АРМОР». На даний момент, крім автоматизованої інформаційно-пошукової системи «АРМОР»,

створені інші системи, які дозволяють працівникам міліції отримувати значно більше даних про осіб, які представляють оперативний інтерес, але за набагато менший проміжок часу ніж раніше. Докладніше проведемо аналіз такої системи, як автоматизована інформаційно-пошукова системи «АРМОР». Вказана інформаційно-пошукова система «АРМОР», або «автоматизоване рабоче місце оперативного працівника» - це автоматизована інформаційно-пошукова система, до основних функцій якої належить: облікова, спостерігаюча, довідкова, пошукова, прогнозуюча та статистична функція. «АРМОР» забезпечує виконання таких завдань, що пов'язані з оперативним управлінським використанням інформації, яка зберігається в інтегрованому банку даних МВС України, а також накопичення та обробку нових даних. При наявності у конкретного користувача права доступу до системи, автоматизована інформаційно-пошукова система «АРМОР» доступна для всіх підрозділів і служб міліції України, що має велике значення при пошуку інформації про особу, яка представляє оперативний чи інший службовий інтерес для працівників підрозділів досудового розслідування, оперативних та інших підрозділів ОВС. На сьогоднішній день, в рамках інтегрованого банку даних МВС України, система «АРМОР» поєднала у собі більше п'ятидесяти автоматизованих підсистем, наприклад: «Адреса», «Адмінпрактика», «Документ», «Розшук», «Розшук-Україна», «Розшук-СНД», «Запити», «Фото», «Сонда», «Юридичні особи», «Угон», «Мігрант», «Злочин», «Загублені документи» та інші. Крім того, лише автоматизований облік осіб, які попали в поле зору міліції, зараз нараховує більше п'ятдесяти категорій, зокрема: «БОМЖ», «раніше засуджений», «умовно засуджений», «гомосексуаліст», «власник зброї», «споживач наркотиків», «наркоман», «дезертир», «організатор злочинної групи», «учасник злочинної групи», «проститутка», «неповнолітній», та інші. В Україні, на даний момент, майже половина усіх зареєстрованих злочинів, виявляються й розкриваються саме завдяки використанню ав-

томатизованих інформаційних обліків МВС України. Ми вважаємо, що введення до навчальних програм вищих навчальних закладів системи МВС України предмету, присвяченого навчанню користування та вивченню можливостей сучасних автоматизованих інформаційних обліків та систем, є нагальною необхідністю для підвищення якості підготовки фахівців для ОВС України. Крім того, здебільшого погоджуючись з Гуславським В. С., Задорожним Ю. А., Розовським В. Г. та іншими вченими [10, с. 38 – 40], ми можемо зазначити основні пріоритети розвитку систем інформаційного забезпечення органів внутрішніх справ, зокрема:

1) реорганізація видання та удосконалення законодавчої і нормативно-правової бази, яка регламентує створення та використання інформаційних систем та підсистем;

2) створення єдиного інформаційного простору в загальній системі МВС України та організація і удосконалення динамічної взаємодії із зарубіжними інформаційними системами;

3) широке використання технологій об'єктна орієнтованого проектування та програмування, при розробці нових інформаційних підсистем, та модернізація існуючих;

4) стимулювання активного формування та використання інформаційних ресурсів;

5) поєднання принципів швидкості та зручності доступу до інформаційних ресурсів, та принципів повного захисту від несанкціонованого доступу;

6) запровадження сучасних новітніх інформаційних технологій, інформаційно-технічне переоснащення підрозділів, забез-
печення підрозділів ліцензійним програмним забезпеченням;

7) технічна підготовка, перепідготовка та підвищення кваліфікації особового складу усіх підрозділів з метою підвищення ефективності використання можливостей сучасних новітніх інформаційних систем та підсистем в службах і підрозділах органів внутрішніх справ України.

Питання для самоперевірки та контролю засвоєння знань:

1. Яким є призначення та основні завдання щодо використання автоматизованих інформаційно-пошукових систем та інформаційно-аналітичного забезпечення працівників ОВС України?

2. Назвіть основні інформаційно-пошукові системи МВС України які можуть бути використані при проведенні слідчих (розшукових) дій, негласних слідчих (розшукових) дій, при проведенні оперативно-розшукових заходів ?

3. Які пріоритети розвитку систем інформаційного забезпечення органів внутрішніх справ можливо виділити у сучасному стані ?

4. Яке практичне значення має використання автоматизованих інформаційно-пошукових систем МВС України для проведення слідчих (розшукових) та негласних слідчих (розшукових) дій ?

Список рекомендованої літератури:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

2. Кримінальний кодекс України. Кримінальний процесуальний кодекс України. – К.: Юрінком Інтер, 2012. – 608 с.

3. Гуславский В. С., Задорожний Ю.А., Розовский В. Г. Информационно-аналитическое обеспечение раскрытия и расследования преступления // Монография – Луганск, ТОВ «Елтон-2», 2008. – 133 с.

4. Цехан Д.М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ // Монографія / Д.М. Цехан ; за науковою редакцією О. О. Подобного. – Одеса : Юридична література, 2011. – 216 с.

2.2 ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ СОЦІАЛЬНИХ МЕРЕЖ ІНТЕРНЕТУ ДЛЯ УДОСКОНАЛЕННЯ АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНО-ПОШУКОВИХ СИСТЕМ МВС УКРАЇНИ

Починаючи з 2004 року широкого розповсюдження набули такі Інтернет – ресурси, як соціальні мережі. Кожен день сотні мільйонів людей спілкуються, знайомляться, обмінюються фотографіями та відеозаписами, і навіть займаються комерційною діяльністю через різноманітні соціальні мережі, що нерідко залишається поза контролем податкової адміністрації та інших правоохоронних органів. Взірцем сучасних соціальних мереж звичайного вигляду у світі є соціальна мережа, розроблена у 2004 року в США Марком Цукербергом, яка має відому та впізнаваєму назву «Facebook» [11]. Сам Марк Цукерберг за створення цієї соціальної мережі, у 2010 році був визнаний Американським журналом «Times» людиною року, та став за її використання наймолодшим мільярдером. На пострадянському просторі, найвідомішими та поширеними у користуванні, навіть серед недостатньо обізнаних осіб щодо повних технічних можливостей мережі Інтернет, соціальними мережами є «Одноклассники» [12] та «Вконтакте» [13]. Обидві соціальні мережі, як «Одноклассники», так і «Вконтакте», на даний момент по своїм функціональним можливостям та структурі істотно відрізняються від соціальної мережі США «Facebook». Однак якщо порівняти сучасний вигляд та структуру соціальної мережі «Вконтакте» з первинним виглядом та структурою соціальної мережі «Facebook», то великих розбіжностей ми не побачимо. Але соціальна мережа «Facebook» була створена раніше за «Вконтакте». Головний принцип, на якому ґрунтуються та використовуються майже усі існуючи соціальні мережі це добровільне створення користувачами своїх профілів та добровільне заповнення цих профілів інформацією про свою особистість. Зокрема, це інформація про особу користувача: місце, дату, місяць та рік його

народження, місце проживання, навчальні заклади, в яких навчався чи навчається користувач, відомості про його родичів, відомості про соціальний та сімейний стан; вподобання користувача, зокрема: улюблені книги, кінофільми, пісні, цитати відомих людей та інше; контактні дані користувача: номера телефонів, адрес електронної пошти, ім'я користувача в сервісі Skype, номер сервісу ICQ, адрес персонального Інтернет – сайту; особисті графічні та аудіо матеріали: фотографії та відеозаписи, на яких є сам користувач, або його родичі чи знайомі, цифрові зображення картин чи інші цифрові зображення, аудіо композиції, відео кліпи та відео ролики, котрі відображають, у тому числі естетичні або незвичайні смаки користувача. Всі ці дані користувачі соціальних мереж розміщують у своїх профілях добровільно, а не малозначним є те, що чим більше інформації про себе користувач розмістить в своєму профілі соціальної мережі, тим більший соціальний статус своєму профілю користувач здобуде за рахунок спілкування в мережі Інтернет. Тобто соціальні мережі стимулюють розміщення користувачами їх особистої інформації всередині самих соціальних мереж. Велика кількість людей, які мають створені в соціальних мережах профілі, тим самим відкривають для працівників ОВС вільний шлях для отримання інформації про певну особу.

Для кращої демонстрації широких можливостей, які надають працівникам досудового розслідування при проведенні слідчих (розшукових) дій, негласних слідчих (розшукових) дій, а також оперативно-розшукових заходів підрозділами ОВС та правоохоронних органів є соціальні мережі. Авторами даного навчального посібника проведено анкетування користувачів соціальної мережі «Вконтакте». Було проведено опитування 140 респондентів віком від 16 до 35 років, за результатами чого було отримано такі результати [додаток А]:

1) 70 % опитаних відвідують свою сторінку соціальної мережі «Вконтакті» щодня;

2) 80 % опитаних відкрили доступ до перегляду даних зі своєї сторінки соціальної мережі «Вконтакті» усім бажаючим;

3) 60 % опитаних використовують свою сторінку соціальної мережі «Вконтакті» для підтримання зв'язків з друзями;

4) 74 % опитаних розміщують на своїй сторінці соціальної мережі «Вконтакті» особисті дані, які повністю відповідають дійсності;

5) 70 % опитаних добавляють людей у список своїх друзів на своїй сторінці соціальної мережі «Вконтакті», спираючись на знайомство, чи на близькі дружні відносини з ними;

6) Лише 30 % опитаних не обмінюються і не планують обмінюватись на своїй сторінці соціальної мережі «Вконтакті» інформацією про вчинення протиправних діянь, шляхом використання повідомлень, хоча останні 70% таку можливість не виключають при спілкуванні через Інтернет.

Виходячи із наведених даних, необхідно наголосити, що використовуючи фотографії користувачів, які вони розміщують у своїх профілях соціальних мереж, таких як наприклад «Facebook та «Вконтакте», можливо дуже швидко та суттєво розширити та поповнити бази даних автоматизованих біометричних та інших систем, якими користуються працівники МВС України відносно осіб що готують, вчиняють замах або вже вчинили кримінальне правопорушення чи ухиляються від досудового розслідування і суду. А це, в свою чергу, надасть і розширить працівникам правоохоронних органів наступні можливості:

1) маючи фотографію чи фоторобот правопорушника – швидко ідентифікувати його особу у тому випадку, якщо його фотографії є в базі даних автоматизованої біометричної чи іншої системи;

2) використати фотографії із списку «друзів» в сторінці соціальної мережі правопорушника з метою пред'явлення їх для впізнання потерпілому, або свідкам кримінального правопорушення, а також для впізнання самого потерпілого в разі його вбивства чи смерті;

3) наявність в базах даних автоматизованих біометричних систем багатьох фотографій однієї особи, але знятих з різних кутів та ракурсів дозволить ідентифікувати особу краще, якісніше й

ефективніше, ніж використати звичайні обліки фотографій МВС, що зменшить чи унеможливить судову помилку;

4) під час проведення оперативно-розшукового заходу дозволить більш повно та швидко встановити коло контактів і зв'язків особи;

5) вказаний перелік не обмежує й інші можливості.

Питання для самоперевірки та контролю засвоєння знань:

1. Які соціальні мережі в Інтернеті є найбільш розповсюдженими й популярними?

2. В яких видах соціальних мереж Інтернету можна отримати додаткову інформацію що буде мати тактичний, оперативний чи інший службовий інтерес при проведенні слідчих (розшукових) дій чи негласних слідчих (розшукових) дій ?

3. Інформацію якого характеру можливо отримати про особу, яка представляє тактичний чи оперативний інтерес, або слугуватиме меті кримінального провадження, а також мати значення для працівників ОВС в соціальних мережах Інтернету?

Список рекомендованої літератури:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

2. Цехан Д.М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ // Монографія / Д.М. Цехан ; за науковою редакцією О.О. Подобного. – Одеса : Юридична література, 2011. 216 с.

3. І.О. Борозенний, О. О. Юхно Особливості використання мережі Інтернет та автоматизованих інформаційно-пошукових систем для забезпечення проведення негласних слідчих (розшукових) дій // Право і Безпека : науковий журнал, № 4 (46) за 2012 рік, - Харківський національний університет внутрішніх справ : видавництво ХНУВС, 2012. – 360 с.

РОЗДІЛ 3.
ПОШУК В МЕРЕЖІ ІНТЕРНЕТ ІНФОРМАЦІЇ ПРО ОСІБ ЯКІ МОЖУТЬ ПРЕДСТАВЛЯТИ ОПЕРАТИВНИЙ ІНТЕРЕС ДЛЯ ПРАЦІВНИКІВ ОВС

3.1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ПОШУКОВИХ СЕРВІСІВ ДЛЯ ВИКОРИСТАННЯ ПРИ ПРОВЕДЕННІ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

Майже вся аудіо, відео та текстова інформація, яка знаходиться на сторінках сайтів в мережі Інтернет, а так само і імена конкретних Інтернет сайтів розшукується його користувачами шляхом формування відповідних пошукових запитів в спеціальних пошукових сервісах. За своєю внутрішньою будовою пошукові сервіси можливо поділити на такі складові частини: відкриту для користувача, та закриту від користувача. В свою чергу, відкриту для користувача частину, умовно можливо поділити на такі зокрема складові частини:

1) одне чи декілька доменних імен Інтернет сайту, через які здійснюється доступ до самого пошукового сервісу;

2) графічна оболонка пошукового сервісу;

3) інструменти для формування пошукових запитів та роботи з ними;

4) блок відображення результатів пошуку інформації за сформованими пошуковими запитами;

В свою чергу закриту від користувача частину можливо, умовно можливо поділити на такі складові частини:

1) пошуковий індекс – перелік доменних імен Інтернет сайтів та конкретної інформації, яка розміщена в мережі Інтернет, що може вивести пошуковий сервіс в блоці відображення результатів пошуку інформації за сформованими пошуковими запитами;

2) пошукові роботи це спеціальні програми, які сканують інформаційний простір мережі Інтернет, та відносять, чи

виключають ту чи іншу інформацію до бази даних пошукового сервісу;

3) внутрішні правила, за якими пошукові роботи відносять ту чи іншу інформацію до пошукового індексу пошукової системи;

4) база даних, в якій зберігається аудіо, відео та текстова інформація, яку було включено до пошукового індексу пошукового сервісу.

Необхідно зазначити, що різні пошукові сервіси використовують різні внутрішні правила та різних пошукових роботів, із-за чого їх пошукові індекси та бази даних можуть суттєво відрізнятись одна від одної. Саме тому під час пошуку інформації, що представляє тактичний чи оперативний інтерес, необхідно користуватись різними пошуковими сервісами. Нижче приведено перелік із шести пошукових сервісів, відображення результатів пошуку в яких відрізняється один від одного, та що розміщено в тому порядку, в якому доцільно їх використовувати при пошуку інформації, яка представляє оперативний інтерес.

«Google Inc.» [15] — американська публічна транснаціональна корпорація, заснована 27 вересня 1998 року як приватна компанія, що займається розробкою, розвитком і дизайном найпопулярнішого в Інтернеті пошукового сервісу. Google підтримує і розробляє низку інтернет-сервісів і продукції, отримуючи дохід передусім від реклами, завдяки своїй програмі AdWords. Google і керує понад мільйоном серверів у центрах опрацювання даних (ЦОД) у всьому світі, опрацьовуючи більше мільярда пошукових запитів і 24 петабайт користувацьких даних щодня. Швидкий ріст Google з моменту його заснування призвів до виникнення великої кількості продукції, незв'язаної безпосередньо з головним продуктом компанії — пошуковою системою. Google має такі онлайн-продукти як поштовий сервіс Gmail, соціальні інструменти Google+ та Google Buzz. У компанії є також і десктопні продукти, такі як браузер Google Chrome, програма для роботи з фото Picasa і програма обміну миттєвими повідомленнями Google Talk. Крім того Google

веде розробку мобільної операційної системи Android, якою користується велика кількість володільців смартфонів, а також ця компанія володіє операційною системою Google Chrome OS, яку вже тепер можна скачати на офіційному сайті Google. За версією BrandZ, Google це найсильніший, а за версією компанії Brand-Finance в свою чергу найдорожчий бренд у світі 2012 року. За 2012 рік Google було визнано компанією з найкращою репутацією в США. Інтерфейс Google містить досить складну мову запитів, що дозволяє обмежити галузь пошуку окремими доменами, мовами, типами файлів тощо. Наприклад, пошук «intitle:Google site: wikipedia.org» видасть всі статті Вікіпедії всіма мовами, в заголовку яких зустрічається слово «Google». Крім того, потужна мова запитів в руках хакерів може бути використана для дослідження Інтернет сайтів на вразливість.

«Яндекс» [16] — російська IT-компанія, що володіє однойменною системою пошуку в Інтернеті та інтернет-порталом. Пошукова система «Яндекс» є четвертою серед пошукових систем світу за кількістю оброблених пошукових запитів (4840 млн, 2,8% від світової кількості, згідно статистики за грудень 2012 року). Станом на 8 лютого 2013 року, згідно з рейтингом Alexa.com, за популярністю сайт yandex.ru займає 20-е місце в світі і 1-ше місце в Росії. Пошукова система Yandex.ru була офіційно анонсована 23 вересня 1997 року, і перший час розвивалася в рамках компанії CompTek International. Як окрема компанія «Яндекс» утворилась в 2000 році. У травні 2011 року компанія «Яндекс» провела первинне розміщення акцій, заробивши на цьому більше, ніж будь-яка з Інтернет-компаній із часів IPO пошуковика Google в 2004 році. Основним і пріоритетним напрямом компанії є розробка пошукового механізму, але за роки роботи «Яндекс» став мультіпорталом. У 2011 році «Яндекс» надає більше 30 сервісів. Найпопулярнішими є: Яндекс. Зображення, Яндекс.Пошта, Яндекс.Карти, Яндекс.Новини, Яндекс.Погода та інші. Пошук в Яндексі здійснється в тому числі серед зображень, відео, у блогах, в оголошеннях про продаж автомобілів тощо. Відмінністю Яндекса можна вважати алгоритм його пошуку — він сконструйований

на морфологічній системі російської мови. Крім стандартних файлів HTML шукає також у файлах формату PDF (Adobe Acrobat), RTF (Rich Text Format), DOC (Microsoft Word), XLS (Microsoft Excel), PPT (Microsoft Power Point), SWF (Macromedia Flash), а також індексує формат RSS.

«МЕТА» [17] — український пошуковий портал в мережі Інтернет. Використовує пошукову систему власної розробки з українською, російською та англійською мовами пошуку. Зона пошуку це українські сайти та сайти, що стосуються України. 12 листопада 1998 року в Харкові відбулося офіційне відкриття пошукової системи МЕТА. Сервер, наданий Харківським державним політехнічним університетом, був розташований на технічному майданчику провайдера «Харків-Онлайн». З моменту старту популярність сервера зростала, і вже через півтора року каналу Харків-Київ стало не вистачати. У травні 2000 року було ухвалено рішення про розміщення сервера в Києві. Відразу після переїзду відвідуваність пошукової системи зросла в 2 рази, з'явилися перші доходи від реклами. У вересні 2000 року було зареєстровано ТОВ «МЕТА», подана заявка на торговий знак і МЕТА стала комерційним підприємством. Належність сайтів до українського сегменту мережі визначається так: сайти в домені UA та піддоменах (com.ua, kiev.ua тощо); українська мова сайту; хостинг на IP українських провайдерів; основна тематика сайту (будь-якою мовою) стосується України. Внаслідок певних технічних складнощів з визначенням належності сайту до України, у випадках 3-4, тобто коли сайт знаходиться в доменах першого рівня (.com, .net, org тощо) і використовує не українську мову, бажано при його використанні доцільно додавати сайт до пошуку в ручному режимі.

«Rambler Media Group» [18] це диверсифікована російськомовна медіа і сервіс-група. Заснована в 2004 році і створена на основі однойменної пошукової системи, що працює в Росії з 1996 року. Зареєстрована на острові Джерсі (Великобританія). Станом на початок 2009 року[1] основним її акціонером є вхідна в холдинг «Проф-медіа» компанія PM Invest Company Ltd., що володіє 54,5% акцій Rambler Media. До складу цієї рупи

входять такі Інтернет-ресурси, як російськомовний Інтернет-портал і пошукова машина Rambler.ru, online-газета Lenta.ru, спеціалізовані web-ресурси Doktor.ru, Mama.ru та інші, сайт порівняння товарів Price.ru, рейтинг-класифікатор Rambler Top 100, система обміну швидкими повідомленнями Rambler-ICQ, інтерактивна рекламна група Index 20. За повідомленнями преси, Rambler займає четверте місце в пошукових системах Росії, поступаючись тільки Яндексу, Google та Mail.ru.

«Yahoo!» [19] — американська компанія, яка володіє другою за популярністю (7.57%) в світі пошуковою системою (при цьому в США і Канаді відповідно до угоди з Майкрософт від 2009 року і станом на 2012 рік пошук на сайті Yahoo! здійснюється пошуковою машиною Bing) і надає низку сервісів, об'єднаних Інтернет-порталом Yahoo! Directory. Компанія Yahoo! була заснована у січні 1994 року студентами магістратури Стенфордського університету Девідом Файло (англ. David Filo) і Джеррі Янгом (англ. Jerry Yang), а 2 березня 1995 року стала корпорацією Портал Yahoo! яка включає в себе популярний сервіс електронної пошти Yahoo! Mail, який є одним з найстаріших і найбільш популярних в Інтернеті. У 2004 році була запущена нова версія поштового інтерфейсу, заснована на AJAX. Головний офіс компанії знаходиться в місті Саннівейл (англ. Sunnyvale), штат Каліфорнія, США. Згідно зі статистикою Alexa Internet, в лютому-квітні 2012 р. Yahoo! стала четвертою за відвідуваністю Інтернет сайт в мережі Інтернет, і приблизно 28% відвідувань якої складаються з питань перегляду тільки однієї сторінки.

«Bing» [20] це пошукова система, розроблена міжнародною корпорацією Microsoft. Bing був представлений генеральним директором Microsoft Стівом Балмером. Доступна за адресою http://www.bing.com/. Раніше мала наступні найменування та адреси:

1) MSN Search (http://search.msn.com/) - з моменту появи в 1998 році і до 11 вересня 2006 року;

2) Windows Live Search (http://search.live.com/) - до 21 березня 2007;

3) Live Search (http://www.live.com/) - до 1 червня 2009 року.

Крім того, з жовтня 2006 року по січень 2009 року діяв сайт Ms. Dewey (www.msdewey.com), а з серпня 2007 до 30 червня 2009 року відповідно Tafiti (tafiti.com), що засновані на тих же технологіях Live Search, але що вони мали інший, експериментальний інтерфейс. В даний час сайт Bing займає 5-е місце в списку найбільш популярних пошукових сайтів за обсягом трафіку, на відміну від яких володіє рядом ексклюзивних технічних можливостей, зокрема таких як перегляд результатів пошуку на одній сторінці (замість гортання численних сторінок результатів пошуку), а також динамічне корегування обсягу інформації, яка відображається для кожного результату пошуку (наприклад, тільки назва, коротке або велике зведення).

Питання для самоперевірки та контролю засвоєння знань:

1. Які пошукові системи в мережі Інтернет є найбільш популярними на території країн СНД ?

2. Які пошукові системи в мережі Інтернет є розробниками та власниками російських та українських компаній ?

3. Які на Вашу думку найбільш ефективними можуть бути для використання при проведенні негласних слідчих (розшукових) дій пошукові системи в мережі Інтернет ?

4. Які функції та можливості надають пошукові системи користувачам мережі Інтернет для використання у правозастосовній діяльності ?

Список рекомендованої літератури:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

2. Кримінальний кодекс України. Кримінальний процесуальний кодекс України. – К.: Юрінком Інтер, 2012. – 608 с.

3. Цехан Д.М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ // Монографія / Д.М. Цехан ; за науковою редакцією О.О. Подобного. – Одеса : Юридична література, 2011. – 216 с.

3.2 ВИКОРИСТАННЯ ПОШУКОВИХ ОПЕРАТОРІВ У ПОШУКОВИХ СЕРВІСАХ ДЛЯ ВИРІШЕННЯ ЗАВДАНЬ ПРОТИДІЇ ЗЛОЧИННОСТІ

Майже всі сучасні пошукові сервіси мають потужні пошукові оператори, які дозволяють найбільш точно формулювати запит до пошукового сервісу, враховуючи найменші нюанси поведінки її пошукових механізмів. Найбільш популярні критерії пошуку можна задавати з допомогою розширеного пошуку, але володіння пошуковими операторами надає можливість вирішувати складні пошукові задачі.

Нижче будуть розглянуті основні пошукові оператори, які майже не відрізняються у більшості пошукових сервісах. Детальніше про специфіку використання пошукових операторів пошукової системи «Google» ви можете знайти на сторінках такого Інтернет – ресурсу, як пошуковий оператор «Google» [Електронний ресурс]. – Режим доступу: http://www.googleguide.com/ advanced_ operators.html або «Google» [Електронний ресурс]. – Режим доступу: http://www.diacr.ru/zametki/20-kak-pravilno-iskat-v-google/ kak-pravilno-iskat-v-google.htm. Про специфіку використання пошукових операторів пошукової системи «Яндекс» можна знайти на сторінках такого Інтернет – ресурсу, як «Яндекс» [Електронний ресурс]. – Режим доступу: http://help.yandex.ru/search чи «Яндекс» [Електронний ресурс]. – Режим доступу: http://help.yandex.ru/search/?id=481920.

Оператор	**Призначення**	**Приклад**
1	2	3
	пробіл – логічне «AND» або «ТАКОЖ», дає команду для пошукового сервісу на пошук усіх слів, розділених пробілом	хочеш миру готуйся до війни

OR	логічне «ЧИ» дозволяє знайти декілька варіантів слів чи словосполучень	хочеш миру OR бажаєш миру
|	логічне «ЧИ» дозволяє знайти декілька варіантів слів чи словосполучень	хочеш миру | бажаєш миру
1	2	3
«»	двійні лапки дозволяють знайти тільки те словосполучення, яке зазначено в них, виключаючи інші варіанти, чи інші слова між зазначеними у словосполученні	«хочеш миру готуйся до війни»
~	символ «~» дає команду для пошукового сервісу на пошук не тільки зазначеного слова, але і його синонімів	~хочеш ~миру ~готуйся ~до ~війни
*	символ «МНОЖЕННЯ» заміняє одне слово, але можливо вказати скільки саме слів може бути між тими, що шукаються	хочеш * * * війни
+	символ «ПЛЮС» дає команду для пошукового сервісу для обов'язкового пошуку слова, перед яким він стоїть	хочеш миру готуйся +до +війни
–	символ «МІНУС» дає команду для пошукового сервісу для обов'язкового виключення з пошуку слова, перед яким він стоїть	хочеш миру війни –хтиш – бачиш

site:	обмежує пошук слів, які стоять перед оператором, тим доменним іменем чи сайтом, який стоїть після оператору	хочеш миру готуйся до війни site:war.com.ua

Питання для самоперевірки та контролю засвоєння знань:

1. Для чого призначені пошукові оператори у пошукових сервісах мережі Інтернет?

2. Які можливості надає використання пошукових операторів у пошукових сервісах мережі Інтернет при проведенні пошуку інформації про особу, яка представляє оперативний інтерес для працівників ОВС ?

3. Наведіть приклади використання пошукових операторів у пошукових сервісах мережі Інтернет при проведенні пошуку інформації про особу, яка представляє оперативний інтерес або при проведенні негласних слідчих (розшукових) дій ?

Список рекомендованої літератури:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

2. Кримінальний кодекс України. Кримінальний процесуальний кодекс України. – К.: Юрінком Інтер, 2012. – 608 с.

3. І. О. Борозенний, О. О. Юхно Особливості використання мережі Інтернет та автоматизованих інформаційно-пошукових систем для забезпечення проведення негласних слідчих (розшукових) дій // Право і Безпека, № 4 (46), 2012 рік, - Харківський національний університет внутрішніх справ : видавництво ХНУВС, 2012. – 360 с.

4. Как надо использовать язык поисковых запросов «Google» [Електронний ресурс]. – Режим доступу: http://www.diacr.ru/zametki/20-kak-pravilno-iskat-v-google/kak-pravilno-iskat-v-google.htm

5. Расширенные возможности поиска в «Яндекс» [Електронний ресурс]. – Режим доступу: http://help.yandex.ru/search/?id=481920

3.3 ПОШУК ІНФОРМАЦІЇ ЯКА ПРЕДСТАВЛЯЄ ТАКТИЧНИЙ ЧИ ОПЕРАТИВНИЙ ІНТЕРЕС З ВИКОРИСТАННЯМ МОЖЛИВОСТЕЙ ПРОТОКОЛУ ПЕРЕДАЧІ ДАННИХ – FILE TRANSFER PROTOCOL (FTP)

«Всесвітня мережа», або «World Wide Web» (скорочено: WWW; також: всемережжя, ВЕБ або тенета) це найбільше всесвітнє багатомовне сховище інформації в електронному вигляді, тобто десятки мільйонів пов'язаних між собою документів, що розташовані на комп'ютерах розміщених на всій земній кулі. Найбільше, та не єдине. А тому інформація, що представляє тактичний чи оперативний інтерес може бути розміщена також і на FTP серверах і може передаватись за допомогою протоколу передачі даних (англійською мовою – File Transfer Protocol), або FTP.

Протокол передачі файлів (FTP) дає можливість абоненту обмінюватися двійковими і текстовими файлами з будь-яким комп'ютером мережі, що підтримує протокол FTP. Установивши зв'язок з віддаленим комп'ютером, користувач може скопіювати файл з віддаленого комп'ютера на свій, або скопіювати файл з свого комп'ютера на віддалений.

При розгляді FTP як сервісу Інтернет мають на увазі не просто протокол, а саме сервіс доступ до файлів, які знаходяться у файлових архівах. FTP це стандартна програма, яка працює за протоколом TCP, яка завжди поставляється з операційною системою. Її початкове призначення це передача файлів між різними комп'ютерами, що працюють у мережах TCP/IP, зокрема: на одному з комп'ютерів працює програма-сервер, на іншому програма-клієнт, що запущена користувачем і з'єднується з сервером та передає або отримує файли через FTP-сервіс. Все це розглядається з припущенням, що користувач зареєстрований на сервері та використовує логін і пароль на цьому комп'ютері.

Такі технічні характеристики стали причиною того, що програми FTP стали частиною окремого сервісу Інтернету. Справа

в тому, що доволі часто сервер FTP налаштовується таким чином, що з'єднатися з ним можна не тільки під своїм ім'ям, але й під умовним іменем, наприклад, anonymous (анонім). У такому випадку для користувача стає доступною не вся файлова система комп'ютера, а лише деякий набір файлів на сервері, що складають вміст серверу anonymous FTP, тобто публічного файлового архіву. Отже, якщо користувач хоче надати у вільне користування файли з інформацією, програмами і таке інше, то йому достатньо організувати на власному комп'ютері, включеному в Інтернет, сервер anonymous FTP. Створення такого серверу це процес доволі простий, програми-клієнти FTP вельми розповсюджені, а тому сьогодні публічні файлові архіви організовані в основному як сервери anonymous FTP. Перелік інформації, яка міститься на таких серверах, включає всі аспекти життя: від звичайних текстів до мультимедіа.

FTP-Server – це серверне програмне забезпечення, яке знаходиться у тієї людини у якої є необхідність скачати відповідну інформацію і за допомогою цього забезпечення здійснюються доступними файли для завантаження по даному протоколу. Наприклад: Cesar FTP Server, Titan FTP Server, ftpd, Serv-U Ftp, XLight Ftp Server.

FTP-Client – це клієнтська програма за допомогою якої є технічна можливість доступитися до якогось FTP-сервера. Наприклад вбудований в операційну систему Windows ftp.exe, Windows Explorer, FTP Voyager, Far manager, Total Commander, Download Master.

Якщо в наявності є спеціальні пошукові сервіси, такі як «Google» [15] та «Яндекс» [16], призначення яких, здебільшого призначено для пошуку інформації у просторі «Всесвітньої мережі» (або «World Wide Web», чи «WWW»), то є також і спеціальні сервіси пошуку інформації на серверах FTP. У країнах СНД, найбільш зручні та функціональні із них це «FileSearch» [25], та «МАМОНТ» [26].

Ці пошукові сервіси, призначені для пошуку файлів на FTP-серверах, які доцільно використовувати тоді, коли працівнику

відомо, що особою, яка представляє тактичний чи оперативний інтерес, було розміщено інформацію у мережі Інтернет (наприклад, на сторінках Інтернет – сайту, що має електронну адресу виду http://www.sample.ua) певний електронний документ, чи файл). Наприклад, нею може бути файл, створений офісними, чи текстовими програмами – *.doc, *.xls, *.ppt, *.pdf, *.fb2, *.txt та інші. Також, це можуть бути мультимедіа файли: *.avi, *.wmv, *.vob, *.mp4, *.mpeg, *.mkv, *.flv, *.mp3, *.wav, *.wma, *.ogg та інші. Крім цього це можуть бути фотографії, чи графічні зображення – *.bmp, *.png, *.jpg, *.jpeg, *.gif, *.pcx, *.tif, *.tga, *.iff, *.psd та інші.

Наприклад, особою, яка має псевдонім «Stanton», та яка підозрюється у розміщенні в мережі Інтернет закликів до дій ксенофобного, чи расистського характеру, на сторінках Інтернет – сайту «http://www.sample.ua» було розміщено текстовий файл під назвою «як_вбити_негра.txt». В такому випадку слід шукати інформацію про дану особу, використовуючи можливості сервісу та серверів FTP наступним чином:

1) необхідно відкрити спеціальний сервіс пошуку інформації на FTP-серверах. В даному випадку скористаємось таким сервісом, як «МАМОНТ» [26]. Для цього необхідно набрати в адресній строчці WEB – браузера, яким ви користуєтесь, адрес «http://mmnt.ru», та натиснути клавішу «ENTER»;

2) у поле вводу пошукового запиту сервісу «МАМОНТ» необхідно ввести ім’я файлу, який треба знайти на FTP-сервері. В даному випадку – це ім’я файлу «як_вбити_негра.txt»;

3) трохи нижче поля вводу пошукового запиту сервісу «МАМОНТ», необхідно вибрати режим «Глобальный поиск файлов (ftp://)», натиснувши на відповідну кнопку;

4) після виконання дій, зазначених вище – необхідно натиснути клавішу «ENTER», чи натиснути на кнопку «НАЙТИ», яка розташована правіше від поля вводу пошукового запиту сервісу «МАМОНТ»;

5) після цього, сервіс пошуку інформації на FTP-серверах «МАМОНТ» [26] сформує блок відображення результатів пошуку інформації за сформованими пошуковими запитами,

якщо буде знайдено якусь інформацію, чи проінформує, що у базах даних сервісу «МАМОНТ» нічого не було знайдено;

6) далі, необхідно перевірити FTP-сервери, на яких було знайдено файли зі схожою, чи ідентичною назвою. Для цього необхідно скопіювати адрес FTP-сервера, який було відображено у блоці результатів пошуку інформації за сформованими пошуковими запитами сервісу «МАМОНТ». Наприклад – це такий адрес: «ftp://83.166.96.170/ALL/Книги/mybooks/як_вбити_негра.txt»;

7) для роботи з файлами, які знаходяться на FTP-серверах ми рекомендуємо користуватись файловими менеджерами, таким як «Total Commander» чи «FAR», або такою програмою для операційної системи Windows, як «Download Master» [27]. Після запуску програми «Download Master», необхідно натиснути клавішу «F7», чи перейти в пункт меню «Инструменты», та вибрати поле «FTP Explorer»;

8) у програмі «FTP Explorer», яка відкрилась, у адресну строку необхідно ввести адрес FTP-сервера, який ми отримали через сервіс пошуку інформації на FTP-серверах «МАМОНТ», та який було скопійовано – «ftp://83.166.96.170/ALL/Книги/mybooks/як_вбити_негра.txt». Після цього необхідно натиснути клавішу «ENTER»;

9) після цього у програмі «FTP Explorer» повинна відобразитись будова директорій (папок) та файлової системи на FTP-сервері, адрес якого було введено. Крім того буде відображено саме ту директорію (папку), де знаходиться файл, який необхідно було знайти. Тому доцільно вивчити склад даної директорії (папки), та при сприятливих умовах (якщо доступ до фалів FTP-серверу не захищений паролем), завантажити усі файли, які знаходяться в ній;

10) проаналізувати інформацію, яка знаходиться у завантажений файлах, на предмет знаходження в ній даних про особу, яка становить тактичний чи оперативний інтерес. При необхідності – завантажити файли з інших директорій (папок), які також знаходяться на даному FTP-сервері;

11) проаналізувати та перевірити і інші FTP-сервери, адреси яких було відображено у блоці результатів пошуку інформації за сформованими пошуковими запитами сервісу «МАМОНТ».

Питання для самоперевірки та контролю засвоєння знань:

1. Яке призначення та можливості має протокол передачі файлів FTP?

2. Чи можливо використовувати протокол передачі файлів FTP в мережі Інтернет при проведенні пошуку інформації про особу, яка представляє оперативний інтерес для працівників ОВС

3. Яке практичне значення мають можливості використання протоколу передачі файлів FTP ?

Список рекомендованої літератури:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

2. Кримінальний кодекс України. Кримінальний процесуальний кодекс України. – К.: Юрінком Інтер, 2012. – 608 с.

3. Таненбаум Э. Архитектура компьютера. 5-е изд. (+CD). — СПб.: Питер, 2007. — 844 с: ил.

4. Цехан Д.М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ // Монографія / Д.М. Цехан ; за науковою редакцією О.О. Подобного. – Одеса : Юридична література, 2011. – 216 с.

5. І. О. Борозенний, О. О. Юхно Особливості використання мережі Інтернет та автоматизованих інформаційно-пошукових систем для забезпечення проведення негласних слідчих (розшукових) дій // Право і Безпека : науковий журнал, № 4 (46) за 2012 рік, - Харківський національний університет внутрішніх справ : видавництво ХНУВС, 2012. – 360 с.

3.4 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ТА МЕТОДИКА ПОШУКУ ЦИФРОВИХ ЗОБРАЖЕНЬ В МЕРЕЖІ ІНТЕРНЕТ

Як вже зазначалось вище, велику групу злочинів складають шахрайства, вчинені з використанням сучасних інформаційних технологій та мережі Інтернет. Такі шахрайства, вчиняються з використанням мережі Інтернет в якості засобу спілкування і входження в довіру до потерпілої особи, що відрізняє від входження в довіру до особи при вчиненні звичайного шахрайства без використання мережі Інтернет. Інші види шахрайств вчиняються із використанням Інтернет – аукціонів, в яких непомітно для покупця самі продавці роблять ставки, штучно створюючи уяву про участь багатьох покупців у аукціоні, з метою підняти ціну виставленого на аукціон товару. В інших видах шахрайств, продавець виставляє на огляд в мережі Інтернет лише фотографії товару, а після отримання грошей пересилку товару покупцеві не здійснює.

Типовими є ситуації, коли шахраї створюють на сторінках Інтернет – аукціонів декількох користувачів, які мають різні особисті данні та імена профілів. Також шахраї можуть створювати декілька різних профілів у різних сервісах по продажу товарів через мережу Інтернет, чи по продажу товарів на сторінках Інтернет – аукціонів. За допомогою цих профілів, шахраї створюють сторінки по продажу товарів, але оскільки дуже часто реального товару на руках у шахраїв немає, вони використовують однакові графічні зображення, чи цифрові фотографії товару для створення оголошення. Крім того, як правило, шахраї використовують відносно одні й ті самі міні-зображення для своїх профілів – так звані «аватарки».

Працівникам ОВС вкрай необхідно мати у розпорядженні якомога більше інформації про ту, чи іншу особу, яка представляє оперативний інтерес. А тому пошук в мережі Інтернет усіх створених оголошень та профілів конкретної особи може принести працівникам ОВС багато значимої інформації. Наприклад: адреси електронної пошти, якою користується особа, номери телефонів, імена профілів в соціальних мережах, контакти особи. Це можливо тому, що при створенні нових

профілів на тих чи інших Інтернет сайтах особа, яка їх створює, залишає свої особисті та контактні данні.

Для реалізації принципу «більша кількість даних створює більшу кількість даних, знайдених з її допомогою», шляхом пошуку ідентичних зображень в мережі Інтернет, необхідно скористатися послугами, що представляють Інтернет сервіси трьох типів: звичайні пошукові сервіси, вбудовані доповнення у звичайні пошукові сервіси, та спеціальні сервіси по пошуку графічних зображень.

Використання пошукових сервісів для пошуку копій графічних зображень :

1) для пошуку копій графічних зображень через звичайний пошуковий сервіс, спочатку необхідно дізнатися ім'я зображення, копії якого необхідно знайти.

2) для цього по зображенню необхідно натиснути правою клавішою маніпулятору «миша», та у меню, що відкрилося необхідно вибрати поле меню «відкрити зображення» (open image), чи «показати зображення» (show image). Після цього, ім'я зображення буде передано до адресної строки WEB браузера, в якому ви відкрили дане зображення;

3) отримане ім'я необхідно ввести в поле пошукового запиту того пошукового сервісу, який необхідно використати;

4) далі необхідно проаналізувати результати пошукового запиту у вигляді текстових посилань на Інтернет сайті, на сторінках яких розміщено схоже графічне зображення, та якщо ця функція є у пошуковому сервісі – переглянути результати пошукових запитів лише у вигляді зображень. Наприклад: «Google Images» [28] чи «Яндекс Картинки» [29];

5) якщо необхідно знайти зображення з назвою «get_slimauto_service.jpg» – саме цю назву зображення і необхідно вводити у поле пошукового запиту пошукового сервісу.

Використання спеціальних сервісів для пошуку копій графічних зображень:

1) для пошуку копій графічних зображень через сервіс по пошуку графічних зображень, доцільно скористатись одним із двох сервісів: «TinEye Reverse Image Search» [30], чи «GazoPa similar image search» [31];

2) для цього необхідно натиснути правою клавішею маніпулятору «миша» по зображенню, копію якого необхідно знайти;

3) у меню, що відкрилося необхідно вибрати поле меню «відкрити зображення» (open image), а потім ще раз натиснути правою клавішею маніпулятору «миша» по зображенню, яке відкрилося, та вибрати поле меню «зберегти зображення» (save image);

4) далі необхідно перейти на сторінки Інтернет сайту того сервісу по пошуку графічних зображень, з допомогою якого буде здійснено пошук. Наприклад – це сервіс «TinEye Reverse Image Search» [30];

5) біля поля даного сервісу «Upload your image» розташована кнопка «View» («Пошук», чи «Обзор»), після натискання на яку буде запропоновано вибрати на комп'ютері користувача те зображення, копії якого необхідно знайти;

6) далі, сервісом по пошуку графічних зображень буде виконаний пошук копій вибраного користувачем зображення по своїм базам даних, після чого буде сформовано сторінку відображення результатів пошуку;

7) крім того, в наведеному сервісі «TinEye Reverse Image Search» [30], можливо не загружати зображення з комп'ютера користувача, а ввести лише його адресу в мережі Інтернет, заповнивши поле «Enter image adress», після чого також буде виконаний пошук копій вибраного користувачем зображення по базам даних сервісу.

Використання вбудованих доповнень у звичайні пошукові сервіси для пошуку копій графічних зображень:

1) для пошуку копій графічних зображень через вбудовані доповнення у звичайні пошукові сервіси, доцільно скористатись сервісом, яким надає компанія «Google Inc.» - «Google Images» [28];

2) для цього необхідно натиснути правою клавішею маніпулятору «миша» по зображенню, копію якого необхідно знайти;

3) у меню, що відкрилося необхідно вибрати поле меню «відкрити зображення» (open image), а потім ще раз натиснути правою клавішею маніпулятору «миша» по зображенню, яке відкрилося, та вибрати поле меню «зберегти зображення» (save image);

4) далі необхідно перейти на сторінки сервісу «Google Images» [28] – з його допомогою буде здійснено пошук копій графічних зображень;

5) праворуч від поля введення пошукового запиту даного сервісу, розміщено маленьке графічне зображення фотоапарату, після натискання на яке буде запропоновано вибрати на комп'ютері користувача те зображення, копії якого необхідно знайти;

6) далі, сервісом «Google Images» буде виконаний пошук копій вибраного користувачем зображення по своїм базам даних, після чого буде сформовано сторінку відображення результатів пошуку, та буде сформовано сторінку відображення результатів пошуку;

7) крім того, в наведеному сервісі «Google Images» [28], можливо не загружати зображення з комп'ютера користувача, а ввести лише його адресу в мережі Інтернет, чи його назву, якщо вона відома, заповнивши поле пошукового запиту, після чого також буде виконаний пошук копій вибраного користувачем зображення по базам даних сервісу, та буде сформовано сторінку відображення результатів пошуку.

Питання для самоперевірки та контролю засвоєння знань:

1. Які методики доцільно використовувати для пошуку графічних зображень та їх копій в мережі Інтернет?

2. Які завдання можливо вирішувати шляхом пошуку графічних зображень та їх копій в мережі Інтернет?

3. Яке практичне значення має пошук графічних зображень та їх копій в мережі Інтернет ?

Список рекомендованої літератури:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

2. Кримінальний кодекс України. Кримінальний процесуальний кодекс України. – К.: Юрінком Інтер, 2012. – 608 с.

3. Цехан Д.М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ // Монографія / Д.М. Цехан ; за науковою редакцією О.О. Подобного. – Одеса : Юридична література, 2011. – 216 с.

4. І. О. Борозенний, О. О. Юхно Особливості використання мережі Інтернет та автоматизованих інформаційно-пошукових систем для забезпечення проведення негласних слідчих (розшукових) дій // Право і Безпека : науковий журнал, № 4 (46) за 2012 рік, - Харківський національний університет внутрішніх справ : видавництво ХНУВС, 2012. – 360 с.

3.5 ОКРЕМІ АСПЕКТИ ПОШУКУ ІНФОРМАЦІЇ ПРО ОСОБУ ЯКА ПРЕДСТАВЛЯЄ ОПЕРАТИВНИЙ ІНТЕРЕС В СОЦІАЛЬНИХ МЕРЕЖАХ

Як вже зазначалось вище, певна кількість даних створює ще більшу кількість даних, знайдених за її допомогою. Тобто якщо про особу невідомо нічого, то без цього пошук є неможливим. У випадках коли про особу відома будь-яка інформація, наприклад, прізвище, ім'я та по-батькові, чи адреса електронної пошти, чи ім'я в сервісі Skype, чи номер ICQ, чи дата народження, чи навчальний заклад та рік, в якому дана особа закінчила навчання, або є інша інформація – це може надати можливість працівникам ОВС знайти ще більшу інформацію про дану особу, навіть використовуючи лише можливості соціальних мереж. Для цього необхідно ввести вказані данні про особу в пошукову систему, наприклад «Google» [15]. Переглядаючи отримані попередні пошукові результати, необхідно перевіряти й інші, і перш за все необхідно перейти на сторінки профілів даної особи в соціальних мережах, якщо такі є. Для цього доцільно буде послідовно ввести в пошукову систему прізвище, ім'я та по-батькові особи, та назву соціальної мережі, наприклад: «Іваненко Іван Іванович facebook», після перевірки результатів – «Іваненко Іван Іванович вконтакте», і так само далі працювати з іншими соціальними мережами. Якщо є відомості про особисті дані особи лише частково, в подальшому доцільно буде застосувати ще й інші три способи пошуку: через пошуковий сервіс, через фільтри соціальної мережі, та комбінований. Зупинимось на кожному із них.

Пошук інформації про особу в соціальній мережі, з використанням пошукового сервісу:

1) необхідно ввести в пошукову систему спочатку всю відому і наявну інформацію про особу та назву соціальної мережі. Наприклад: «Гадюченко Григор Григорович 11.11.1981 +380661235456 Харків Gadyuka@mail.ru Facebook»;

2) якщо це не принесло бажаних результатів, то в подальшому доцільно буде ввести по черзі частку інформації про особу, та назву соціальної мережі. Це пов'язано з тим, що особа, яка цікавить правоохоронців, може створювати в соціальних мережах профілі з іншими прізвищами та частково, або повністю зміненими особистими даними;

3) наприклад працівникам ОВС відомі дата народження та номер телефону особи, про яку необхідно отримати певну інформацію, отже для цього доцільно використати відомі дані, для чого необхідно ввести в пошуковій системі: «11.11.1981 +380661235456 одноклассники», потім «11.11.1981 одноклассники», потім «+380661235456 одноклассники», потім «11.11.1981 +380661235456 вконтакте», потім «11.11.1981 вконтакте», і так далі;

4) проаналізувати отримані результати.

Пошук інформації про особу в соціальній мережі, з використанням пошукових фільтрів самої соціальної мережі:

1) пошук може вестись всередині самих соціальних мереж, для чого необхідно зареєструватись в соціальній мережі, та створити власний профіль;

2) цей метод пошуку дуже доцільний завдяки тому, що у кожній соціальній мережі є функціональна система пошуку з багатьма фільтрами. Фільтри в соціальних мережах – це пошук інформації по відповідній умові, наприклад: по віку, по місцю народження, по вподобанням, по назві навчального закладу, тощо. В системах пошуку всередині соціальних мереж можна шукати особу тільки по прізвищу, чи по віку, чи по даті народження, чи по місту народження, чи по ставленню, наприклад до вживання спиртних напоїв. Список фільтрів пошуку, які можна використати при пошуку певної особи є дуже великий та різноманітний.

Комбінований пошук інформації про особу в соціальній мережі, з використанням пошукового сервісу, та з використанням пошукових фільтрів самої соціальної мережі:

1) дуже корисним для правоохоронців може бути спосіб перевірки діяльності особи в мережі Інтернет, коли відомі

справжні та заповнені відповідною інформацією профілі даної особи в соціальних мережах.

2) спочатку, використовуючи пошукові фільтри соціальних мереж, необхідно зібрати якомога більше інформації про особу;

3) далі, використовуючи адрес електронної пошти, номер ICQ, ім'я в сервісі Skype та телефонний номер особи, яка цікавить правоохоронців, а також добавляючи у подальшому ключові слова при пошуку – необхідно здійснити пошук інформації про особу використовуючи пошукові сервіси. Це пов'язано із тим, що левова частка користувачів Інтернету використовує різноманітні вузько направлені Інтернет – ресурси для спілкування, під час якого вони спілкуються під вигаданими прізвищами, наприклад: Magistro, Billy, Crazy. В цій діяльності можна навести приклад пошукового запиту, якщо завданням є пошук особи по форумах, Інтернет – магазинах, та для вивчення її листування і кола осіб, з якими дана особа спілкується;

4) для прикладу, правоохоронцям відомі такі дані про особу: адрес електронної пошти – Savage@yandex.ru, номер ICQ – 776558339, ім'я в сервісі Skype – Savage, телефонний номер – +380973455820. Тоді доцільним буде використання таких пошукових запитів: «Savage@yandex.ru 776558339 Savage +380973455820 форум», далі «Savage@yandex.ru 776558339 Savage +380973455820 інтернет магазин», далі «Savage@yandex.ru 776558339 Savage +380973455820 купити», далі «Savage@yandex.ru 776558339 Savage +380973455820 продати», а ще далі інші слова, чи речення, або словосполучення що найчастіше використовує при спілкуванні особа, що цікавить правоохоронців;

5) володіючи лише номером ICQ особи, що представляє оперативний інтерес, чи її ім'ям в сервісі Skype, вводячи ці данні в пошукові сервіси, і переходячи по усім зноскам, які виведе пошуковий сервіс, можливо знайти ще досить багато інформації про особу, а також визначити назви додаткових поштових скриньок цієї особи, а вже

зібрану інформацію використати для ще більш широкого пошуку в мережі Інтернет даних про таку особу.

Питання для самоперевірки та контролю засвоєння знань:

1. Які соціальні мережі Інтернету найбільше використовують для спілкування користувачі на території країн СНД?

2. Які особисті дані користувачів соціальних мереж Інтернету найбільш доцільно використовувати для пошуку інформації про осіб, які представляють оперативний інтерес для працівників ОВС України?

Список рекомендованої літератури:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

2. Кримінальний кодекс України. Кримінальний процесуальний кодекс України. – К.: Юрінком Інтер, 2012. – 608 с.

3. Цехан Д.М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ // Монографія / Д.М. Цехан ; за науковою редакцією О.О. Подобного. – Одеса : Юридична література, 2011. – 216 с.

4. І.О. Борозенний, О. О. Юхно Особливості використання мережі Інтернет та автоматизованих інформаційно-пошукових систем для забезпечення проведення негласних слідчих (розшукових) дій // Право і Безпека : науковий журнал, № 4 (46) за 2012 рік, - Харківський національний університет внутрішніх справ : видавництво ХНУВС, 2012. – 360 с.

5. Соціальна мережа «Facebook» [Електронний ресурс]. – Режим доступу: http://www.facebook.com

6. Соціальна мережа «Одноклассники» [Електронний ресурс]. – Режим доступу: http://www.odnoklassniki.ru

7. Соціальна мережа «Вконтакте» [Електронний ресурс]. – Режим доступу: http://www.vk.com

3.6 ОСОБЛИВОСТІ ПОШУКУ ІНФОРМАЦІЇ ПРО ОСОБУ ЯКА ПРЕДСТАВЛЯЄ ОПЕРАТИВНИЙ ІНТЕРЕС ПО ІДЕНТИФІКАТОРУ МЕРЕЖЕВОГО РІВНЯ (ПО IP АДРЕСІ)

IP-адреса (Internet Protocol address) — це унікальний числовий номер, або ідентифікатор мережевого рівня, що використовується для адресації комп'ютерів чи пристроїв у мережах, що побудовані з використанням протоколу TCP/IP. Прикладом такої мережі є Інтернет.

Будь-яка IP-адреса складається з чотирьох 8-бітних чисел, які називають октетами (вад латинського «ОКТ» - вісім). Найпростішим прикладом IP-адреси може бути адреса 192.168.0.31. Будь-якому доменному імені WEB-сайту, чи конкретному користувачу мережі Інтернет відповідає певний IP-адрес. Процес перетворення доменного імені у IP-адресу виконується DNS-сервером.

IP-адреса складається з двох частин: номера мережі і номера вузла. У разі ізольованої мережі її адреса може бути обрана адміністратором зі спеціально зарезервованих для таких мереж блоків адрес (14.14.0.0 / 6, 192.192.0.0 / 16 або 192.111.1.1 / 12). Але у разі, коли мережа повинна працювати як складова частина Інтернету, то адреса мережі видається провайдером або регіональним Інтернет-реєстратором (Regional Internet Registry, RIR). Згідно з даними на сайті IANA [32] існує п'ять RIR: ARIN, обслуговуючий Північну Америку; APNIC, обслуговуючий країни Південно-Східної Азії; AfriNIC, обслуговуючий країни Африки; LACNIC, обслуговуючий країни Південної Америки і басейну Карибського моря; та RIPE NCC, обслуговуючий Європу, Центральну Азію, Близький Схід. Ті регіональні реєстратори, які отримують номери автономних систем і великі блоки адрес у IANA, а потім видають номери автономних систем та блоки адрес меншого розміру локальним Інтернет-реєстраторам (Local Internet Registries, LIR), зазвичай є великими провайдерами.

Номер вузла в протоколі IP призначається незалежно від локальної адреси вузла. Маршрутизатор по визначенню входить відразу в кілька мереж. Тому кожен порт маршрутизатора має власну IP-адресу. Кінцевий вузол також може входити в кілька IP-мереж. У цьому випадку комп'ютер повинен мати кілька IP-адрес, по числу мережевих зв'язків. Таким чином, IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережеве з'єднання. Саме тому, завдяки наявності IP-адреси особи, яка представляє оперативний інтерес, можливо встановити місцезнаходження точки її доступу до Інтернету (країну, місто), та назву провайдера, який надає особі можливість такого доступу до Інтернету.

Головним завданням, в даному випадку, виступає спосіб отримання IP-адреси особи, яка представляє оперативний інтерес. Основними способами є такі, як: запити до адміністрації звичайних (комерційних чи некомерційних) Інтернет-сайтів та використання легендованих Інтернет-сайтів.

Запити до адміністрації звичайних (комерційних чи некомерційних) Інтернет-сайтів – є доцільними у тому випадку, коли працівнику ОВС відомо, що саме на цьому Інтернет-сайті зареєстрована та веде переписку (чи іншу діяльність, пов’язану з використанням можливостей конкретного Інтернет-сайту) особа, яка представляє тактичний чи оперативний інтерес. Запит є доцільним тому, що майже у всіх сучасних «двигунах» Інтернет-сайтів та Інтернет-форумів є функція фіксації IP-адреси кожного конкретного користувача, який зареєстрований на даному Інтернет-ресурсі, чи користувача, який заходив до Інтернет-ресурсу анонімно. У запиті необхідно указати підстави та причини звернення до адміністрації, та ім’я (вигадане чи справжнє) тієї особи, щодо якої необхідно узнати IP-адресу. Також доцільним є вказати в запиті настання відповідальності за розголошення відомостей, що містяться у запиті.

Використання легендованих Інтернет-сайтів – є доцільними у тому випадку, коли працівнику ОВС не вдалося у інший спосіб отримати IP-адресу особи, яка представляє оперативний інтерес, чи використання іншого способу отримання IP-адреси

є ризикованим (наприклад – витік інформації). У даному випадку головними завданнями є: використання достатньо легендованого сайту, який би не виглядав «порожнім», чи не був щойно створенним, та обережність при спрямуванні особи, яка представляє тактичний чи оперативний інтерес на даний Інтернет-ресурс. Обережність повинна виявлятись в тому, що необхідно пам'ятати про те, що настирливість у намаганнях спрямувати особу до легендованого сайту може її просто відклякати від нього, та навіть заставити її «залягти на дно». Тактично правильним рішенням буде визначити вподобання особи, визначити коло Інтернет-ресурсів, якими особа користується, дізнатися адреси електронної пошти особи, а потім, нібито не для неї,
залишати послання на легендований Інтернет-сайт. Це можуть бути графічні зображення малого розміру, що зумовлює бажання натиснути на них для того, щоб вони збільшились у розмірі, але замість цього – це буде масковане посилання на легендований Інтернет-сайт. Так само посилання можливо замаскувати під графічне зображення відео кліпу, чи аудіо запису, тощо. Звісно, на самому легендованому сайті повинна бути присутня функція фіксації IP-адрес користувачів, які до нього зайшли.

Розглянемо приклад, в якому працівнику ОВС відомо, що IP-адреса особи, яка розповсюджує відеофільми порнографічного характеру, має наступний ідентифікатор: 178.151.128.221 :

1) для отримання похідних даних від IP-адреси, зручно скористатись сервісом «WHOIS», наприклад таким, який надає Інтернет-ресурс «2IP.RU» [33];

2) для цього необхідно перейти на сторінку Інтернет-ресурсу за адресою «http://2ip.ru/whois», та у поле «IP адрес или домен» ввести ідентифікатор IP-адреси, яка представляє оперативний інтерес, після чого необхідно нажати клавішу «ENTER». У даному випадку – це IP-адрес: 178.151.128.221;

3) після цього буде сформовано сторінку, на якій буде відображено наступну інформацію:

ПАРАМЕТР	ЗНАЧЕННЯ	ПОЯСНЕННЯ
IP	178.151.128.221	IP-адреса, стосовно якої був виконаний запит
ХОСТ	224.128.151.178.triolan.net	IP-адреса серверу, через який користувач IP-адреси 178.151.128.221 здійснює доступ до Інтернету
МІСТО	Харьков	Місто, де знаходиться користувач IP-адреси 178.151.128.221
КРАЇНА	Ukraine	Країна, де знаходиться користувач IP-адреси 178.151.128.221
IP-діапазон	178.151.128.0 - 178.151.128.255	Діапазон IP-адрес, до якого належить IP-адреса 178.151.128.221
НАЗВА ПРОВАЙДЕРА	Kharkov , Odesskaya	Інтернет-провайдер, через який користувач IP-адреси 178.151.128.221 здійснює доступ до мережі Інтернет

4) далі, використовуючи отримані дані, а головне – країну, місто та назву Інтернет-провайдеру, через якого користувач IP-адреси 178.151.128.221 здійснює доступ до мережі Інтернет, від імені правоохоронного органу формується запит до Інтернет-провайдеру, в якому ставиться питання про те, до якої конкретної фізичної адреси прив’язана IP-адреса користувача. В да-

ному випадку – до якої фізичної адреси відноситься IP-адреса 178.151.128.221;

5) після отримання відповіді на запит, працівники органу внутрішніх справ приймають рішення про подальші дії: необхідність проведення негласних слідчих (розшукових) дій, обшуку чи інших слідчих дій;

6) аналіз отриманих результатів.

Питання для самоперевірки та контролю засвоєння знань:

1. Що являє собою та для чого призначений ідентифікатор мережевого рівня (IP–адреса)?

2. Яким чином по IP-адресі користувача можливо встановити місце його фактичного знаходження?

Список рекомендованої літератури:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

2. Кримінальний процесуальний кодекс України. – К.: Юрінком Інтер, 2012. – 608 с.

3. Таненбаум Э. Архитектура компьютера. 5-е изд. (+CD). — СПб.: Питер, 2007. — 844 с: ил.

4. Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ // Монографія / Д. М. Цехан ; за науковою редакцією О. О. Подобного. – Одеса : Юридична література, 2011.– 216 с.

5. Сервіс ідентифікації користувача за IP адресою «WHOIS» Інтернет–ресурсу «2IP.RU» [Електронний ресурс]. – Режим доступу: http://2ip.ru/whois

6. Ищенко Е. П. Новые информационные технологии обеспечения раскрытия и расследования преступлений / Е. П. Ищенко // Вісник ЛДУВС. - 2010. - № 1, спец. вип. № 2. - С. 3-14.

7. Захарченко В.Ю., Лазуренко В. И., Олифиров А. В . , Рогозин С.Н. Компьютерные преступления: их выявление и предотвращение: Учебное пособие / Под общ. редакцией В. И. Лазуренко. – К.: Центр учебной литературы, 2007. – 170 с.

РОЗДІЛ 4.
РЕКОМЕНДАЦІЇ ЩОДО УДОСКОНАЛЕННЯ МЕТОДИКИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

4.1 ЗАСТОСУВАННЯ НОВІТНІХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ЗАПОБІГАННІ РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ КСЕНОФОБНОГО ТА ПОРНОГРАФІЧНОГО ХАРАКТЕРА

На даний момент однією з найбільш нагальних проблем для України є саме поширення в мережі Інтернет різних видів інформації расистського, ксенофобного, та іншого характеру, що підбурює до насильницьких дій, ненависті чи дискримінації окремої особи або групи осіб, і ґрунтується на расовій, національній, релігійної або етнічної приналежності (в законодавстві України відповідальність за такі дії передбачена в ч.2 та ч.3 ст.109, ст.258-2, ст.295, ст.300, ст.436, ч.2 ст.442, КК України [7]), а також дитячої порнографії та матеріалів порнографічного характеру (в законодавстві України відповідальність за такі дії передбачена в ст. 300 КК України [7]). Проблема полягає в тому, що будь який користувач мережі Інтернет в Україні має змогу отримати доступ до електронного ресурсу, на якому розміщена зазначена вище інформація, навіть якщо він не знає назви даного Інтернет сайту. Достатньо лише ввести пошуковий запит «дивитись порнографію», чи «дивитись порно», чи «відео про вбивство» до пошукової системи, наприклад до такої як «Google» [15], і користувач отримає відповідь на свій запит у вигляді посилань на Інтернет ресурси, на яких і розміщена інформація, щодо якої у користувача виник інтерес. Навіть якщо батьки на домашніх комп'ютерах своїх дітей поставлять спеціальні програмні фільтри для того, щоб діти не мали змоги отримати режим доступу до заборонених батьками Інтернет ресурсів, ніщо не заважатиме дітям отримати режим доступу до цих Інтернет ресурсів з інших комп'ютерів. І це є великою проблемою для будь якої країни, адже за таких умов в мережі Інтернет можливо розміщувати аудіо, відео, текстові та графічні матеріали будь якого змісту, і кожен пересічний громадянин матиме змогу ознайомитись із

інформацією, яка містить в собі, наприклад, заклики до повалення конституційного ладу в країні, чи відеофільм дитячої порнографії.

Якщо Інтернет сайти розміщені на комп'ютерах, які фізично перебувають на території України, та на яких розміщена інформація, розміщення та розповсюдження якої підпадає під склад певного злочину Кримінального кодексу України, то це ще невелика проблема для правоохоронних підрозділів. Але зачасту буває так, що такі Інтернет сайти розміщені на комп'ютерах, що фізично перебувають, наприклад, на Філіппінських островах, і тоді припинити режим доступу до таких сайтів становить проблему для українських правоохоронців.

Фізично, будь які Інтернет ресурси розміщені на певних комп'ютерах, що розміщені по всьому світу. Для того, щоб будь-який користувач міг отримати доступ до певного ресурсу, данні про те, на якому саме комп'ютері розміщений той чи інший Інтернет сайт заносяться до спеціальних цифрових таблиць DNS серверів, які фізично розміщені на території США. Проміжною ланкою між користувачем і DNS сервером є Інтернет провайдер, тобто юридична особа, яка платно чи безоплатно забезпечує зв'язок між користувачем, DNS сервером, та Інтернет сайтом, режим доступу до якого хоче отримати користувач. На території України існую безліч Інтернет провайдерів, але їхня діяльність ґрунтується лише на законах та підзаконних актах України. А оскільки будь який Інтернет провайдер може налаштувати програмні фільтри так, щоб користувачі підключені до нього не мали доступу до певного Інтернет сайту чи ресурсу, ми пропонуємо:

1) створити відповідний підрозділ в системі Міністерства внутрішніх справ України, на який би покладалось завдання по пошуку та виявленню Інтернет ресурсів, де розміщена інформація расистського, ксенофобного, та іншого характеру, яка підбурює до насильницьких дій, ненависті чи дискримінації окремої особи або групи осіб, що ґрунтується на расовій, національній, релігійної або етнічної приналежності, а також різних видів дитячої порнографії та матеріалів порнографічного характеру;

2) на законодавчому рівні створити Єдиний державний реєстр заборонених Інтернет ресурсів, до якого вносити Інтернет ресурси виявлені зазначеним вище підрозділом;

3) законодавчо закріпити зобов'язання Інтернет провайдерів вносити Інтернет ресурси, що потрапили до зазначеного вище Єдиного державного реєстру заборонених Інтернет ресурсів до своїх програмних фільтрів, з метою блокування режиму доступу до них користувачами мережі Інтернет; 4) зважаючи на те, що кожен день в мережі Інтернет з'являється багато нових Інтернет ресурсів, а вже існуючі можуть змінювати характер та склад інформації, яка розміщується на них – регулярно проводити обновлення Єдиного державного реєстру заборонених Інтернет ресурсів, тобто включати до нього нові Інтернет ресурси, та виключати ті, які зі свої сторінок видалили інформацію забороненого характеру.

Можна зробити висновок, що для реалізації зазначених пропозицій щодо протидії розповсюдженню забороненої законодавством інформації в мережі Інтернет і впровадження вищезазначеного, необхідно створити відповідну законодавчу і нормативно-правову базу.

Питання для самоперевірки та контролю засвоєння знань:

1. Які новітні інформаційні технології доцільно використовувати для запобігання розповсюдження інформації ксенофобного та порнографічного характера?

Список рекомендованої літератури:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

2. Кримінальний кодекс України. Кримінальний процесуальний кодекс України. – К.: Юрінком Інтер, 2012. – 608 с.

3. Конвенція Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185, ратифіковано Верховною Радою України із застереженнями і заявами Законом N 2824-IV (2824-15) від 07.09.2005, ВВР, 2006, N 5-6, ст.71.

4. Таненбаум Э. Архитектура компьютера. 5-е изд. (+CD). — СПб.: Питер, 2007. — 844 с: ил.

5. Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ // Монографія / Д.М. Цехан ; за науковою редакцією О. О. Подобного. – Одеса : Юридична література, 2011. –216 с.

4.2 УДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА УКРАЇНИ ПРО КРИМІНАЛЬНУ ВІДПОВІДАЛЬНІСТЬ ЩОДО ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

На протязі останніх двох років серед працівників органів внутрішніх справ і науковців однією із найбільш дискусійних була і залишається проблема запобігання і протидії кіберзлочинності, а також впровадження нового Кримінального процесуального кодексу України [34]. Крім того, дуже дискусійною є новела з нового Кримінального процесуального кодексу України, щодо впровадження Єдиного реєстру досудових розслідувань [35] (далі – ЄРДР). Оскільки ЄРДР, з одного боку – «це створена за допомогою автоматизованої системи електронна база даних», порядок формування та ведення якої регулюється наказом, а з іншого боку – це «інструмент усього слідства України», то відповідно до ч. 2 ст. 214 КПК України факт внесення відомостей до Єдиного реєстру прирівнюється і є початком досудового розслідування.

На нашу думку, проблемою у функціонуванні ЄРДР перш за все може стати незаконне втручання в його роботу ззовні, тобто так звані «хакерські атаки», тому що ні для кого не є таємницею, що перша «хакерська атака» на Пентагон була вчинена ще у середині 1970-х років, і це було зроблено із хуліганських мотивів, а ЄРДР – це автоматизована комп'ютерна система, яка напряму пов'язана із функціонуванням великого державного апарату, зокрема слідчого. Проблема кіберзлочинності у всьому світі є дійсно досить важливою проблемою, що підтверджується постійним зростанням кількості особового складу спеціальних підрозділів по боротьбі з кіберзлочинністю і збільшення країн, якими було ратифіковано Конвенцію Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185 [4] (більш відомої в Україні під назвою «Конвенція про кіберзлочинність»). Крім того, про збільшення загрози автоматизованим комп'ютерним системам, якими обслуговується державні установи та державні апарати свідчить і те, що за даними

Nua Internet Surveys кількість користувачів глобальної мережі Інтернет з 80 тисяч у 1988 році зросла до 2,7 мільярдів на кінець 2013 року [1].

У розділі XVIII Кримінального кодексу України [7] передбачено статтю № 376-1 «Незаконне втручання в роботу автоматизованої системи документообігу суду», але немає спеціалізованої статті, яка б передбачала настання кримінальної відповідальності за незаконне втручання в роботу автоматизованої системи документообігу слідчих підрозділів, тобто в роботу ЄРДР. У випадку незаконного втручання в роботу такої автоматизованої системи, як ЄРДР – дії злочинця необхідно буде кваліфікувати за відповідною статтею розділу № XVI Кримінального кодексу України, але ми вважаємо, що більш доречним було б введення в КК України саме спеціалізованої статті, наприклад такої, як: стаття № 376-2 «Незаконне втручання в роботу автоматизованої системи документообігу слідчих підрозділів».

Виникають проблемні питання щодо подальшого кримінального провадження щодо ст. 361-2 КК України «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або носіях такої інформації», що вилучена із підслідності служби безпеки України згідно чинного КПК України, але охорона інформації з обмеженим доступом є одним з основних елементів забезпечення контр розвідувального режиму в державі, а сама інформація з обмеженим доступом є першочерговим об'єктом розвідувальних спрямувань з боку іноземних спецслужб, організацій та осіб. Крім того, в залежності від обставин вчинення кримінального правопорушення, злочинні дії можуть містити ознаки інших статей КК України, зокрема 111, 114, 328, 330, 442 КК, що залишилися у підслідності СБУ України. У зв'язку з викладеним було б доцільним внести в ст. 216 КПК України зміни з метою повернення статті 361-2 КК України до підслідності органів безпеки. Крім цього, до вже вказаного розділу XVI КК України доцільно додатково ввести статтю

361-3 КК України щодо встановлення кримінальної відповідальності за «Несанкціоноване втручання в роботу державних електронних інформаційних ресурсів або критичної інформаційної інфраструктури держави» та ст.362-1 КК України за «Несанкціоновані дії з інформацією яка оброблюється в державних електронних інформаційних ресурсах або технологічною інформацією в критичній інформаційній інфраструктурі держави, вчинені особою, яка має право доступу до неї».

Питання для самоперевірки та контролю засвоєння знань:

1. Які на вашу думку нові види злочинів у сфері використання інформаційних технологій є доцільним внести до відповідного розділу Кримінального кодексу України?

Список рекомендованої літератури:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

2. Кримінальний кодекс України (із змінами та доповненнями станом на 1 січня 2013 року). – Х. : Одіссей, 2013. – 232 с.

3. Кримінальний процесуальний кодекс України. – К.: Юрінком Інтер, 2012. – 608 с.

4. Кіберзлочинність в Україні: перспективи протидії [Електронний ресурс]. / Комітет протидії корупції та організованої злочинності. – Режим доступу: http://kpk.org.ua/2007/02/05/kberzlochinnst_v_ukran_perspektivi_protid.html.

4.3 АКТУАЛЬНІСТЬ СТВОРЕННЯ АВТОМАТИЗОВАНОЇ КОМП'ЮТЕРНОЇ СИСТЕМИ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФІКСАЦІЇ СЛІДІВ ЗЛОЧИННОГО СПРЯМУВАННЯ У МЕРЕЖІ ІНТЕРНЕТ ДЛЯ ВИКОРИСТАННЯ ПРАЦІВНИКАМИ ОРГАНІВ ВНУТРІШНІХ СПРАВ

На базі використання системи класифікації способів вчинення кримінальних правопорушень у сфері сучасних інформаційних технологій, працівниками Інтерполу було розроблено кодифікатор Генерального Секретаріату Інтерполу, де окремо передбачена класифікація комп'ютерних злочинів [3]. В Європі, ще у 2001 році було підписано Конвенцію Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185 [4], яка більш відома в Україні під умовною назвою «Конвенція про кіберзлочинність». Крім того, Європейським
комітетом з проблем злочинності Ради Європи у 1990 році, з метою визначення в Європі злочинів, пов'язаних із використанням сучасних комп'ютерних та інформаційних технологій, були підготовлені рекомендації про включення в законодавство європейських країн кримінальних норм «Мінімального списку» і «необов'язкового списку» щодо комп'ютерних злочинів. Всі зазначені закони, конвенції та підзаконні акти містять в собі визначення та класифікацію різноманітних злочинів у сфері комп'ютерної інформації. Але треба зазначити, що найбільшою проблемою в сфері розслідування злочинів вчинених у мережі Інтернет є виявлення та фіксації слідів злочинного спрямування. Це пов'язано з тим, що у разі, коли злочинець вчиняє протиправні дії на окремо взятому комп'ютері потерпілої особи чи використовує для цього свій комп'ютер, то навіть після видалення з комп'ютера даних злочинного спрямування, працівник правоохоронного органу все одно може ці данні знайти, відновити та вилучити в якості доказів. Інша річ, коли сліди злочинного спрямування знаходяться в мережі Інтернет.

Це може бути листування між злочинцями, чи листування між злочинцем і потерпілою особою. Також це можуть бути матеріали ксенофобного, чи порнографічного характеру. У разі, якщо злочинець видалить інформацію злочинного спрямування з Інтернет ресурсу, то в таких випадках вже виникають проблеми збереження інформації, яка цікавить працівників правоохоронних органів, адже комп'ютер, на якому фізично була розміщена інформація злочинного спрямування може знаходитись, наприклад в Новій Зеландії, і вилучити його для проведення експертизи буде дуже не просто, а в більшості випадків навіть неможливо. На сьогоднішній день в Україні склалася така практика фіксації слідчим слідів злочинного спрямування в мережі Інтернет, як виготовлення у присутності понятих електронного знімку (так званий «print screen») екрану монітору комп'ютера, на якому відображається Інтернет ресурс
зі слідами злочинного спрямування, після чого дане зображення роздруковується, та приєднується до інших матеріалів кримінального провадження, а самі сторінки Інтернет-ресурсу зберігаються на жорсткий диск, а потім записуються на CD-R чи DVD-R диск. Але у разі видалення інформації злочинного характеру зі сторінок Інтернет ресурсу, описаний вище електронний знімок втрачає свою процесуальну силу. Для того, щоб спростити процедуру виготовлення електронного знімку (так званий «print screen») екрану монітору комп'ютера, на якому відображається Інтернет ресурс зі слідами злочинного спрямування, і використати його, як один із видів доказу під час кримінального провадження, ми пропонуємо створити програмне забезпечення для функціонування автоматизованої комп'ютерної системи, робота якої повинна ґрунтуватися на певних принципах, та мати в собі інформаційні блоки. Зокрема:

1) автоматизована комп'ютерна система повинна мати блок взаємодії з Єдиним державним реєстром досудового розслідування, чи повинна мати вигляд блоку-розширення функцій зазначеного ЄДРДР. Тобто вхід до такої системи працівником

правоохоронного органу повинен бути здійснений з використанням кодів доступу слідчих до ЄДРДР; 2) автоматизована комп'ютерна система повинна мати автоматизований блок виготовлення електронного знімку (так званий «print screen») будь якої частини чи сторінки Інтернет ресурсу, а також автоматизований блок збереження усієї інформації, що знаходиться у будь-якій частині чи сторінці Інтернет ресурсу. За таких умов працівнику правоохоронного органу необхідно лише ввести в дану систему посилання на той чи інший Інтернет ресурс на якому є інформація злочинного спрямування, а автоматизована комп'ютерна система вже без участі людини зробить вище зазначені дії з таким Інтернет ресурсом;

3) виготовлений електронний знімок (так званий «print screen»), а також вся збережена інформація з будь якої частини чи сторінки Інтернет ресурсу (а це може бути текст, графічна, аудіо та відео інформація), повинні зберігатись у вигляді окремих розділів бази даних, які повинні маркуватись із зазначенням: дати створення розділу бази даних; номеру кримінального провадження; посади працівника правоохоронного органу, який створив даний розділ; справжньої назви та електронного адресу Інтернет ресурсу, чи його частини, з якого зроблено електронний знімок та копія інформації країни та міста, де фізично знаходиться комп'ютер, на якому було розміщено Інтернет ресурс з інформацією злочинного спрямування, чи з інформацією, яка є слідами злочину.

Можна зробити висновок, що для реалізації вирішення зазначених проблем, щодо створення програмного забезпечення для функціонування автоматизованої комп'ютерної системи, необхідно провести відповідні дослідження, результати яких запровадити у практичну діяльність новостворених при ГУМВС-УМВС України підрозділів боротьби з торгівлею людьми та кіберзлочинністю.

Питання для самоперевірки та контролю засвоєння знань:

1. Чи існує визначення поняття «цифровий доказ» у законодавстві України?

2. Які проблеми виникають під час процесуальної фіксації працівниками ОВС слідів злочинів, вчинених із використанням мережі Інтернет?

Список рекомендованої літератури:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

2. Кримінальний кодекс України (із змінами та доповненнями станом на 1 січня 2013 року). – Х. : Одіссей, 2013. – 232 с.

3. Кримінальний процесуальний кодекс України. – К.: Юрінком Інтер, 2012. – 608 с.

4. Таненбаум Э. Архитектура компьютера. 5-е изд. (+CD). — СПб.: Питер, 2007. — 844 с: ил.

5. Гуславский В.С., Задорожний Ю. А., Розовский В. Г. Информационно-аналитическое обеспечение раскрытия и расследования преступления // Монография – Луганск, ТОВ «Елтон-2», 2008. – 133 с.

6. Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ // Монографія / Д. М. Цехан ; за науковою редакцією О. О. Подобного. – Одеса : Юридична література, 2011.- 216 с.

7.Ищенко Е.П. Новые информационные технологии обеспечения раскрытия и расследования преступлений / Е. П. Ищенко // Вісник ЛДУВС. - 2010. - № 1, спец. вип. № 2. - С. 3-14.

8. Категорія: кіберзлочинність. [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/ категорія: кіберзлочинність.

9. Словарь криминологических и статистических терминов / А. Г. Кальман, И. А. Христич. – Х. : Гимназия : Ин-т изучения проблем преступности АПрН Украины, 2001. – 94 с.

10. Стратегія національної безпеки України [Електронний ресурс] : указ Президента України від 12 лют. 2007 р. № 105/2007. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/105/2007.

4.4 МЕТОДИКА ФІКСАЦІЇ СЛІДІВ ЗЛОЧИННОГО СПРЯМУВАННЯ У МЕРЕЖІ ІНТЕРНЕТ

Факторами та чинниками, які суттєво ускладнюють можливість фіксації працівником ОВС цифрової інформації, є: можливість у адміністратора Інтернет-ресурсу (чи власника, що нерідко є синонімом) оперативно в управлінському розумінні змінювати його зміст, чи повністю його видалити з серверу; наявність можливості розташування серверів на території інших держав, та зокрема, на території тих держав, які не підписали міжнародні угоди щодо протидії кіберзлочинності; використання зловмисниками анонімних програмних пакетів. Як зазначає Д. М. Цехан, «особливої гостроти ця проблема набуває у зв'язку з тим, що встановлення факту такого порушення є чи не найбільш значимою складовою процесу доказування у відповідних провадженнях» [14, с. 127].

Нижче ми приводимо декілька основних способів фіксації працівником ОВС цифрової інформації, яка знаходиться в мережі Інтернет та представляє тактичний чи оперативний інтерес:

1) складання (друк) та подання відповідного рапорту працівником ОВС;

2) відповідь провайдера, чи адміністрації Інтернет-хостінгу на запит щодо змісту певного Інтернет-сайту;

3) огляд в присутності понятих, та друк тієї сторінки Інтернет-ресурсу, яка представляє тактичний чи оперативний інтерес, через засоби WEB-браузеру (комбінація клавіш «CTRL+P» чи вибір поля головного меню «Печать» або «Print»). Складання відповідного протоколу огляду;

4) огляд в присутності спеціаліста, та друк тієї сторінки Інтернет-ресурсу, яка представляє оперативний інтерес, через засоби WEB-браузеру (комбінація клавіш «CTRL+P» чи вибір поля головного меню «Печать» або «Print»). Складання відповідного протоколу огляду;

5) огляд в присутності понятих Інтернет-ресурсу, який представляє оперативний інтерес. Виготовлення електронного

знімку (так званий «print screen») екрану монітору комп'ютера, на якому відображається Інтернет-ресурс та його збереження. Збереження самого Інтернет-ресурсу, який представляє тактичний чи оперативний інтерес, на жорсткий диск комп'ютера працівника ОВС. Далі здійснюється друк виготовлених електронних знімків екрану та приєднання їх до інших матеріалів кримінального провадження. Запис на CD-R чи DVD-R диск, виготовлених електронних знімків екрану, та збережених під час огляду на жорсткий диск сторінок Інтернет-ресурсу, що представляє тактичний чи оперативний інтерес. Після цього складається відповідний протокол щодо усіх виконаних дій.

Питання для самоперевірки та контролю засвоєння знань:

1. Які методики доцільно використовувати для фіксації слідів злочинного спрямування у мережі Інтернет працівниками ОВС України?

2. Як процесуально оформляються результати фіксації слідів злочинного спрямування у мережі Інтернет працівниками ОВС України?

Список рекомендованої літератури:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

2. Кримінальний кодекс України (із змінами та доповненнями станом на 1 січня 2013 року). – Х. : Одіссей, 2013. – 232 с.

3. Кримінальний процесуальний кодекс України. – К.: Юрінком Інтер, 2012. – 608 с.

4. Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ // Монографія / Д. М. Цехан ; за науковою редакцією О. О. Подобного. – Одеса : Юридична література, 2011. – 216 с.

5. Ищенко Е. П. Новые информационные технологии обеспечения раскрытия и расследования преступлений / Е. П. Ищенко // Вісник ЛДУВС. - 2010. - № 1, спец. вип. № 2. - С. 3-14.

6. Таненбаум Э. Архитектура компьютера. 5-е изд. (+CD). — СПб.: Питер, 2007. — 844 с: ил.

4.5 МЕТОДИКА ОГЛЯДУ СТРУКТУРИ ФАЙЛОВОЇ СИСТЕМИ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА ЗАХИЩЕНОГО ПАРОЛЕМ

Під час проведення працівниками органів внутрішніх справ тимчасового доступу до речей і документів, обшуків чи оглядів місця події на підприємствах, установах, організаціях або у приватних осіб, може виникнути необхідність перевірити структуру файлової системи персонального комп'ютера (далі – ПК), чи серверу на предмет неліцензійного програмного забезпечення або інформації, яка представляє для слідчого тактичний чи для оперативного працівника оперативний інтерес.

В ході проведення зазначених дій, як правило, працівники ОВС проводять їх без увімкнення комп'ютера, та вилучають і опечатують лише системний блок (персональний комп'ютер без монітору, колонок, маніпулятору «миша» та клавіатури), чи жорсткий диск, а після проведення зазначених процесуальних дій призначають проведення комп'ютерно-технічної експертизи. Але для більш надійної фіксації слідів злочину та швидкого використання при виявленні, розкритті та розслідуванні кримінального правопорушення доцільним є при проведенні названих дій увімкнення персонального комп'ютера та здійснення огляду його файлової системи в присутності понятих, внесення до протоколу огляду даних про версію та серійний номер встановленої на комп'ютері операційної системи, назви та характеристики внутрішніх пристроїв комп'ютеру, а також зазначення шляхів до папок, чи окремих файлів, що розташовані на жорсткому диску персонального комп'ютера чи серверу що оглядається. У практичній діяльності, коли працівники ОВС будуть мати тимчасовий доступ до персонального комп'ютера чи сервера в ході чого він буде вилучений і по наявній інформації будуть призначені експертизи, то в деяких випадках висновок експерта може надійти у термін понад одного місяця. В цей же період у працівників ОВС можуть виникнути питання про наявність чи відсутність такої інформації на жорсткому диску для подальшої роботи у кримінальному провадженні. Таким чином,

при виявленні неліцензійного програмного забезпечення, чи інформації, яка представляє тактичний чи оперативний інтерес на персональному комп'ютері чи сервері, файлова система яких оглядається, та після фіксації місцезнаходження зазначеної інформації у протоколі огляду – працівники правоохоронних органів отримують додаткові підстави для тимчасового доступу і вилучення персонального комп'ютера чи серверу та додаткову можливість поставити експерту більш конкретні запитання.

Але проблемність даних процесуальних і суто технічних дій полягає у тому, що у більшості випадків на вхід до операційної системи персональних комп'ютерів та серверів встановлено пароль і власник персонального комп'ютера чи серверу може відмовитися надати пароль для входу. Крім того, оскільки попередній огляд персонального комп'ютера чи серверу проводиться в присутності понятих, огляд доцільно проводити саме в тій операційній системі, що проінстальована на персональний комп'ютер чи сервері та під ім'ям кожного користувача, якщо їх декілька, а не взагалі зробити загальний огляд файлової системи. Це необхідно для того, щоб наглядно показати й роз'яснити понятим, що за операційна система встановлена на персональному комп'ютері чи сервері, скільки користувачів зареєстровано в даній операційній системі, яке програмне забезпечення встановлено у кожного з цих користувачів, та яка інформація зберігається в особистих розділах цих користувачів.

Окремо слід зазначити, що у будь-якому випадку включати під час огляду персональний комп'ютер, не знаючи заздалегідь пароль для входу в операційну систему є ризикованим кроком, тому, що існує багато видів програмного забезпечення, яке може просто видалити всі файли на жорсткому диску у разі, якщо було введено не вірний пароль. І таким програмним забезпеченням правопорушники користуються не рідко. Саме тому й працівники ОВС в свою чергу намагаються здійснити тимчасовий доступ до комп'ютера без його вмикання, що є логічним, але позбавляє можливості швидко отримати інформа-

цію, яка може представляти для них тактичний чи оперативний інтерес.

На підставі викладеного при тимчасовому доступі до комп'ютера чи сервера можна рекомендувати два алгоритми огляду або вилучення системного блоку персонального комп'ютера чи сервера: перший – вилучення без увімкнення комп'ютера і другий – вилучення з увімкненням комп'ютера та оглядом структури його файлової системи.

При тимчасовому доступі до комп'ютера чи сервера і проведенні огляду і їх вилучення без його увімкнення, доцільним буде провести такі дії: в присутності понятих провести фотографування (або здійснити відео зйомку) системного блоку з усіх боків, обережно від'єднати від системного блоку усі сторонні пристрої та кабелі, провести зовнішній огляд системного блоку та окремо крупним планом сфотографувати чи зняти на відео наявні на ньому роз'єми та наклейки, після чого обклеїти усі бокові панелі системного блоку папером з відтисками печатки «для пакетів» того підрозділу органу внутрішніх справ, що проводить тимчасовий доступ до комп'ютера чи сервера і здійснює огляд чи вилучення. Обклеювання папером з відтисками печатки бокових панелей системного блоку необхідно провести для того, щоб не санкціоноване відкриття панелей, в подальшому, без пошкодження паперу з відбитками печатки було б не можливо, і таким чином було б гарантовано збереження інформації на жорсткому диску комп'ютера до проведення комп'ютерно-технічної експертизи. Після цього системний блок персонального комп'ютера чи сервера необхідно помістити в ящик, мішок чи полімерний пакет, який необхідно прошити ниткою, обклеїти нитку та ящик, мішок чи пакет пояснювальною запискою, із зазначенням місця та часу огляду чи вилучення, вказати конкретно, що саме вилучається та упаковується, а також інформацію про понятих та особу, яка проводить вказані дії, після чого пояснювальна записка повинна бути підписана всіма учасниками.

Тимчасовий доступ до комп'ютера чи серверу та огляд їх з увімкненням комп'ютера та оглядом структури його фай-

лової системи проводиться декількома способами, але після закінчення огляду структури файлової системи, системний блок персонального комп'ютера чи сервера необхідно оглянути та провести його вилучення так само, як і у випадку без включення комп'ютера. Не зважаючи на те, який саме алгоритм огляду комп'ютера при його увімкненні буде використаний, необхідно звернути увагу на те, що особі, яка отримала тимчасовий доступ до комп'ютера чи сервера і проводить огляд, необхідно буде спочатку загрузитись не з жорсткого диску комп'ютеру, а з CD чи DVD диску, або через підключений USB пристрій. Для цього працівнику ОВС, який проводить огляд комп'ютеру, необхідно мати доступ до базової системи вводу – виводу (англійською мовою – це широко відома абревіатура «BIOS») комп'ютеру, який може мати пароль для користування. Зазвичай, пароль в BIOS стирають таким чином: в присутності понятих відкривають системний блок, виймають батарейку з материнської плати, знаходять замкнуті контакти (зазвичай їх три) на материнській платі з підписом «cmos», або «clear cmos», або «clr cmos», або «clr_cm», перемикають замикач контактів (сленгова назва «джампер») на протилежні контакти (тобто, якщо було замкнено перший та другий контакти, то замикач контактів перемикають на другий та третій контакти), після чого вмикають комп'ютер, який може увімкнутись та не виводити жодної інформації на монітор, або комп'ютер може взагалі не увімкнутись. Далі, хоча б через п'ять хвилин після того, як було достагнуто батарейку, цю саму батарейку необхідно поставити на своє місце, та ще раз увімкнути комп'ютер, який знову таким може увімкнутись та не виводити жодної інформації на монітор, або може взагалі не увімкнутись. Після цього, замикач контактів переставляють у те положення, в якому він був на момент відкриття системного блоку, вставляють батарейку на своє місце, закривають системний блок, та вмикають комп'ютер. У переважній більшості випадків, після зазначених дій з комп'ютером, пароль BIOS буде стертий. Але крім самого паролю, в BIOS також будуть стерті усі настройки роботи пристроїв комп'ютеру, а самий факт розбирання

комп’ютера та фізичне втручання в роботу його електронної, а не програмної частини працівником ОВС – є негативним фактором для збору і отримання вагомості доказів, які можливо отримати в майбутньому при тимчасовому доступі до комп’ютера чи серверу і які оглядаються. Таким чином, при загрузці з CD чи DVD диску, або через підключений USB пристрій. ми рекомендуємо спочатку намагатись вибрати черговість загрузки пристроїв комп’ютера не через настройки BIOS, а шляхом вибору меню загрузки пристроїв (інша широко відома назва – «boot menu»), яке визивається при натисканні клавіш «F8», чи «F9», чи «F10», чи «F11», чи «F12» (в залежності від виробника материнських плат) відразу після увімкнення комп’ютера.

Огляд або вилучення з увімкненням комп’ютера та оглядом структури його файлової системи здійснюється декількома способами, але після закінчення огляду структури файлової системи, системний блок персонального комп’ютера чи сервера необхідно оглянути та провести його вилучення так само, як і у випадку без включення комп’ютера, тобто так само, як і у прикладі наведеному у першому випадку. Як вже зазначалось, огляд чи вилучення з увімкненням комп’ютера та оглядом структури його файлової системи проводиться декількома способами а саме: огляд файлової системи персонального комп’ютеру чи серверу без загрузки операційної системи, що встановлена на комп'ютері, та відключення паролів користувачів операційної системи, що встановлена на комп'ютері і огляд файлової системи персонального комп’ютеру, після чого зокрема слід здійснити:

1) для огляду файлової системи персонального комп’ютера чи серверу доцільно використати загрузочну операційну систему, таку як: «Windows Live CD», чи будь-який «Linux Live CD». В даному випадку необхідно налаштувати загрузку комп’ютера що оглядається так, щоб в першу чергу комп’ютер загружався не зі свого жорсткого диску, а з CD/DVD носія, на якому записана операційна система «Linux Live CD», або «Windows

Live CD». Пріоритет загрузки пристроїв на комп'ютері, файлову систему якого необхідно оглянути, необхідно налаштувати в базовій системі вводу-виводу комп'ютера (на англійській-BIOS), а далі вставити диск з загрузочною операційною системою в CD чи DVD пристрій, та загрузити операційну систему з нього. При цьому файлова система комп'ютера, що оглядається змінена не буде, а загрузочна операційна система встановиться в оперативно-запам'ятовуючий пристрій, який очиститься від пароля після перезавантаження комп'ютера. Після встановлення в оперативно-запам'ятовуючий пристрій загрузочної операційної системи, працівник правоохоронного органу може отримати змогу оглянути файлову систему персонального комп'ютера чи серверу без обмеження доступу до файлової системи в цілому, чи без обмеження доступу до окремих файлів чи папок. Перед завантаженням загрузочної операційної системи, і під час огляду структури файлової системи, необхідно запросити понятих до монітору комп'ютера, що оглядається для того, щоб вони могли побачити й підтвердити перелік дій, що здійснив працівник ОВС під час огляду персонального комп'ютера чи сервера. Під час огляду файлів та папок на комп'ютері, що оглядається доцільним є відеозапис дій працівника ОВС на відеокамеру, та здійснити зокрема відеозапис екрану монітору комп'ютера, що оглядається за допомогою спеціального програмного забезпечення, яке може входити в склад програмного забезпечення загрузочного диска. Крім того, усі дії під час огляду комп'ютера необхідно заносити до протоколу огляду, а у разі виявлення файлів, що представляють тактичний, оперативний чи процесуальний інтерес, необхідно заносити до протоколу огляду їх назву, повний шлях до них у файловій системі, розмір у байтах, та бажано створювати для них MD5 суму із спеціальним програмним забезпеченням та подальшим внесенням цієї

MD5 суми до протоколу. Треба наголосити, що при створенні MD5 суми для конкретного файлу ця сума у вигляді цифр та знаків буде унікальною для кожного файлу, що відрізняється від іншого файлу хоча б на один байт, а значить ця MD5 сума буде підтверджувати автентичність та незмінність файлу і в подальшому, тобто в ході проведення експертиз, чи під час судового розгляду кримінального провадження (справи) по суті в суді. Треба зазначити, що використання загрузочної операційної системи «Windows Live CD» потребує наявності у користувача ліцензії на її використання, але така операційна система має дещо менше можливостей, ніж загрузочна операційна система «Linux Live CD». Крім того, загрузочна операційна система «Linux Live CD» здебільшого є безкоштовною, і може працювати майже з будь-якими файловими системами. Саме тому ми рекомендуємо користуватись загрузочною операційною системою «Linux Live CD». Як приклад, ви можете завантажити загрузочний диск з операційною системою «Lubuntu» з російськомовного Інтернет ресурсу цієї операційної системи [36], а потім, записавши завантажений образ на диск, користуватись нею для проведення оглядів персонального комп’ютера чи сервера наведеним вище способом;

2) для відключення паролів користувачів операційної системи, встановленої на персональному комп'ютері чи сервері, доцільніше за все використати спосіб наведений вище, але з використанням спеціалізованої загрузочної операційної системи та спеціалізованого програмного забезпечення саме для зміни чи відключення паролів, а вже потім, після перезавантаження комп'ютера, вийняти диск з загрузочною операційною системою, та загрузитись зі встановленої на персональному комп’ютері чи сервері операційної системи. В даному випадку ми рекомендуємо використовувати загрузочну операційну систему «BartPE» [37] та програмне забезпечення до неї

під назвою «Password Renew» [38]. Особливістю загрузочної операційної системи «BartPE» є те, що її може створити (зібрати) на основі звичайної операційної системи «Windows» будь-який користувач, але у випадку володіння ліцензійної версії операційної системи «Windows». Враховуючи те, що МВС України активно закупає ліцензійні операційні системи «Windows» – це не викличе суттєвих складнощів у працівників органів внутрішніх справ. Під час створення збірки загрузочної операційної системи «BartPE» до її складу необхідно додати програму «Password Renew» [38], за допомогою якої, після встановлення загрузочної операційної системи «BartPE» в оперативно-запам'ятовуючий пристрій персонального комп'ютеру чи серверу, файлову систему якого необхідно оглянути, працівниками ОВС буде можливо змінити, чи видалити паролі користувачів з тієї операційної системи, яка вже встановлена на персональний комп'ютер чи сервер, що оглядається. Саму файлову систему комп'ютера, а так само особисті файли користувачів пошкоджено чи змінено не буде. Детальніше про створення загрузочної операційної системи «BartPE» ви можете прочитати на російськомовному сайті, присвяченому цій операційній системі [37].

Але як і в першому випадку, проводити наведені дії комп'ютером, що оглядається необхідно лише в присутності понятих перед монітором комп'ютера, а всі свої дії працівник ОВС повинен вносити до відповідного процесуального протоколу згідно положень, зокрема ст.ст. 223, 234, 236, 237, 242, 243, 256 та інших Кримінально-процесуального кодексу України, в залежності від обставин вчинення конкретного кримінального правопорушення.

Більшості працівників міліції та тих хто цікавиться проблемами програмного забезпечення при використанні комп'ютерної техніки відома базова система введення і виведення «BIOS» комп'ютера за допомогою якої (на думку бага-

тьох осіб, у тому числі працівників ОВС) нібито можна без пошкодження вскрити комп'ютерну програму на яку встановлено пароль для користування нею без володільця. В той же час для питань правозастосовної діяльності, на нашу думку вона у використанні не доцільна, оскільки при її застосуванні все ж таки при огляді комп'ютерної техніки може бути знищена необхідна для використання у кримінальному провадженні доказова інформація на комп'ютері захищеному паролем.

Питання для самоперевірки та контролю засвоєння знань:

1. Які проблеми виникають під час огляду працівниками ОВС України структури файлової системи персонального комп'ютера захищеного паролем?

2. Яке програмне забезпечення доцільно використовувати для огляду структури файлової системи персонального комп'ютера захищеного паролем працівниками ОВС України?

3. Які проблеми можуть виникнути перед працівниками ОВС при тимчасовому доступі до комп'ютера і при його вилучені у разі його огляду у вимкнутому режимі або у не вимкнутому режимі ?Наведіть алгоритм дій працівників ОВС можливий у таких випадках ?

4. Як Ви вважаєте чи є перспектива подальшого використання базової системи введення і виведення «BIOS» комп'ютера для вскриття комп'ютера захищеного паролем ?

Список рекомендованої літератури:

1. Конституція України [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/254к/96-вр

2. Кримінальний кодекс України. Кримінальний процесуальний кодекс України. – К.: Юрінком Інтер, 2012. – 608 с.

3. Таненбаум Э. Архитектура комп'ютера. 5-е изд. (+CD). — СПб.: Питер, 2007. — 844 с: ил.

4. Цехан Д.М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ // Монографія / Д.М. Цехан ; за науковою редакцією О.О. Подобного. – Одеса : Юридична література, 2011. – 216 с.

ДОДАТКИ

Додаток А

Діаграма №1 **Рівень зареєстрованої кіберзлочинності в Україні за 2002-2011 роки**

Додаток Б

Рівень та динаміка кіберзлочинності в Україні за 2002-2011 роки

Роки	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Зареєстровано злочинів у сфері використання ЕОМ(комп'ютерів), систем та комп'ютерних мереж	30	74	53	62	97	145	189	217	190	131
Приріст до 2002р. (у %)		146,6	76,6	106,6	223,3	383,3	530	623,3	533,3	336,6
Приріст до попереднього року (у %)		146,6	-28,4	17	56,4	49,9	30,3	14,8	-12,4	-31

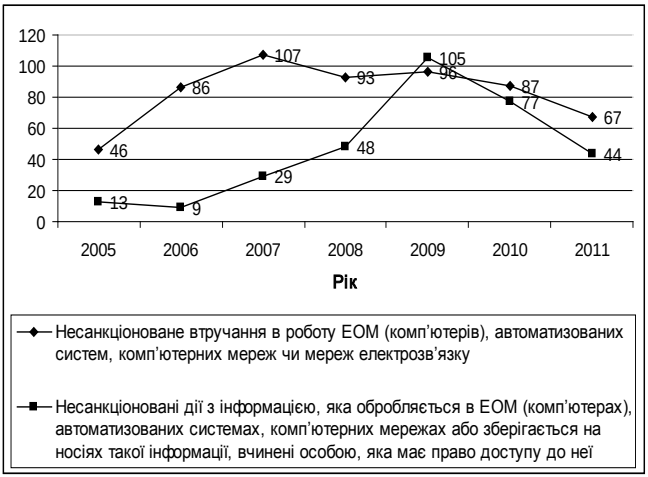
Додаток В

Рівень та динаміка кіберзлочинності в Україні за 2005-2013 роки (за видами злочинів)

	Зареєстровано злочинів у сфері використання ЕОМ(комп'ютерів), систем та комп'ютерних мереж	2005	2006	2007	2008	2009	2010	2011	2012	2013
За видами злочинів	Несанкціоноване втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку	46	86	107	93	96	87	67	74	48
	Створення з метою використання, розповсюдження або збуту шкідливих програм чи технічних заходів, а також їх розповсюдження або збут	0	2	6	3	5	12	10	22	5
	Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації	0	0	2	17	11	14	8	18	5
	Несанкціоновані дії з інформацією, яка обробляється в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї	13	9	29	48	105	77	44	38	8
	Порушення правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється	3	0	1	28	0	0	1	2	2
	Перешкоджання роботі ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку	0	0	0	0	0	0	1	0	0
	Всього	65	99	155	138	130	166	69	154	68

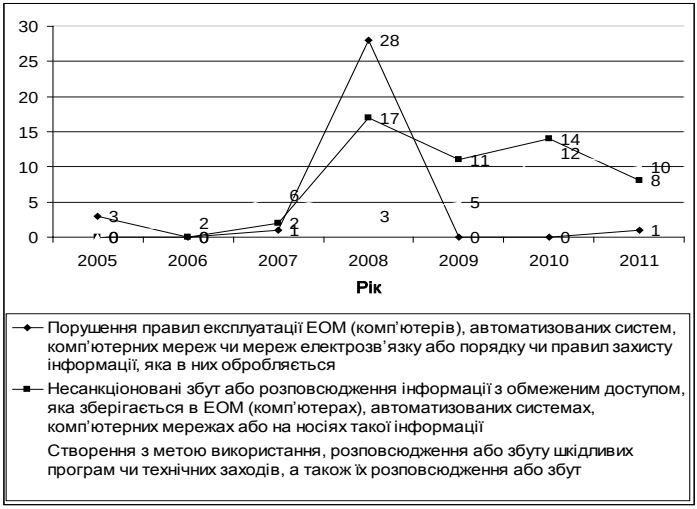
Додаток Г

Динаміка кіберзлочинності в Україні за 2005—2011рр. (за видами злочинів)



Додаток Д

Динаміка кіберзлочинності в Україні за 2005-2011 роки (за видами злочинів)



СЛОВНИК ТЕРМІНІВ, ЩО ВИКОРИСТОВУЮТЬСЯ В МЕРЕЖІ ІНТЕРНЕТ

ADSL (Asymmetrical Digital Subscriber Line) – асиметрична цифрова абонентська лінія.

ASCII (American Standard Code for Information Interchange) – американський стандартний код для обміну інформацією.

ASCIIZ – рядок символів коду ASCII, що закінчується символом NULL.

BIOS (Basic Input/ Output System) – базова система вводіння ви-водіння.

B-ISDN (Broadband ISDN) – широкосмугова цифрова мережа інтегрованих послуг.

CDMA (Code Division Multiple Access) – множинний доступ з кодовим розділянням (каналів).

CD-ROM (Compact Disk Rcad-Only Memory) – постійна пам'ять на компакт-диску; постійний запам'ятовувальний пристрій на компакт-диску; компакт-диск, який не можна перезаписати.

CD-ROM XA, CD-ROM/XA (Compact Disk Read-Only Memory cXtcnded Architecture) – компакт-диск, який не можна пере¬записати, з розширеною архітектурою; нестирана пам'яті, на компакт-диску з розширеною архі тсктурою.

DB (DataBase) – базові дані, база даних.

Dbkey (DataBase KEY) – ключ бази даних.

DBS (Digital Banking System) – цифрова банківська система.

DDD (Direct Distance Dialing) – автоматичний виклик віддаленого абонента.

DHCP (Dynamic Host Configuration Protocol) – протокол динамічного налагоджування конфіїгурації головної ЕОМ.

DNS 1. (Domain Name System) доменна (доменова) – система імен.

DNS 2. (Domain Name System (Service)) – система (служба) іменування доменів (протокол обслуговування каталогів у TCP/IP).

DRAM (Dynamic Random Access Memory) – динамічна оперативна пам'ять.

DRAW (Direct Read After Write) – безпосереднє читання після записування (контроль запису на оптичний диск); читання безпосередньо після записування.

DRCS (Dynamically Redefinable Character Set) – динамічно завантажувані шрифти.

DSN (Digital Switching Network) – цифрова комунікаційна мережа.

EACC (Error-Adaptive Control Computer) – стійка до помилок керівна ЕОМ.

EBCS (Electronic Business Communication System) – система передавання ділової інформації.

ETC (Enhanced Throughput Cellular) – удосконалений стільниковий зв'язок (протокол корпорації AT&T для виправлянння помилок передавання в стільникових мережах).

FA (Final Address (register)) – регістр кінцевої адреси.

FAQ (Frequently Asked Questions) – часто задавані запитання.

FAT (File Allocation Table) – таблиця розміщення файлів (в операційній системі ДОС).

FTP 1. (File Transfer Program) – програма передавання файлів.

FTP 2. (File Transfer Protocol) – протокол передавання файлів.

FTU (First-Time User) – новий користувач.

GEOS (Geostationary Earth-Orbiting Satellite) – геостаціонарний супутник.

GIF (Graphic Interchange Format) – формат для обміну графічною інформацією; формат обміну графічними даними.

GM (Global Memory) – глобальна пам'ять.

HDD (Hard Disk Drive) – дисковод жорсткого диска, вінчестер.

HS (High-Speed) – швидкопрохідний, швидкісний.

IBM-compatible – IBM-сумісний.

IR 1. (Information Retrieval) – пошук інформації, інформаційний пошук.

IR 2. (InfraRed) – інфрачервоний.

IR 3. (Instruction Register) – регістр команд.

IR 4. (Internal Resistance) – внутрішній опір.

IR 5. (Interrogator-Responder) – запитувач-відповідач.

IR 6. (Interrupt Register) – регістр переривань.

ISDN (Integrated Services Digital Network) – цифрова мережа інтегрованих послуг; цифрова мережа зв'язку з інтеграцією служб і комплексними послугами.

JPEG (Joint Photographies Expert Group) – спеціальний графічний формат, який розробила об'єднана група експертів з фотографії. Дає змогу зберігати картинки у файлах найменших розмірів.

LBA (Linear-Bounded Automaton) – автомат з лінійно обмеженою пам'яттю.

LBN (Logical Block Number) – номер логічного блоку.

LPT (Line PrinTer) – паралельний порт для принтера.

MAC 1. (Machine-Aided Cognition) – навчання за допомогою (обчислювальної) машини.

MAC 2. (MACintosh) – серія персональних комп'ютерів (комп'ютерів) фірми Apple.

MAC 3. (Maximum Allowable Concentration) – максимально допустима концентрація.

MAC 4. (Medium Access Control) – керування доступом до середовища (даних).

MAC 5. (Message Authentication Code) – код підтвердження автентичності повідомлення.

MAC 6. (Microprocessor-Array Computer) – обчислювальна машина на основі матриці мікропроцесорів.

MBR (Master Boot Record) – первинний завантажувач диска.

MODEM (MOdulator/DEModulator) – модулятор-демодулятор, модем.

NETACP (NETwork Ancillary Process) – процес допоміжного керування мережею.

NETBEUI (NETBIOS End User Interface) – інтерфейс кінцевого користувача з NETBIOS.

NETBIOS (NETwork Basic Input/Output System) – мережева базова система вводіння виводіння.

NT 1. (Nested Task) – вкладена задача.

NT 2. (Network Terminal) – мережевий термінал.

NT 3. (New Technology) – нова технологія.

NT 4. (No Transmission) – немає передавання.

NVROM (Non-Volatile Read-Only Memory) – снергонезалежна постійна пам'ять.

PDB 1. (Physical Data Base) – фізична база даних.

PDB 2. (Populated DataBase) – заповнена база даних.

PDB 3. (Process DataBase) – база даних про процеси.

PDB 4. (Protected DataBase) – захищена база даних.

PDBR (Page DirecloryBase Register) – базовий регістр каталогу сторінок.

PDF 1. (Portable Data File) – компактний файл даних.

PDF 2. (Portable Document Format) – переносний формат документів.

POSI (Portable Operating System Interface) – переносимий інтерфейс для операційних систем.

RAM (Random Access Memory) – запам'ятовувальний пристрій з довільним вибиранням, робоча (оперативна) пам'ять.

RIP (Raster Image Processor) – процесор растрових зображень; растровий процесор.

RISC 1. (Reduced Instruction Set Computer) – комп'ютер зі скороченим набором команд.

RISC 2. (Reduced Instruction Set Computing) – спрощена система машинних команд.

ROM (Read-Only Memory) – постійна пам'ять, постійний запам'ятовувальний пристрій, пам'ять тільки для читання.

SMTP (Simple Mail Transfer Protocol) – простий протокол пересилання (передавання) пошти. Стандартний протокол Internet для передавання повідомлень електронної пошти між комп'ютерами (компуторами).

SNAP (Standard Network Access Protocol) – стандартний протокол мережевого доступу.

STD (Subscriber Trunk Dialing) – набирання номера для міжміського зв'язку.

SYS (SYStem library) – системна бібліотека.

TCP/IP (Transmission Control Protocol/Internet Protocol) – протокол керування передаванням (міжмережевин протокол). Набір протоколів, які керують Internet і визначають способи передавання даних між комп'ютерами (компуторами).

TCSEC (Trusted Computer System Evaluation Criteria) – критерії оцінювання придатності комп'ютерних (компуторних) систем.

TXT (TeXT) – текст.

UFD (User File Directory) – каталог файлів користувача.

UFI (User Friendly Interface) – дружній інтерфейс.

VBF (Variable-length Bit Field) – бітове поле змінної довжини.

WIN (Wireless Inbuilding Network) – безпроводова внутрішня мережа.

WRU (Who aRc yoU) – «хто ви?» (сигнал запиту).

WTH (What The Heck) – «якого чорта!».

WWW (World-Wide Web) – «всесвітня павутина». Система, яка використовує для переходів між джерелами даних гіпертекстові посилання, а це дає змогу одержувати доступ до мережевих ресурсів з різних точок входу.

WYDIWYS (What You Do Is What You See) – «що зробиш, те й побачиш"» (на екрані дисплея).

WYPIWYF (What You Print Is What You Fax) – «що надрукуєш, те й буде передано по факсу».

WYSIWYG (What You Sec Is What You Get) – «що бачиш, те й маєш» (зображення на екрані еквівалентне надрукованому); режим повної візуальної відповідності: що побачиш на екрані, те й одержиш друком.

Адміністратор (administrator) – це власник сайту, особа, яка має найбільші повноваження.

Анімація (animation) – це один із способів подання рухомих зображень у мережі Інтернет.

Байт (byte) – це основна одиниця виміру кількості інформації, що дорівнює 8 Біт.

Банер (banner) – це графічний об'єкт, який рекламує певний сайт або продукцію.

Біт – це найменша одиниця виміру кількості інформації.

Браузер (browser) – це клієнтська програма для роботи у Всесвітній Павутині , яка дозволяє користувачу переглядати зміст web-сторінок.

Гіперпосилання (hyperlink) – це слово чи зображення в електронному документі, що містять посилання на інші файли.

Гіпертекст (hypertext) – це електронний текст, що містить у своїй структурі посилання на адреси інших файлів.

Головна сторінка (home page) – це початкова (титульна) сторінка web-сайта.

Дизайн (design) – зовнішній вигляд чогось: сайту, логотипу, листівки...

Домен, доменне ім'я (domen) – це літерне (літерно-цифрове) позначення сайту, тобто його ім'я.

Електронна пошта (Electronic Mail, E-mail) – це канал передачі текстових повідомлень і вкладених файлів між двома підключеними до Інтернету комп'ютерами.

Інтернет (Internet) – це складна електронна інформаційна структура, що представляє собою глобальну мережу, яка може пов'язувати між собою комп'ютери, розташовані в будь-якій точці Земної кулі, і здійснювати між ними обмін інформацією.

Інтернет-магазин – це складна автоматизована електронна система, призначена для реалізації товарів і послуг комерційних підприємств із застосуванням мережевих технологій.

Інтернет-сторінка – це документ особливої структури, створений спеціально для перегляду в Інтернеті.

Кеш (cache) – це системна папка, в яку комп'ютер записує всі документи, отримані користувачем з мережі.

Клік (click) – це натиснення на якийсь об'єкт на інтернет-сторінці, що містить посилання на картинку, банер, текст.

Контент (content) – це зміст. Під даним терміном частіше усього розуміється змістовне наповнення електронних ресурсів, наприклад, web-сайтів.

Партнерська програма – це спеціальна схема отримання фінансового прибутку в Інтернеті, відповідно до якої учаснику платять за кожного унікального відвідувача, що прийшов на

сайт рекламодавця з рекламного банера, розміщеного на сторінці учасника.

Підтримка web–сайту – це спеціальний комплекс процедур, що забезпечують працездатність ресурсу Інтернету.

Портал (portal) – це Інтернет–сайт, що надає максимально широкий спектр послуг, які відповідають потребам середньостатистичного користувача мережі.

Просування сайту – це дії, спрямовані на залучення відвідувачів на сайт і на просування його до вершин пошукових систем.

Розсилка – це розсилання багатьом користувачам певної інформації, яка їх зацікавить.

Рунет – це російський Інтернет, тобто всі сайти перебувають на російській зоні Інтернету.

Сайт (site) – це сукупність логічно зв'язаних web-сторінок, розміщених, як правило, на одному комп'ютері.

Сервер (server) – це комп'ютер, який надає свої ресурси іншим комп'ютерам мережі, або програма, що обслуговує запити на доступ до ресурсів свого комп'ютера.

Серфінг (serfing) – це перегляд інтернет - сторінок.

Спам (spam) – це незаконне розсилання листів, оголошень без погодження з власником поштової скриньки чи сайту.

Трафік (traffic) – 1. Потік повідомлень або об’єм переданої інформації. 2. Кількість відвідувачів web-сайту або будь-якої його сторінки за одиницю часу (день, місяць, рік).

Форум (forum) – це такий модуль для спілкування, де можна створювати теми, задавати питання і чекати від інших користувачів відповідей.

Хіт (від англ. hit – натиснення) – це одне відвідування будь-якої сторінки web-сайту.

Хост – це будь-який підключений до Інтернету комп’ютер, незалежно від його призначення.

Хостинг (hosting) – це послуга виділення місця на сервері для розміщення свого сайту.

Чат (chat) – це модуль для спілкування в реальному часі. Може бути у вигляді програмного забезпечення, або Інтернет-сайту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Класифікація комп'ютерних злочинів по кодифікатору Генерального Секретаріату Інтерполу [Електронний ресурс]. – Режим доступу: http://www.cyberpol.ru/cybercrime.shtml

2. Конвенція Ради Європи про злочинність у сфері комп'ютерної інформації ETS № 185, ратифіковано Верховною Радою України із застереженнями і заявами Законом N 2824-IV (2824-15) від 07.09.2005, ВВР, 2006, N 5-6, ст. 71.

3. Уголовный кодекс Российской Федерации / Авт.-сост. Коммент. Д. А. Гайдуков, С. А. Перчаткина. – М. : Эксмо, 2009. – 336 с.

4. Уголовный кодекс Республики Польша / Науч. ред. А. И. Лукашова, Н. Ф. Кузнецовой; Пер. с польск. Д. А. Барилович. – СПб. : Юридический центр Пресс, 2001. – 234 с.

5. Кримінальний кодекс України за станом на 05.07.2012 року // Відомості Верховної Ради України. – 2001.

6. Уголовный кодекс Федеративной Республики Германии / Науч. ред. и вступ. статья Д. А. Шестакова; предисл. доктора права Г. Г. Йешека; перевод с нем. Н. С. Рачковой. – СПб. : Юридический центр Пресс, 2003. – 524 с.

7. 15-й, 17-й, 18-й, 42-й, 47-й зводи законів США // Современное право средств массовой информации в США. - М. - 2000. - С. 205-223.

8. Розділ статистичних досліджень організації Nua Internet Surveys [Електронний ресурс]. – Режим доступу: http://www.virtualref.com/subj/101.htm

9. Закон України «Про основи національної безпеки України» зі змінами та доповненнями – Відомості Верховної Ради України (ВВР), 2003, N 39, ст. 351.

10. Гуславский В. С., Задорожний Ю. А., Розовский В. Г. Информационно-аналитическое обеспечение раскрытия и расследования преступления // Монография – Луганск, ТОВ «Елтон-2», 2008. – 133 с.

11. Соціальна мережа «Facebook» [Електронний ресурс]. – Режим доступу: http://www.facebook.com

12. Соціальна мережа «Одноклассники» [Електронний ресурс]. – Режим доступу: http://www.odnoklassniki.ru

13. Соціальна мережа «Вконтакте» [Електронний ресурс]. – Режим доступу: http://www.vk.com

14. Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ // Монографія / Д. М. Цехан ; за науковою редакцією О. О. Подобного. – Одеса : Юридична література, 2011. – 216 с.

15. Пошуковий сервіс «Google» [Електронний ресурс]. – Режим доступу: http://www.google.com

16. Пошуковий сервіс «Яндекс» [Електронний ресурс]. – Режим доступу: http://www.yandex.ru

17. Пошуковий сервіс «META» [Електронний ресурс]. – Режим доступу: http://www.meta.ua

18. Пошуковий сервіс «Rambler» [Електронний ресурс]. – Режим доступу: http://www.rambler.ru

19. Пошуковий сервіс «Yahoo!» [Електронний ресурс]. – Режим доступу: http://www.yahoo.com

20. Пошуковий сервіс «Bing» [Електронний ресурс]. – Режим доступу: http://www.bing.com

21. Пошукові оператори «Google» [Електронний ресурс]. – Режим доступу: http://www.googleguide.com/advanced_operators.html

22. Как надо использовать язык поисковых запросов «Google» [Електронний ресурс]. – Режим доступу: http://www.diacr.ru/zametki/20-kak-pravilno-iskat-v-google/kak-pravilno-iskat-v-google.htm

23. Базовые возможности поиска в «Яндекс» [Електронний ресурс]. – Режим доступу: http://help.yandex.ru/search

24. Расширенные возможности поиска в «Яндекс» [Електронний ресурс]. – Режим доступу: http://help.yandex.ru/search/?id=481920

25. Сервіс пошуку файлів на FTP-серверах «FileSearch» [Електронний ресурс]. – Режим доступу: http://www.filesearch.ru

26. Сервіс пошуку файлів на FTP-серверах «МАМОНТ» [Електронний ресурс]. – Режим доступу: http://www.mmnt.ru

27. Менеджер завантажень файлів «Download Master» [Електронний ресурс]. – Режим доступу: http://www.westbyte.com/dm

28. Пошуковий сервіс «Google Images» [Електронний ресурс]. – Режим доступу: https://www.google.com.ua/imghp

29. Пошуковий сервіс «Яндекс Картинки» [Електронний ресурс]. – Режим доступу: http://images.yandex.ua

30. Пошуковий сервіс графічних зображень «TinEye Reverse Image Search» [Електронний ресурс]. – Режим доступу: http://www. tineye.com

31. Пошуковий сервіс графічних зображень «GazoPa similar image search» [Електронний ресурс]. – Режим доступу: http://www.gazopa.com

32. Офіційний сайт «Internet Assigned Numbers Authority» (IANA) [Електронний ресурс]. – Режим доступу: http://www.iana.org

33. Сервіс ідентифікації користувача за IP адресою «WHOIS» Інтернет–ресурсу «2IP.RU» [Електронний ресурс]. – Режим доступу: http://2ip.ru/whois

34. Кримінальний процесуальний кодекс України. – Х. : Одіссей, 2012.

35. Єдиний реєстр досудових розслідувань України [Електронний ресурс]. – Режим доступу: https://erdr.gp.gov.ua

36. Сторінка завантаження образ диску з операційною системою «Lubuntu» [Електронний ресурс]. – Режим доступу: http://www.lubuntu.ru/download

37. Інтернет ресурс присвячений створенню збірки загрузочної операційної системи «BartPE» [Електронний ресурс]. – Режим доступу: http://www.bartpe.ru

38. Доповнення для загрузочної операційної системи «BartPE», яке дозволяє змінювати чи відключати паролі користувачів в операційних системах [Електронний ресурс]. – Режим доступу: http://www.kood.org/windows-password-renew.

39. Зацеркляний М.М. Інформаційні системи і технології в діяльності правоохоронних органів: навч.посіб. / Зацеркляний М.М., Наумов В.В. – Харків: Тимченко, 2010. – 382 с. з іл.

40. Афанасьев В. Г. Социальная информация и управление обществом / В. Г. Афанасьев. — М.: Политиздат, 1975. — 408 с.

41. Венгеров А. Б. Категория «информация» в понятийном аппарате юридической науки / А. Б. Венгеров // Советское государство и право. - 1977. - № 10. - С. 70-78.

42. Кудрявцев Ю. В. Ценность правовой информации / Ю. В. Кудрявцев // Известия высш. учеб. заведений. — 1977. — № 1. — С. 45—51. — (Сер. : Правоведение).;

43. Информация и оперативно-розыскная деятельность : монография / А. С. Овчинский ; [под ред. В. И. Попова]. — М.: ИНРФА-М, 2002. — 97 с.;

44. Горбачов А. Електронна інформація як доказ при розслідуванні злочинів у сфері комп'ютерних технологій / А. Горбачев // Компьютерная преступность и кибертерроризм : сб. науч. ст. — Запорожье, 2005. — Вып. 3. — С. 157.

45. Айламазян А. К. Информатика и теория развития / А. К. Айламазян, Е. В. Стась. — М.: Наука, 1989. — С. 31.

46. Головчик В. Я. Історія ОРД // Актуальні проблеми сучасної науки і правоохоронної діяльності: Матеріали XI науково-практичної конференції курсантів та слухачів, 29 травня 2004 р. - Харків: Вид-во Нац. ун-ту внутр. справ, 2004. - 276 с.

47. Ищенко Е. П. Новые информационные технологии обеспечения раскрытия и расследования преступлений / Е. П. Ищенко // Вісник ЛДУВС. - 2010. - № 1, спец. вип. № 2. - С. 3-14.

48. Кримінальний кодекс України. Кримінальний процесуальний кодекс України. – К.: Юрінком Інтер, 2012. – 608 с.

49. «Про оперативно-розшукову діяльність» [Електронний ресурс] : закон України від 18.01.2006 р. № 2135-XI1 в редакції Закону України від 01.01.2011 р. № 2756-17. — Електрон, дан. (1 файл). — Режим доступу : http://zakon1.rada.gov.ua — Назва з екрана.

50. Жукова Е. А. Hi-Tech : феномен, функции, формы / Е. А. Жукова ; [под ред. И. В. Мелик-Гайказян]. — Томск : ТГПУ, 2007. — 367 с.

51. Румянцева Е. Л. Информационные технологии : учеб. пособ. / Е. Л. Румянцева, В. В. Слюсарь; [под. ред. Л. Г. Гагариной]. — М.: Форум : Инфра-М, 2007. — С. 15.

52. І. О. Борозенний, О. О. Юхно Особливості використання мережі Інтернет та автоматизованих інформаційно-пошукових систем для забезпечення проведення негласних слідчих (розшукових) дій // Право і Безпека : науковий журнал, № 4 (46) за 2012 рік, - Харківський національний університет внутрішніх справ : видавництво ХНУВС, 2012. – 360 с.

53. Таненбаум Э. Архитектура компьютера. 5-е изд. (+CD). — СПб.: Питер, 2007. — 844 с: ил.

54. Организация ЭВМ. 5-е изд. / К Хдоэхор. З. Вранешич. С. Зэки. — СПб.-Питер; Киев. Издательская группа BHV. 2003. — 848 с.: ил. — (Серия «Классика computer science»).

57. Кримінологія. (Загальна частина): Підручник / Кол. авторів Блага А. Б., Богатирьов І. Г., Давиденко Л. М. та ін.; за заг. ред. О.М. Бандурки. − Харків: Вид-во ХНУВС, 2010. − 280 с.

58. Кримінальний кодекс України (із змінами та доповненнями станом на 1 січня 2013 року). – Х. : Одіссей, 2013. – 232 с.

59. Захарченко В.Ю., Лазуренко В. И., Олифиров А. В . , Рогозин С.Н. Компьютерные преступления: их выявление и предотвращение: Учебное пособие / Под общ. редакцией В. И. Лазуренко. – К.: Центр учебной литературы, 2007. – 170 с.

60. Кіберзлочинність в Україні: перспективи протидії [Електронний ресурс]. / Комітет протидії корупції та організованої злочинності. – Режим доступу: http://kpk.org.ua/2007/02/05/ kberzlochinnst_v_ukran_perspektivi_protid.html.

61. Словарь криминологических и статистических терминов / А. Г. Кальман, И. А. Христич. – Х. : Гимназия : Ин-т изучения проблем преступности АПрН Украины, 2001. – 94 с.

62. Категорія: кіберзлочинність. [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/ категорія: кіберзлочинність.

63. Компьютерные преступления их предупреждение и выявление : Учеб. пособие. – К. : Центр учеб. лит., 2007. – 170 с.

64. Голубєв, В. Суб'єкт злочинної діяльності у сфері використання електронно-обчислювальних машин // Підприємництво, господарство і право . – 2004 . – № 6. – С. 109–112.

65. Типология и классификация в социологических исследованиях. / В. Г. Андреенков, Ю. Н. Толстова; Институт социологических исследований (Академия наук СССР) – М, 1982. – 295 с.

66. Голубев В. А., Головин А. Ю. Проблемы расследования преступлений в сфере использования компьютерных технологий. [Электронный ресурс]. – Режим доступа: www.crime–research.ru.

67. Голубев В. О. Розслідування комп'ютерних злочинів: Монографія. – Запоріжжя, 2003. – С. 82–92.

68. Комп'ютерна злочинність: Навч. посібник / П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін. – К. : 2002. – 240 с.

69. Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора // Группа экспертов для проведения всестороннего исследования киберпреступности Вена, 25–28 февраля 2013 года : [Электронный ресурс] / UNODC/CCPCJ/EG.4.– 2013. – 21 с. – Режим доступа. : http://www.unodc.org/documents/organized–crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf

70. Конвенція про кіберзлочинність від 23 листоп. 2001 р. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_575.

71. Войціховський А.В. Міжнародне співробітництво в боротьбі з кіберзлочинністю / А.В. Войціховський / Науковий журнал «Право і Безпека». – 2011. – №4. [Електронний ресурс]. – Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/pib/2011_4/PB–4/PB–4_26.pdf

72. Селико Ю. Internet – отмычка для компьютера / Ю. Селико, А. Прохоров // Комп’ютер-пресс. –2002. –№3.–С. 40–43.

73. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно–правовые меры борьбы /Т. Л. Тропина // Владивосто-

кский центр исследования киберпреступности. – 2007. [Электронный ресурс]. – Режим доступа: http://www.crime.vl.ru/ index.php?p= 3626&more=1&c=1&tb=1&pb=1

74. Бутузов В.М. До питання специфіки протидії комп'ютерній злочинності // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2008. – № 18. – С. 38–47.

75. Про ратифікацію Конвенції про кіберзлочинність : закон України від 7 верес. 2005 р. № 2824–IV // Відомості Верховної Ради України. – 2006. – №5–6. – Ст. 71.

76. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [Електронний ресурс]. – Режим доступу: http://www. zakon1.rada.gov.ua/cgi–bin/laws/main.cgi?=nreg=994_687.

77. Одиннадцатый Конгресс ООН по предупреждению преступности и уголовному правосудию [Электронный ресурс]. – Режим доступа: http://www.un.org/russian/events/ 11thcongress/ index.html.

78. Двенадцатый Конгресс ООН по предупреждению преступности и уголовному правосудию [Электронный ресурс]. – Режим доступа: http://www.un.org/ru/conf/crimecongress2010.

79. Агентства ООН объединились против киберпреступности [Электронный ресурс]. – Режим доступа: http://www.unmultimedia.org/radio/russian/detail/84626.html.

80. Стратегія національної безпеки України [Електронний ресурс] : указ Президента України від 12 лют. 2007 р. № 105/2007. – Режим доступу: http://zakon1.rada.gov.ua/ laws/show/105/2007.

81. Вехов В. Б. Компьютерные преступления, способы совершения методики расследования / Вехов В. Б. – М., 1996. – 182с.

82. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27.09.1999 № 1229/99 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1229/99. – Редакція від 04.05.2008.