МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ГУНП УКРАЇНИ В ДНІПРОПЕТРОВСЬКІЙ ОБЛАСТІ

В.Г. Телійчук, Д.Б. Санакоєв, О.В. Козорог, Я.М. Ковч

АЛГОРИТМ ДІЙ ПРАЦІВНИКІВ ПІДРОЗДІЛІВ КАРНОГО РОЗШУКУ ПІД ЧАС РОЗКРИТТЯ ШАХРАЙСТВ, ВЧИНЕНИХ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ

Методичні рекомендації

Дніпро – 2018

Схвалено Науково-методичною радою
Дніпропетровського державного університету
внутрішніх справ, протокол від 19.04.2018 № 8.

Рецензенти:

Вишня В.Б. – доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, доктор технічних наук, професор;

Кирбят'єв О.О. – інспектор відділу протидії кіберзлочинам в Запорізькій області Придніпровського управління кіберполіції Департаменту кіберполіції Національної поліції України, підполковник поліції, кандидат юридичних наук.

Алгоритм дій працівників підрозділів карного розшуку під час розкриття шахрайств, вчинених через мережу Інтернет: методичні рекомендації / В.Г. Телійчук, Д.Б. Санакоєв, Я.М. Ковч, О.В. Козорог. – Дніпро : Дніпропетровський державний університет внутрішніх справ, 2018. – 55 с.

У методичних рекомендаціях надана оперативно-розшукова та криміналістична характеристика Інтернет-шахрайств, визначені основні напрями виявлення та оперативно-розшукового запобігання, а також запропоновано типові алгоритми дій працівників підрозділів карного розшуку щодо розкриття цих злочинів у процесі досудового розслідування та здійснення оперативного супроводження кримінального провадження.

Методичні рекомендації розраховані для використання у практичній діяльності підрозділів карного розшуку, а також наукових працівників, які досліджують проблеми протидії умисним вбивствам.

ЗМІСТ

Перелік умовних скорочень

ДБО	- дистанційне банківське обслуговування
ЕОМ	– електронна обчислювальна машина, комп’ютер
ЕЦП	- електронний цифровий підпис
ЕМА	- Українська міжбанківська асоціація членів платіжних систем «ЄМА»
ЄРДР	– Єдиний реєстр досудових розслідувань
КПК України	– Кримінальний процесуальний кодекс України
КП	– кримінальна поліція
КР (КР)	– карний розшук
МВС України	– Міністерство внутрішніх справ України
НПУ, НП України	– Національна поліція України
НСРД	- негласні слідчі (розшукові) дії
ОНП	– органи Національної поліції України
ООН	– Організація Об’єднаних Націй
ОТЗ	– оперативно-технічні заходи
ПЗ	– програмне забезпечення
ПОТЗ	– підрозділи оперативно-технічних заходів
СОГ	– слідчо-оперативна група
УЗЕ	- управління захисту економіки

Вступ

Актуальність розробки методичних рекомендацій визначається стрімким розвитком нового виду протиправної діяльності – транснаціональних злочинів у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, різким підвищенням кримінального комп'ютерного професіоналізму, активної міграції злочинців і організованістю їх дій, що суттєво ускладнює криміногенну обстановку і є складним феноменом, що вимагає інтеграції багатьох галузей знань і, зокрема, юридичної науки для поглибленого дослідження природи цих злочинів, особливостей їх оперативно-розшукової та криміналістичної характеристик, тактики виявлення і запобігання з урахуванням сучасних досягнень вітчизняної й зарубіжної теорії та практики оперативно-розшукової діяльності, кримінального процесу та криміналістики.

З часу набрання чинності КПК України (2012), кожен службовий персональний комп'ютер (ПК) 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, у т.ч. й негласних. Зростання кількості ПК та користувачів мережі Інтернет впливає на кількість злочинів, що дедалі частіше вчиняються із використанням інформаційних технологій. Так, згідно з даними Української міжбанківської асоціації членів платіжних систем ЕМА, у 2016 році кожен сотий власник платіжної картки в Україні став жертвою шахраїв. Внаслідок вішингу (телефонне шахрайство з виманюванням реквізитів банківських карток і переказом коштів на карту злодіїв) з рахунків українців було вкрадено 275,45 млн. грн., а внаслідок фішингу (виманювання конфіденційних даних – паролів, номерів банківських карток, PIN-кодів тощо) – 63,68 млн. грн. Загалом – 339,13 млн. грн. Для порівняння, у 2015 році шахраї викрали з рахунків українців 84,36 млн. грн. Як зазначають аналітики, рекордно зросла кількість фішингових сайтів (в 4,5 рази – з

38 до 174), а, в цілому, від фішингу та інших видів шахрайства в Інтернеті постраждало 0,59% клієнтів-власників банківських карт. Жертвами телефонного шахрайства стали 0,63% власників карт. За даними ЕМА, з 1 серпня по 26 вересня 2017 року кількість шахрайських операцій за картами досягла 1 928. Сума, яку зловмисникам вдалося вкрасти з рахунків менш ніж за два місяці, оцінюється приблизно в 238 млн. грн. І це при тому, що за весь 2016 рік злочинці вкрали з карток українців 340 млн. грн. У зв'язку з цим в системі НПУкраїни створено спеціальні підрозділи щодо протидії 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, захопленням повітряних суден, морським піратством, заволодінням наземного транспорту, шахрайством, 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, у т.ч. й дошкільного віку, то в діяльності правоохоронних органів і, зокрема Національної поліції, у зв'язку з обмеженням фінансування, їх застосування та вирішення питань ліцензування, здійснюється досить повільно. В той же час автори методичних рекомендацій, 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 кримінальної поліції (карного розшуку) та досудового розслідування НП України, 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. Вказане дозволить продовжити дослідження не тільки з технічних, але й правових питань, по розширенню можливостей, напрацюванню пропозицій та рекомендацій щодо удосконалення кримінального процесуального і кримінального законодавства України. Нагальність вказаних проблем сьогодні досить гостро відчувають як вчені, так і оперативні працівники, слідчі, процесуальні керівники та представники інших правоохоронних органів.

Методичні рекомендації виконані на замовлення, що надійшло згідно листа ГУНП в Дніпропетровській області від 27.07.2017 № 5281/Гр, а також виконано у відповідності з п. 2.7 Плану науково-дослідних та дослідно-конструкторських робіт ДДУВС на 2018 рік, розраховані передусім для працівників карного розшуку, проте можуть використовуватись у навчальному процесі для курсантів, студентів, слухачів, ад'юнктів, аспірантів, викладачів, а також всіх, хто цікавиться вказаною проблематикою.

І.ОСНОВНІ ВИДИ ТА СПОСОБИ ВЧИНЕННЯ ШАХРАЙСТВ, УЧИНЕНИХ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ

На сьогодні проблема інтернет-шахрайства надзвичайно актуальна, особливо гостро вона стоїть у банківській та фінансовій сферах, телекомунікаціях, рітейлі, електронній торгівлі. Організації, що працюють у вказаних сегментах ринку, регулярно стикаються зі спробами так званих кібершахраїв незаконно отримати товари чи послуги. Окрім того, від віртуальних злочинців доволі часто страждають клієнти банків та платіжних систем, користувачі телефонних мереж та Інтернету, сервісів електронної та мобільної комерції.

Вказана категорія злочинів становить підвищену суспільну небезпеку, оскільки злочини завдають невідворотної шкоди економічній та інформаційній безпеці держави.

Інформаційно-аналітичні матеріали про результати правоохоронної діяльності в Україні свідчать про активізацію роботи з попередження, припинення і розслідування шахрайств, вчинених із використанням сучасних інформаційних технологій. Привертає на себе увагу значне зростання цієї категорії кримінальних проваджень, що знаходяться у провадженні органів досудового розслідування НП України.

Основними видами злочинів цього виду є: шахрайство у мережі Інтернет (хибні пропозиції товарів та послуг через мережу інтернет-магазинів та інтернет-аукціонів, фінансові інтернет-афери, «нігерійські листи»), шахрайство з кредитними картками (кардінг) та в системах дистанційного банківського обслуговування, телефонні шахрайства.

Окрім того, на низькому рівні перебуває робота з організації, методичного забезпечення та формування правозастосовної практики з виявлення і розслідування шахрайства, вчиненого з використанням сучасних інформаційних технологій.

Розслідування більшості видів високотехнологічних шахрайств ускладнено тим, що якісні характеристики мережі Інтернет дають можливість злочинним елементам використовувати сервери, що знаходяться поза юрисдикцією України, для приховування фактів своєї злочинної діяльності.

Від способу вчинення конкретного злочину залежать хід розслідування, ступінь організованості взаємодії, алгоритм та черговість проведення слідчих (розшукових) дій, у т.ч. негласних.

Беручи до уваги практику виявлення та розслідування фактів інтернет-шахрайства, нами виокремлено такі типові способи:

Спосіб № 1. Знайомства по Інтернет, реалізовані шахраями через сайти знайомств і електронну пошту (наприклад, представляючись молодими жінками і залучаючи потенційних жертв до особистого спілкування, шахраї просять перевести грошові кошти для поїздки до останнього. Жертва переводить кошти на вказаний рахунок. Переказ коштів здійснюється з використанням так званих «грошових мулів» або «фінансових агентів». При отриманні грошових коштів шахраї видаляють обліковий запис з сайту знайомств. «Грошові мули» чи «фінансові агенти» - це так звані грошові кур'єри, які формують основу для передачі злочинних доходів від жертви злочинцю. Їх основна роль – відкрити рахунок або надати дані про свій вже відкритий рахунок. Після отримання коштів на свій рахунок їх надаються інструкції про переказ цих коштів на інший рахунок чи за кордон, використовуючи електронний переказ і, як наслідок, полегшуючи відмивання коштів, утримуючи при цьому комісію).

Спосіб № 2. Соціальний інжиніринг (метод проникнення у захищені системи, заснований на використанні соціальної психології) використовується із застосуванням комп'ютера або телефону для отримання доступу до рахунку або полегшення такого доступу або отримання цінної інформації (адреса електронної пошти особи) для цілеспрямованої крадіжки персональних даних (*наприклад, 1) особа має умисел на вчинення розкрадання, в рамках його реалізації здійснює дзвінок по телефону співробітнику компанії під виглядом представника служби технічної підтримки з метою отримання індивідуального пароля, необхідного*

«для вирішення проблеми в комп'ютерній системі співробітника»; 2) особа, яка має намір на вчинення розкрадання, під виглядом службовця компанії здійснює телефонний дзвінок в службу технічної підтримки, орієнтованої на невідкладну допомогу співробітникам організації, представляючись службовцем, посилаючись на те, що забув пароль, отримує індивідуальний пароль особи, від імені якої здійснив дзвінок, змінює його на свій, отримуючи доступ до інформації; 3) на телефон абонента надходить SMS-повідомлення, що містить відомості про взяті і непогашені кредити, через місяць на цей же номер телефону здійснюється дзвінок особою, яка представляється оператором служби технічної підтримки банку, в телефонній розмові з'ясовує П.І.Б. абонента, наявність у нього банківської пластикою карти (БПК), її номер. Отриманої інформації достатньо для розкрадання грошових коштів з рахунку БПК шляхом здійснення покупки в інтернет-магазині від імені особи, дані якої використовує шахрай).

Спосіб № 3. Фішинг – вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів - логінів і паролей. Це досягається шляхом проведення масових розсилок електронних листів від імені популярних брендів, а також особистих повідомлень всередині різних сервісів, наприклад, від імені банків (Приватбанк, Укрсоцбанк), сервісів (Rambler, Mail.ru, Gmail) або всередині соціальних мереж (Facebook, Instagram, Telegram). У листі часто міститься пряме посилання на сайт, зовні тотожній справжньому або на сайт з редіректом (автоматичне (примусове) перенаправлення користувача з однієї веб-адреси на іншу (сторінка-перенаправлення). Після потрапляння користувача на підроблену сторінку, шахраї намагаються різними психологічними прийомами спонукати користувача ввести на підробленій сторінці свої логін і пароль, які він використовує для доступу до певного сайту, що дозволяє шахраям отримати доступ до акаунтів і банківських рахунків (*наприклад, на електронну поштову скриньку спрямовується електронний лист від імені банку, що містить недостовірну інформацію про оновлення клієнтської бази, для чого необхідно перейти за посиланням, запропонованим у листі, на сайт банку, залишити в*

запропонованій на сайті формі особисті дані (П.І.Б.), номер БПК, термін її дії. Насправді користувач електронної пошти, скориставшись посиланням, запропонованим в електронному листі, переадресовується на так званий сайт-«двійник», а надані їм дані виявляються у розпорядженні шахраїв, які згодом, користуючись ними, здійснюють розкрадання грошових коштів з рахунку БПК).

Спосіб № 4. Поширення шкідливого програмного забезпечення (ПЗ), що блокує можливість користування комп'ютером або робить його використання «некомфортним» (половина екрана закрита зображенням з вимогою відправити SMS на короткий номер). Для розблокування комп'ютера необхідно отримати код, надіславши платне SMS за вказаним номером, однак відправка SMS на платний номер не гарантує розблокування комп'ютера.

Спосіб № 5. Пропозиція явно неіснуючої послуги або методики (генератора електронних коштів, поповнення так званих гаманців з електронними грошима, ставки на спорт).

Спосіб № 6. Розсилка різного роду електронних листів на електронні поштові скриньки, текст яких вводить в оману одержувача, акцентує увагу останнього на необхідності певного роду платежів.

Спосіб № 7. Кардінг. Цей вид шахрайства в Інтернет пов'язаний з банківськими картами. Для цих цілей використовують фіктивні інтернет-магазини, де передбачена оплата банківськими картами. Злочинні елементи, отримавши доступ до чужої банківської пластикової картки, переводять у готівку гроші.

Спосіб № 8. Скандинавські аукціони. На інтернет-аукціоні виставляється товар за значно заниженою ціною (2-3 гривні тощо), учасники роблять мінімальні ставки, і за кожну ставку з них знімається певна сума.

Наведені вище способи знайшли найбільшу частоту відображення у судовій і слідчій практиці, проте зазначимо, що їх перелік не є вичерпним і може бути розширений.

Приводом для початку кримінального провадження є заява фізичної особи або уповноваженого представника юридичної особи про відомі їй факти

розкрадання грошових коштів, а також інформація, отримана при проведенні НСРД співробітниками поліції.

Обставини, що підлягають встановленню:

1. Факт неправомірного доступу до інформації в комп'ютерній системі або мережі.

2. Місце несанкціонованого проникнення в комп'ютерну систему або мережу, IP-адреса комп'ютера, з якого відбувався запуск шкідливого ПЗ.

3. Час вчинення злочину.

4. Надійність засобів захисту комп'ютерної інформації (наявність пароля, шифрування і т.п.).

5. Спосіб несанкціонованого доступу.

6. Особи, які вчинили неправомірний доступ, їх винність і мотив злочину.

7. Наявність і розмір збитків, заподіяних злочином.

8. Обставини, що сприяли злочину.

ІІ. ТИПОВІ ДІЇ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ (КАРНОГО РОЗШУКУ) ПРИ ВИКОРИСТАННІ ОСНОВНИХ МЕТОДІВ ПОШУКУ ЦИФРОВИХ ЗОБРАЖЕНЬ В МЕРЕЖІ ІНТЕРНЕТ

Вже зазначалось, що велику групу злочинів складають *шахрайства, вчинені з використанням сучасних інформаційних технологій та мережі Інтернет.* Такі шахрайства вчиняються із 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 *кримінальної поліції (карного розшуку)* 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 *карного розшуку* 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» чи «Яндекс Картинки»;

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», чи «GazoPa similar image search»;

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»;

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», 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»;

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» – 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», 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.

ІІІ. ТИПОВІ ДІЇ ПРАЦІВНИКІВ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ (КАРНОГО РОЗШУКУ) ПІД ЧАС ПОШУКУ ІНФОРМАЦІЇ ПРО ОСОБУ

Основні способи 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 КП (КР) 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». 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.

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

Григорій 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 карного розшуку 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 про-дати», 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.

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 «OKT» - 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 створеним, 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 відлякати від нього, та навіть змусити 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 **карного розшуку** 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 натиснути 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 даному випадку – до якої фізичної адреси відноситься IP-адреса 178.151.128.221;

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

6) аналіз отриманих результатів.

IV. ТИПОВИЙ АЛГОРИТМ ДІЙ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ (КАРНОГО РОЗШУКУ) НА ПОЧАТКОВОМУ ЕТАПІ ДОСУДОВОГО РОЗСЛІДУВАННЯ

Особливості тактики провадження окремих слідчих (розшукових) дій

У ході здійснення досудового розслідування у кримінальному провадженні необхідно:

1) сформувати слідчо-оперативну групу (СОГ) з урахуванням специфіки даної категорії злочинів (слідчий, співробітники, які здійснюватимуть оперативне супроводження, фахівець по роботі з радіоелектронними засобами і спеціальними технічними засобами, співробітник територіального підрозділу ОТЗ НП України, фаховий співробітник Управління кіберзлочинності НП України);

2) визначити послідовність і черговість проведення слідчих (розшукових) та інших процесуальних дій, скласти узгоджений план всіх заходів. Так, кожна конкретна слідча (розшукова) дія має бути завчасно підготовлена і детально спланована, визначене коло учасників її реалізації;

3) залучити в якості понятих осіб, що володіють знаннями у сфері комп’ютерної інформації.

Встановлення місця злочину, фактичної адреси, де встановлена комп'ютерна техніка, що використовує відповідну IP-адресу. З цією метою необхідно встановити інтернет-провайдера, якому належить шукана IP-адреса, після чого направити йому відповідний запит. Як тексту запиту можна навести такий приклад: *«Прошу Вас надати інформацію по IP-адресою ..., а саме фактична адреса розташування клієнта даної IP-адреси, з зазначенням особи, яка уклала договір надання послуг щодо надання доступу в Інтернет з Вашою організацією. Якщо особа, що уклала договір, орендувало простір на Вашому сервері, прошу вказати це у відповіді. Додатково прошу повідомити наявні дані по з'єднаннях із вказаної IP-адреси за протоколами POP3 / SMTP, HTTP за період ...»*.

У ряді випадків злочинці використовують сервери, орендовані за межами України. Встановлюється інтернет-провайдер, якому належить шукана IP-адреса, його фактичне місце розташування і у відповідну державу надсилається міжнародний запит про надання інформації. Текст запиту, фабула кримінального провадження, а також копії матеріалів, що свідчать про належність IP-адреси інтернет-провайдеру, перекладаються на офіційну мову держави-одержувача міжнародного запиту.

Фактичне встановлення місця, звідки здійснювалося розкрадання з використанням сучасних інформаційних технологій за отриманою від провайдера адресою.

Якщо в ході розслідування буде встановлено, що кілька організацій мають одну IP-адресу, слід враховувати, що дані організації можуть бути сумлінними, незалежно один від одного здійснювати реальну фінансово-господарську діяльність. Наявність у них однієї IP-адреси може пояснюватися, наприклад, знаходженням їх офісів в бізнес-центрі або іншому орендованому ними приміщенні, власник якого може надавати їм доступ в Інтернет зі своєї IP-адреси.

При **огляді місця події** до складу СОГ залежно від конкретної слідчої ситуації, крім слідчого, можуть входити: спеціаліст-криміналіст, що знає особливості роботи зі слідами за злочинами даної категорії; фахівець в області комп’ютерної техніки (фахівець з мережних технологій); оперативні співробітники (ПОТЗ або УЗЕ); дільничний інспектор поліції, який обслуговує цю територію; інспектор відділу позавідомчої охорони (у разі, коли місце події або засоби обчислювальної техніки одночасно є об'єктами охорони).

При необхідності до огляду місця події до складу СОГ можуть бути залучені незацікавлені в справі фахівці, які знають специфіку роботи об'єкта, що оглядається (інженери-електрики, бухгалтери зі знанням засобів обчислювальної техніки, спеціалісти супутникових систем зв'язку, оператори комп'ютерних систем і мереж електрозв’язку та ін.).

Метою огляду місця події є встановлення конкретного засобу обчислювальної техніки (комп’ютера), накопичувача на жорстких магнітних дисках (НЖМД), що виступає в якості предмета і (або) знаряддя вчинення злочину і містить сліди злочинної діяльності. При проведенні слідчої (розшукової) дії доцільніше використовувати тактичний прийом «від центру – до периферії», де в якості «центру» (відправної точки огляду місця події) буде виступати конкретний засіб обчислювальної техніки. Детальний опис всіх комп'ютерних засобів, їх з’єднань (фізичних і логічних) має супроводжуватися (фото-) відеозйомкою, що фіксує послідовність дій слідчого і фахівців, а також отриманий при цьому результат.

Якщо при проведенні даної слідчої (розшукової) дії відсутні фахівці, комп'ютер включений і виникають сумніви в збереженні наявної на ньому інформації, доцільно його відключити (в тому числі і шляхом відключення від електричної мережі), не дотримуючись встановленого операційною системою порядку.

Якщо при проведенні огляду місця події використовуються засоби обчислювальної техніки (зовнішній накопичувач на жорстких магнітних дисках тощо), про це робиться відповідна відмітка в протоколі слідчої (розшукової) дії із зазначенням їх індивідуальних ознак (тип, марка, назва, заводський номер і т.д.).

Оперуповноваженому та слідчому необхідно враховувати, що до зміни або знищення комп'ютерної інформації (слідів злочинця і злочину) може привести не тільки робота за пультом управління засобів обчислювальної техніки (клавіатурою), а й одноразове короткочасне включення-виключення засобів обчислювальної техніки або розрив з'єднання між ними. Тому до початку проведення слідчої (розшукової) дії необхідно проконсультуватися з фахівцями і визначити доцільність знеструмлення засобів комп'ютерної техніки. Якщо на момент проведення слідчої (розшукової) дії будь-які засоби обчислювальної техніки і інші електротехнічні прилади та обладнання були включені або виключені, то вони повинні залишатися в такому положенні до моменту

закінчення огляду їх фахівцем. З цієї ж причини підлягають обов'язковій охороні всі пункти відключення електроживлення, що знаходяться на місці події.

У протоколі огляду місця події фіксуються: технічні і конструктивні особливості, пов'язані з установкою і експлуатацією засобів обчислювальної техніки, у т.ч. розташування і основні характеристики струмопровідних комунікацій; розташування засобів обчислювальної техніки відносно один одного і кінцевих пристроїв; відсутність або наявність з'єднань між ними (видимих і дистанційних); наявність або відсутність з'єднань засобів обчислювальної техніки з обладнанням, у т.ч. що знаходиться поза територією огляду (на це можуть вказувати кабелі та проводи, що йдуть від засобу обчислювальної техніки, що оглядається, за межі місця огляду або до апаратів електрозв'язку (в такому випадку межі огляду місця події значно розширюються); наявність, зовнішній стан, розташування і вид охорони засобів обчислювальної техніки і комп'ютерної інформації від несанкціонованого доступу, їх основні технічні характеристики; розташування засобів обчислювальної техніки щодо дверей та вікон, технічних засобів відеоспостереження, а також щодо інших робочих місць; наявність в одному приміщенні з засобами обчислювальної техніки інших електричних пристроїв і приладів (телефонів і інших апаратів електрозв'язку, оргтехніки і т.д.).

Особливо ретельно повинні бути оглянуті та описані в протоколі: наявні машинні носії; виявлені спеціальні технічні засоби негласного отримання (знищення, блокування) комп'ютерної інформації та магнітних носіїв; специфічні сліди злочинця і злочину; показання записуючого устаткування (відеотехніки, електронного журналу обліку операцій з комп'ютерною інформацією, доступу до неї та засоби обчислювальної техніки; показання спеціальних моніторингових (тестових) програмно-апаратних засобів, у т.ч. електронного цифрового підпису; сліди пальців рук на засобах обчислювальної техніки, охоронних і сигнальних пристроях, на їх клавіатурі, сполучних проводах та роз'ємах електроживлення, на розетках і вилках, тумблерах, кнопках і перемикачах, що включають і відключають засоби обчислювальної техніки та електрообладнання; сліди

вдавлення, проплавлення, проколу, надрізу ізоляції струмопровідних і сполучних (керуючих) проводів, приклеювання до них сторонніх предметів і пристроїв).

Якщо на момент огляду місця події комп'ютер знаходиться в робочому стані, необхідно детально описати: розташування його робочих механізмів і зображення на його відеоконтрольному пристрої (екрані, моніторі, дисплеї); основні дії, виконані фахівцем при огляді комп'ютерної техніки (порядок коректного призупинення роботи і закриття виконуваної операції або програми, виключення засобів обчислювальної техніки, відключення від джерела електроживлення, роз'єднання (або з'єднання), від'єднання проводів, результати вимірювання технічних параметрів контрольно-вимірювальної або тестової апаратури і т.п.).

Огляду в організаціях підлягають:

а) обліково-довідкова документація по роботі із засобами обчислювальної техніки та комп'ютерною інформацією (технічний паспорт або документ, що його замінює; журнал оператора або протокол автоматичної фіксації технологічних операцій, доступу до засобу обчислювальної техніки і конфіденційної комп'ютерної інформації; журнали (картки) обліку машинних носіїв інформації, машинних документів, замовлень (завдань або запитів), видачі машинних носіїв інформації і машинних документів, масивів (ділянок, зон), програм, записаних на машинних носіях інформації; журнали обліку знищення дефектів паперових машинних носіїв інформації і машинних документів; акти на стирання конфіденційної інформації та знищення машинних носіїв з нею);

б) документація, що відображає санкціонованість доступу (посвідчення особи, електронні ключі доступу, паролі, персональні ідентифікаційні номери (пін-коди), електронний цифровий підпис та інші засоби (предмети або пристрої) ідентифікації і аутентифікації санкціонованого користувача);

в) обліково-реєстраційна та бухгалтерська документація (ліцензії та ліцензійні угоди; сертифікати відповідності засобів обчислювальної техніки, програм для ЕОМ, засобів захисту інформації (у т.ч. і ЕЦП), протоколів обміну інформацією та форматів електронних документів встановленим вимогам);

договори (угоди) на користування засобами обчислювальної техніки і доступ до комп'ютерної інформації з відповідним комплектом документів; розрахунково-касові та інші бухгалтерські документи, що відображають факт оплати користувачем наданої йому послуги, відпущеного товару або здійсненої ним кредитно-банківської операції);

г) документація, що регламентує дії обслуговуючого персоналу (посадові інструкції по роботі із засобами обчислювальної техніки, програмами для ЕОМ, засобами захисту від несанкціонованого доступу, дій оператора в нештатній (аварійній) ситуації; чорнова робоча документація оператора засобів обчислювальної техніки).

Як правило, наступний огляд вилучених документів, проведений за участю фахівця, дозволяє встановити спосіб вчинення розкрадання із використанням сучасних інформаційних технологій, використані для цього злочинцем матеріали і засоби, наявність у суб'єкта спеціальних навичок і знань.

Огляд комп'ютерної техніки, системного блоку і комп'ютерної інформації, енергонезалежних носіїв інформації, енергозалежних носіїв інформації, мережевого обладнання, серверів, проведений за участю фахівця, в більшості випадків є початковою слідчою (розшуковою) дією і проводиться для виявлення слідів злочину, вирішення питань про те, ким, з якою метою і за яких обставин було скоєно злочин, з'ясування обстановки події, що відбулася, відновлення механізму скоєння злочину. Оглядаються: вміст енергонезалежних носіїв інформації (жорсткі диски, компакт-диски, накопичувачі USB Flash тощо); вміст енергозалежних носіїв інформації (оперативна пам'ять); лог-файли мережевого обладнання, серверів; мережевий трафік.

Огляд машинного носія і комп'ютерної інформації проводять за принципом «від загального до конкретного». Спочатку описують зовнішні індивідуальні ознаки носія: його колір, розмір, тип, вид, назва, марка, заводський і індивідуальний номер, наявність наклейки і написів на ній, наявність або відсутність фізичних пошкоджень корпусу і слідів на ньому, положення елемента

захисту від запису / стирання комп'ютерної інформації. Далі переходять до огляду комп'ютерної інформації, що міститься на машинних носіях інформації.

У протоколі огляду, крім вказаного, необхідно відобразити: наявність, індивідуальні ознаки захисту носія від несанкціонованого використання (голографія, штрих-код, ембоссінг, флуоресціювання, перфорація, ламінування особистого підпису та (або) фотографії власника, їх розміри, колір, вид тощо); внутрішню специфікацію носія – серійний номер і (або) мітку тому.

Обшук. Готуючись до проведення обшуку, необхідно ретельно вивчити обставини провадження і зібрати орієнтовну інформацію про предмет обшуку, місце його проведення. За даної категорією проваджень предметом обшуку можуть бути не тільки різноманітні засоби обчислювальної техніки, машинні носії і відповідна інформація на них, але і документи, засоби електрозв'язку, розроблені і пристосовані спеціальні технічні пристрої, побутові електротехнічні пристрої та обладнання, матеріали та інструменти.

Особливу увагу потрібно приділяти предметам, що містять коди, паролі доступу, ідентифікаційні номери, назви, електронні адреси користувачів конкретних комп'ютерних систем і мереж, алгоритми входу і роботи в системах і мережах.

При проведенні обшуку необхідно залучати працівників ДОТЗ НП України, які здійснюють заходи щодо збереження інформації, що знаходиться на жорстких магнітних дисках; у засобах електронно-обчислювальної техніки; в енергонезалежних носіях інформації, в енергозалежних носіях інформації; в лог-файлах; в мережевому обладнанні; на серверах; в мережевому трафіку.

Так, блокатори запису дозволяють підключити досліджуваний носій інформації без ризику запису на нього будь-яких даних з вини операційної системи або сторонніх програм.

Спеціалізовані операційні системи, як правило, застосовуються для копіювання носіїв інформації без їх вилучення з досліджуваного комп'ютера за рахунок завантаження на його апаратне забезпечення довіреного (криміналістичного) програмного середовища.

Зазвичай такі операційні системи завантажуються з CD або накопичувачів USB Flash і містять програмні блокатори запису, що запускаються в процесі завантаження.

Зазначимо, що копіювання вмісту енергонезалежних носіїв інформації перед дослідженням не є обов'язковим кроком – у випадках, коли забезпечується цілісність вмісту оригінальних носіїв (тобто у випадках справності носіїв і при використанні блокаторів запису), дослідження копій замість оригіналів проводити недоцільно.

Збір енергозалежних даних проводиться із працюючих систем перед їх вимкненням. Як правило, процес збору енергозалежних даних полягає в копіюванні: вмісту оперативної пам'яті комп'ютера; вмісту домонтованих зашифрованих файлових систем і мережних сховищ; списків працюючих процесів і сервісів; списків поточних мережевих з'єднань і відкритих портів; мережевої конфігурації досліджуваної системи; перемінних оточення; зображення, що бачить користувач на екрані монітора (створення знімка екрана).

Для копіювання цих даних до працюючої досліджуваної системи може підключатися зовнішній носій, з якого здійснюється запуск спеціалізованої програми, що збирає дані. Іноді спеціалізована програма завантажується в систему по мережі.

Копіювання логів може здійснюватися кількома способами: копіюванням тільки записів, що мають відношення до злочину (наприклад, що відносяться до певної IP-адреси або проміжку часу); копіюванням лог-файлів повністю; копіюванням усього носія інформації.

Основними факторами при виборі того чи іншого способу копіювання є: ступінь довіри логам і відповідно обсяг дослідження, спрямованого на визначення ступеня коректності і незмінності лог-файлів. Якщо ймовірність зловмисної зміни або фальсифікації лог-файлів низька, то допустимо копіювати тільки лог-файли або окремі їх записи. В іншому випадку доцільно використовувати для копіювання вмісту всього носія інформації (для подальшого пошуку слідів несанкціонованого доступу до системи, слідів модифікації лог-файлів тощо).

Для створення копії (дампа) мережевих пакетів необхідно організувати підключення точки знімання мережевого трафіку в ділянці мережі, який забезпечує збір всіх криміналістично значущих потоків даних. У процесі створення дампа мережевих пакетів необхідно мінімізувати обмін даними між вузлом, який здійснює знімання мережевого трафіку, і вузлами мережі, які стосуються інциденту інформаційної безпеки.

Зазначені дії здійснюються у присутності понятих, яким фахівцями пояснюється алгоритм Ваших дій, їх доцільність, необхідність.

Докази можуть бути виявлені і при особистих обшуках підозрюваних.

Предметом тимчасового доступу (виїмки) в переважній більшості випадків інтернет-шахрайства, є персональні комп'ютери, мобільні телефони, інші машинні носії інформації та різноманітні документи (в т.ч. й електронні), що відображають і регламентують різні операції, технологічні процеси, пов'язані з обробкою, накопиченням, створенням, передачею та захистом комп'ютерної інформації, використання ЕОМ, системи ЕОМ та їх мережі.

Окрім вказаного, можуть бути вилучені спеціальні технічні засоби для негласного отримання, модифікації і знищення інформації, бланки і фрагменти документів, вихідні тексти програм для ЕОМ, чернетки та інші зразки для порівняльного дослідження.

Перед вилученням магнітних носіїв інформації вони повинні бути в обов'язковому порядку упаковані.

Допит. При розслідуванні розкрадань з використанням мережі Інтернет у підозрюваного під час допиту слід з'ясувати: наявність професійних навичок зі створення шкідливого програмного забезпечення або наявності відповідних зв'язків; спосіб придбання шкідливого ПЗ; обставини оренди серверів для управління бот-мережею; обставини покупки трафіку; обставини отримання інформації про ПЗ системи «Банк-клієнт» відповідної банківської організації; джерела отримання інформації про клієнтів банківської організації, стан їхніх рахунків, контрагентів; наявність співучасників; обставини придбання так званої

фірми-«одноденки»; ким, за допомогою яких настановних даних виготовлялося підроблене платіжне доручення; спосіб легалізації викрадених грошових коштів.

Допитавши осіб, які обслуговують комп'ютерну систему, можна встановити, хто запускав нештатну програму, чи було це зафіксовано будь-яким способом. Слід також з'ясувати, хто захоплюється програмуванням, вчиться або вчився на комп'ютерних курсах.

Допит свідків з числа осіб: обслуговуючих комп'ютер, комп'ютерну систему або мережу (системний адміністратор, оператори), розробників системи і, як правило, постачальників ПЗ. У цьому випадку необхідно з'ясувати, як злочинець міг подолати засоби захисту даної системи, дізнатися ідентифікаційний номер законного користувача, код, пароль для доступу до неї, отримати відомості про інші засоби захисту тощо.

Призначення судових експертиз. При розслідуванні злочинів даної категорії зазвичай типовими є судові комп'ютерна та комп'ютерно-технічна експертизи. Зазначені експертизи дозволяють вирішити такі питання: відтворення і роздруківки всієї або частини комп'ютерної інформації (з певних тем, ключовими словами і т.д.), що міститься на машинних носіях; відновлення комп'ютерної інформації, що раніше містилася на машинних носіях, але згодом стерта (знищена) або змінена (модифікована) з різних причин; встановлення дати і часу створення, зміни (модифікації), знищення або копіювання інформації (документів, файлів, програм); розшифрування закодованої інформації, підбору паролів і розкриття системи захисту від несанкціонованого доступу; дослідження засобів обчислювальної техніки і комп'ютерної інформації на предмет наявності програмно-апаратних модулів і модифікацій, що призводять до несанкціонованому знищення, блокування, модифікації або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їх мережі; встановлення авторства, місця (засобів) підготовки і способу виготовлення документів (файлів, програм), що перебувають на машинних носіях інформації; встановлення можливих несанкціонованих способів доступу до охоронюваної законом комп'ютерної інформації та її носіїв; з'ясування технічного стану, справності

засобів обчислювальної техніки, оцінки їх зносу, а також індивідуальних ознак адаптації засобів обчислювальної техніки під конкретного користувача; встановлення причин і умов, що сприяють вчиненню злочину в сфері комп'ютерної інформації.

У провадженнях цієї категорії з криміналістичних експертиз найбільш часто призначають дактилоскопічну, трасологічну, почеркознавчу, фоноскопічну, авторознавчу і техніко-криміналістичну експертизу документів, експертизу матеріалів, речовин і виробів з них.

У ряді випадків потрібно призначити специфічні дослідження, що проводяться недержавними ліцензійними організаціями. До їх числа відносять: дослідження інцидентів в системі ДБО; встановлення обставин роботи користувача в мережі Інтернет (використання реквізитів доступу в мережу Інтернет); дослідження баз даних; дослідження імовірно шкідливих програм; дослідження обставин здійснення несанкціонованого доступу до інформації; дослідження дампів мережевого трафіку; відновлення даних на різних носіях інформації; дослідження програм для обміну повідомленнями (пошта, програми миттєвого обміну повідомленнями); дослідження носіїв інформації, пов'язаних з DDoS; дослідження мобільних пристроїв, дослідження енергонезалежних носіїв інформації та їх копій тощо.

Так, дослідження енергонезалежних носіїв інформації та їх копій в більшості випадків полягає в дослідженні вмісту файлових систем і у відновленні даних.

Криміналістичне дослідження файлових систем полягає в аналізі різного роду інформаційних слідів, що виникають в результаті дій підозрюваного, роботи програмного і апаратного забезпечення досліджуваної системи. Кількість таких слідів (як джерел криміналістично значимої інформації) в файлових системах велике (від тимчасових міток створення, зміни, відкриття файлів і фрагментів віртуальної пам'яті в файлах підкачки до MAC-адрес, записаних у ярликах Windows), в зв'язку з чим відсутні будь-які вичерпні методики і алгоритми

проведення криміналістичних досліджень файлових систем при розслідуванні інтернет-шахрайства.

На завершення зазначимо, що масова комп'ютеризація суспільства, вільний доступ до ресурсів глобальної мережі Інтернет, відсутність візуального контакту шахрая і потенційної жертви, призводить до розвитку нових способів розкрадання. А значить, і до гострої необхідності в розробці та впровадженні в діяльність співробітників кримінальної поліції та органів досудового розслідування сучасних методик виявлення та розслідування інтернет-шахрайства, найбільш оптимізованих до сучасної криміногенної обстановки.

V. ТИПОВИЙ АЛГОРИТМ ДІЙ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ (КАРНОГО РОЗШУКУ) ПРИ ПРОВЕДЕННІ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

Використання соціальних мереж Інтернет при проведенні негласних слідчих (розшукових) дій

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 впізнавану назву «Facebook». Сам Марк Цукерберг за створення цієї соціальної мережі, у 2010 році був визнаний Американським журналом «Times» людиною року, та став наймолодшим мільярдером. На пострадянському просторі, найвідомішими та поширеними у користуванні соціальними мережами, навіть серед недостатньо обізнаних осіб щодо повних технічних можливостей мережі Інтернет, є «Одноклассники» та «Вконтакте». Обидві соціальні мережі на сьогодні за своїми функціональними можливостями та структурою 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 аудіоматеріали: фотографії та відеозаписи, де є сам користувач, або його родичі чи знайомі, цифрові зображення картин чи інші цифрові зображення, аудіокомпозиції, відеокліпи та відеоролики, що відображають, у т.ч. естетичні або незвичайні смаки користувача. Всі ці дані користувачі соцмереж розміщують у своїх профілях добровільно, а важливо те, що чим більше інформації про себе, тим більший соціальний статус своєму профілю користувач здобуде за рахунок спілкування в мережі Інтернет. Тобто соцмережі стимулюють розміщення користувачами їх особистої інформації всередині самих соцмереж. Велика кількість людей, які мають створені в соцмережах профілі, тим самим відкривають для працівників ОНП вільний шлях для отримання інформації про певну особу. За результатами дослідження, проведеного Ю.О. Юхно та Д.О. Максимусом, під час якого опитано користувачів соцмережі «Вконтакте» (140 респондентів віком від 16 до 35 років), було отримано такі результати:

70% відвідують свою сторінку соціальної мережі «Вконтакті» щодня; 80% відкрили доступ до перегляду даних зі своєї сторінки усім бажаючим; 60% використовують свою сторінку для підтримання зв’язків з друзями; 74%

розміщують на своїй сторінці особисті дані, які повністю відповідають дійсності; 70 % опитаних добавляють людей у список своїх друзів на своїй сторінці соціальної мережі «Вконтакті», спираючись на знайомство, чи на близькі дружні відносини з ними; лише 30% не обмінюються і не планують обмінюватись на своїй сторінці інформацією про вчинення протиправних діянь, шляхом використання повідомлень, хоча останні 70% таку можливість не виключають при спілкуванні через Інтернет. Виходячи із наведених даних, наголосимо, 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 ОНП України відносно осіб що готують або вже вчинили кримінальне правопорушення чи ухиляються від досудового розслідування і суду. Це, відповідно, може надати і розширити співробітникам ***підрозділів кримінальної поліції (карного розшуку)*** *такі 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 у НП, 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.

Використання пошукових сервісів при проведенні негласних слідчих (розшукових) дій

Майже вся аудіо-, відео- та текстова інформація, що знаходиться на сторінках сайтів у мережі Інтернет, а так само й імена конкретних Інтернет-сайтів, відшукується його користувачами шляхом формування відповідних пошукових запитів у спеціальних пошукових сервісах. За своєю внутрішньою будовою пошукові сервіси поділяють на такі складники: *відкриту для користувача, та закриту*.

Відповідно, *відкриту* для користувача частину умовно поділяють на *такі частини*:

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

- графічна оболонка пошукового сервісу;

- інструменти для формування пошукових запитів та роботи з ними;

- блок відображення результатів пошуку інформації за сформованими пошуковими запитами.

Закриту від користувача частину умовно поділяють на *такі складники*:

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

- пошукові роботи це спеціальні програми, які сканують інформаційний простір мережі Інтернет, та відносять, чи виключають ту чи іншу інформацію до бази даних пошукового сервісу;

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

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

Зазначимо, що різні пошукові сервіси використовують різні внутрішні правила та різних пошукових роботів, через що їх пошукові індекси та бази даних

можуть суттєво відрізнятись одна від одної. Саме тому під час пошуку інформації, що становить *тактичний чи оперативний* інтерес, необхідно користуватись різними пошуковими сервісами. Далі наведено перелік із шести пошукових сервісів, відображення результатів пошуку в яких відрізняється один від одного, та розміщено в порядку, в якому доцільно їх використовувати при пошуку інформації, що представляє оперативний інтерес.

«Google Inc.» - 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» надасть 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» - 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 мультипорталом. 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 здійснюється 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.

«META» - 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 META. 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, при його використанні доцільно додавати сайт до пошуку в ручному режимі.

«Rambler Media Group» 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 групи 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 по-рівняння 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!» - американська компанія, що 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!, що включає 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» 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:

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

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

- 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 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)

Пошук інформації, що становить оперативний інтерес, із використанням можливостей протоколу передачі даних – FILE TRANSFER PROTOCOL (FTP)

«Всесвітня мережа», або «World Wide Web» (скорочено: WWW; також: 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 по 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» та «Яндекс», 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», та «МАМОНТ».

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 графі-чні 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 разі слід шукати інформацію про дану особу, використовуючи можливості сервісу та серверів FTP таким чином:

1) необхідно відкрити спеціальний сервіс пошуку інформації на FTP-серверах. В даному випадку скористаємось таким сервісом, як «МАМОНТ». 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» 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». 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 адресу 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) у програмі «FTP Explorer» повинна відобразитись будова директорій (папок) та файлової системи на FTP-сервері, адресу 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 за сприятливих умов (якщо доступ до фалів FTP-серверу не захищений паролем), завантажити усі файли, що знаходяться в ній;

10) проаналізувати інформацію, що знаходиться у завантажений файлах, на предмет вмісту 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 й інші FTP-сервери, адреси яких було відображено у блоці результатів пошуку інформації за сформованими пошуковими запитами сервісу «МАМОНТ».

Глосарій

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 вводу-виводу.

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 перезаписати, з розширеною архітектурою; нестирана пам'ять, на компакт-диску з розширеною архітектурою.

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 конфігурації 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 виправляння 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. Одержав найбільше поширення в Інтернет за рахунок можливості збереження зображень, що мають до 256 кольорів, підтримування прозорості, анімації і здатності збереження в одному файлі декількох зображень. GIF має гарний алгоритм стиснення, що вкрай важливо для створення компактних графічних файлів.

GM (Global Memory) – глобальна пам'ять.

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

HS (High-Speed) – швидкопрохідний, швидкісний.

HTML (Hyper Text Markup Language) - мова розмітки гіпертексту, що дозволяє за допомогою керуючих міток (тегів) визначати структуру і зовнішній вигляд HTML-документа (web-сторінки) при відображенні в браузері, а також створювати посилання на інші файли.

HTTP (Hyper Text Transfer Protocol) - протокол, що забезпечує взаємодію користувача, який запитує доступ до web-документів, із сервером, що надає можливість такого доступу.

IBM-compatible – IBM-сумісний.

ICQ (I Seek You) - додаток Інтернет, використовуваний для прямого інтерактивного спілкування між користувачами. За допомогою ICQ можливий обмін текстовими повідомленнями, пересилання файлів, участь у колективних іграх тощо.

IP-адреса - числовий ідентифікатор, що надається кожному комп'ютеру (хосту), підключеному до Інтернету. IP-адреса складається з адреси мережі й адреси даного хоста в цій мережі і являє собою чотири десяткових числа (від 0 до 255), розділених крапкою. Наприклад: 217.174.97.59.

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 інтеграці-єю 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 вводу-виводу.

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) – енергонезалежна 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) – переносний 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.

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 (міжмережевий протокол). Набір протоколів, які керують Internet і визначають способи передавання даних між комп'ютерами.

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

TXT (TeXT) – текст.

UFD (User File Directory) – каталог файлів користувача.

UFI (User Friendly Interface) – дружній інтерфейс.

URL (Uniform Resource Locator) – Інтернет-адреса, надана кожній web-сторінці. Кожен URL в Інтернет унікальний.

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

WAP (Wireless Application Protocol) – стандарт для додатків, що використовують безпровідні мережі. Фактично являє собою протокол, що забезпечує безпечний доступ безпровідних пристроїв (КПК і стільникових телефонів) до текстової інформації, в тому числі web-сторінки, чат-сесії та електронну пошту. Web-браузер - див. Браузер. Web-сайт - див. Сайт

Web-сервер - комп'ютер зі спеціальним програмним забезпеченням, що забезпечує доступ багатьох користувачів до розташованої на ньому інформації.

Web-сторінка (HTML-документ) - логічна одиниця Інтернет (точніше, Всесвітньої павутини), однозначно визначена адресою (URL). Фізично являє собою HTML-файл. Може містити текст, зображення, аудіо- і відеофрагменти, Java-апплети та інші елементи. Web-сторінка може бути статичною або динамічно згенерованою (приклади динамічних сторінок - переліки результатів, які видають пошукові машини). У випадку використання фреймів, кожен фрейм розглядається як окрема сторінка. Сторінки завантажуються і проглядаються користувачем на своєму комп'ютері за допомогою браузера. Логічно зв'язана сукупність web-сторінок утворює сайт.

WIN (Wireless Inbuilding Network) – бездротова 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 See 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.

Агент передачі пошти (MTA) -

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) – клієнтська програма для роботи у Всесвітній Павутині (WWW). Дозволяє користувачу переглядати зміст web-сторінок. Браузер звертається до web-сервера (сайту), запитує HTML-документ, інтерпретує отриману інформацію і відображає документ на екрані комп'ютера. Браузери поділяються на графічні і текстові. Останній варіант браузерів, прикладом якого є Lynx, у даний час практично цілком вийшли з уживання. Приклади браузерів: Mosaic, Netscape Navigator, Internet Explorer, Opera, Mozilla.

Вузол - пристрій в мережі (ним можуть бути робоча станція, принтер або файловий сервер).

Дозвіл - установлення обмежень для користувачів, які мають доступ до деякого об'єкта системи, і режим цього доступу (повний, обмежений, недозволений).

Гіперпосилання (hyperlink) – слово чи зображення в електронному документі, що містять посилання на інші файли. Клацання «мишею» по гіперпосиланню дозволяє перейти до іншого файлу чи фрагменту електронного документа. Як правило, гіперпосилання виділяються кольором. При наїзді на них «мишею», замість стрілки з'являється зображення руки з вказівним пальцем.

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. Найпоширеніший спосіб спілкування в Інтернет. У даний час електронною поштою можна пересилати не тільки текст, але й усі інші види даних додатками до листів. Самі листи нині можуть підтримувати всі операції зі шрифтами, в т. ч. фон, таблиці й ілюстрації.

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 комерцій-них 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.

Клієнт - комп'ютер, що споживає ресурси інших комп'ютерів мережі, насамперед, серверів. Також - програма, що виробляє запити на доступ до віддалених ресурсів і передає їх мережею на певний комп'ютер.

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.

Кукі (Cookies) – елемент даних, якими web-сервер позначає конкретний браузер при його відвідуванні. При наступному візиті сервер уже впізнає користувача і може запропонувати йому інформацію з урахуванням заявлених раніше уподобань, чи навпаки, не показувати клієнту ті дані (наприклад, рекламний банер), які він уже бачив. Cookies не здатні читати диск комп'ютера користувача. Деякі їхні значення зберігаються тільки протягом одного сеансу роботи із сервером і видаляються після закриття браузера. Інші записуються у файл і зберігаються на жорсткому диску в спеціальних директоріях.

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.

Поштова адреса - ідентифікатор поштової скриньки користувача. Утворюється з імені користувача і доменного імені поштового сервера,

розділених символом @ (комерційна «ет»). Наприклад: pastushenko@univ.kiev.ua Ця електронна адреса захищена від спам-ботів, Вам потрібно включити JavaScript для перегляду , ivanov@inbox.ua Ця електронна адреса захищена від спам-ботів, Вам потрібно включити JavaScript для перегляду , info@krotus.org Ця електронна адреса захищена від спам-ботів, Вам потрібно включити JavaScript для перегляду . В інтранет-мережах організацій реєстрація поштової адреси виконується системним адміністратором, на безкоштовних поштових серверах — самими користувачами.

Поштовий сервер – сервер, що забезпечує прийом-передачу і маршрутизацію персональних електронних листів користувачів. Організація поштового сервера вимагає установки на комп'ютер відповідного програмного забезпечення, наприклад, Mdaemon. Електронна пошта є основним засобом спілкування в Інтернет.

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

Протокол - набір правил, що визначає поведінку функціональних блоків при передачі даних у мережі.

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

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.

Бібліографічний список

1. Бутузов В.М. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток : [наук.-практ. посіб.] / В.М. Бутузов, В.Д. Гавловський, К.В. Тітунина, В.П. Шеломенцев; за ред. І.В. Бондаренка. – К. : Вид. дім "Аванпост-Прим", 2009. – 182 с.

2.Біленчук П.Д. Організована транснаціональна комп'ютерна злочинність: глобальна проблема третього тисячоліття [Електронний ресурс] – Режим доступу: http://www.crime-research.ru/a2002.html

3. Поливанюк В. Використання спеціальних знань при розслідуванні кримінальних справ щодо злочинів, вчинених у сфері використання комп'ютерних технологій [Електронний ресурс] – Режим доступу: http://www.crime-research.ru/library/Polivan2.htm

4. Поливанюк В. Попередження комп'ютерних злочинів у банківській діяльності [Електронний ресурс] – Режим доступу: http://www.crime-research.ru/library/Polivanyuk4.htm

5.Поливанюк В. Криміналістична характеристика злочинів, вчинених у банківській системі з використанням сучасних інформаційних технологій [Електронний ресурс] – Режим доступу: http://www.crime-research.ru/library/Polivan3.htm

6. Економічні злочини у сфері інформаційних технологій [Електронний ресурс] – Режим доступу: http://www.rusnauka.com/ONG_2006/Pravo/17885.doc.htm

7. 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: Ніка Нова, 2013. – 102 с.

9. Негласні слідчі (розшукові) дії та використання результатів оперативно-розшукової діяльності у кримінальному провадженні: навчально-практичний посібник / С.С. Кудінов, Р.М. Шехавцов, О.М. Дроздов, С.О. Гриненко. – Х.: Оберіг, 2013. – 344 с.

10. Самойлов С.В. Розслідування шахрайств, учинених із використанням мережі Інтернет [Електронний ресурс] – Режим доступу: https://mydisser.com/en/avtoref/view/28951.html

11. Санакоєв Д.Б. Взаємодія оперативних підрозділів ОВС та Інтерполу у протидії кіберзлочинності // Сучасні проблеми теорії та практики оперативно-розшукової діяльності органів внутрішніх справ: Матеріали міжнародної науково-практичної конференції, 3 червня 2011 року. – Запоріжжя: Юридичний ін-т ДДУВС, 2011. – С.121-125.

12. Санакоєв Д.Б. Попередження витоку конфіденційної інформації мережею Інтернет в системі органів внутрішніх справ // Оперативно-розшукова діяльність органів внутрішніх справ : проблеми теорії та практики: Матеріали

Всеукраїнської науково-практичної конференції, 21 вересня 2012 року. – Дніпропетровськ: ДДУВС, 2012. – С.178-180.

13. Санакоєв Д.Б. Контроль доступу до web-контенту як засіб протидії порнографії оперативними підрозділами ОВС // Актуальні проблеми правоохоронної діяльності та юридичної науки: матер. Міжнар. наук.-практ. конф. (Дніпропетровськ, 19-20 верес. 2013 р.). – Дніпропетровськ: ДДУВС, 2013. – С.284-287.

14. Телійчук В.Г. Протидія злочинам, що вчиняються організованими злочинними угрупованнями з використанням комп'ютерних технологій / В.Г. Телійчук // Організація і тактика документування підрозділами ДСБЕЗ злочинів у комп'ютерних мережах та мережах електрозв'язку» : Матеріали всеукр. наук.-практ. конф (м.Донецьк, 04 грудня 2009р.). – Донецький юрид. ін-т ЛДУВС ім.. Е.О. Дідоренка. – Донецьк: ДЮІ ЛДУВС, 2009. – с.198-202

15.Телійчук В.Г. Способи вчинення комп'ютерних злочинів у сфері високих технологій та заходи протидії / В.Г. Телійчук // Актуальні питання юридичної науки: теорія та практика: Матеріали міжнар. наук.-практ. конф. (м.Кіровоград, 11 грудня 2013 р.) – Кіровоградський ін-т. держ. та муніц. упр. КПУ – Кіровоград:КІДМУ КПУ, 2013 –с.280-283

16.Телійчук В.Г. Способи вчинення злочинів у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та заходи протидії / В. Г. Телійчук // Держава та регіони. Сер.: Право. - 2014. - № 2. - С.31-37. - Режим доступу: http://nbuv.gov.ua/UJRN/drp_2014_2_8