УДК 343.98

МЕРЕЖА ІНТЕРНЕТ У ДІЯЛЬНОСТІ СЛІДЧОГО

Артур ПАНАСЮК,
аспірант кафедри криміналістики
Національного університету «Одеська юридична академія»

SUMMARY

To research the Internet to the investigator, the analysis of the current state of differentiation on the call sign and negative aspects, identification of important events in its development, the formation of his own categorical apparatus. Characterized investigating possibilities for the use of the Internet in detecting, preventing, investigating and solving crimes. Highlight the place and importance of the Internet in a professional investigator with the increasing number of crimes that are committed by the help of which the Internet is both a means of committing a crime and localization of the main trace of the picture.

Key words: investigator, investigating crimes, network, Internet, software, online fraud, spamming, DoS-attacks, Website defacement, phishing, cybersquatting, cyber-war, karderstvo, pseudo-site.

АНОТАЦІЯ

Стаття присвячена дослідженню мережі Інтернет в діяльності слідчого, аналізу її сучасного стану з диференціацією на позивні та негативні аспекти, виокремленню важливих подій у її розвитку, формуванню власного категоріального апарату. Охарактеризовано можливості слідчого щодо використання мережі Інтернет при виявленні, запобіганні, розслідуванні й розкритті злочинів. Виділено місце та значення мережі Інтернет у професійній діяльності слідчого з урахуванням збільшення кількості злочинів, що вчинюються за її допомогою, де Інтернет є водночас і засобом вчинення злочину, і місцем локалізації його основної слідової картини.

Ключові слова: слідчий, розслідування злочинів, мережа, Інтернет, програми, онлайн-шахрайство, спам-розсилки, DoS-атаки, дефейс, фішинг, кіберсквотинг, кібервійна, кардерство, псевдосайт.

Постановка проблеми. Інтернет у діяльності слідчого загалом, а особливо при розслідуванні злочинів у сфері електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку посідає центральне й вагоме місце. Інтернет бере свій початок з кінця 60-х років XX століття у вигляді оборонного проекту, створеного у вигляді комунікаційної мережі, де відсутній єдиний центр управління й де один комп'ютер не більш важливий, ніж будь-який інший у ній, при цьому основною умовою була його здатність функціонувати під час атомної війни. Історичним моментом було створення єдиного стандарту комунікацій TCP/IP міжмережевого протоколу управління передачею, який дав змогу різним мережам з'єднуватися одна з одною. З цього моменту й бере свій початок саме мережа Інтернет, у якій надалі було створено всесвітню павутину – World Wide Web (w.w.w.) з новим методом передачі інформації (протоколи передачі гіпертекстів, гіпермедіа).

Метою статті є дослідження мережі Інтернет у діяльності слідчого, визначення її місця серед інших технологічних розробок, розкриття початкових основ її розвитку та функціонування, окреслення уявлень щодо її можливостей на сьогодні та в майбутньому, аналіз її сучасного стану з диференціацією на позивні й негативні аспекти.

Виклад основного матеріалу. Питанням дослідження Інтернету в криміналістиці присвячені роботи Б.В. Андрєєва щодо розслідування злочинів у сфері комп'ютерної інформації [1], П.Д. Біленчука відносно комп'ютерної злочинності [2], В.Б. Вехова стосовно методики розслідування злочинів у сфері комп'ютерної інформації [3], В.В. Крилова щодо інформаційних комп'ютерних злочинів [4], В.О. Мещерякова відносно правового та криміналістичного аналізу злочинів у сфері комп'ютерної інформації [5], О.І. Усова стосовно судово-експертних досліджень комп'ютерних засобів [6], Д.М. Цехана щодо використання високих інформаційних технологій в оперативно-розшуковій діяльності [7], І.Ф. Хараберюша відносно використання оперативно-технічних засобів у протидії злочинам, що вчинюються у сфері нових інформаційних технологій [8], В.І. Федотова стосовно виявлення й розслідування комп'ютерних злочинів [9] та ін. Аналізуючи вищезазначені роботи, приходимо до висновку, що варто приділити увагу менш дослідженому питанню, як мережа Інтернет у діяльності окремого суб'єкта, а саме слідчого.

Слідчому для початкового уявлення устрою Інтернету необхідно насамперед ознайомитися з великою кількістю інформації щодо неї. Ми не будемо зупинятися на розкритті цих понять і їх значенні в мережі, але поділимо ці знання на сфери для виявлення слідчим злочинних подій у ній. Отже, саме подальше розуміння мережі Інтернет у діяльності слідчого вимагає викладу основних категорій (понять, термінів) у цій сфері.

Варто розпочати зі структури. Мережа Інтернет – це всесвітня комп'ютерна мережа, тобто комп'ютери, які територіально віддалені один від одного, з'єднані між собою для спільної роботи. Види комп'ютерних мереж: локальні (комп'ютери, що знаходяться в одному приміщенні) та глобальні (декілька локальних мереж чи окремі комп'ютери, віддалені один від одного в радіусі 1000 м.). Тобто, Інтернет – це всесвітня комп'ютерна мережа, що складається з різних комп'ютерних мереж, об'єднаних стандартними угодами про способи обміну інформацією, єдиною системою адресації з наступними з'єднувальними лініями: лінії зв'язку, оптиковолоконні, радіозв'язок, супутниковий зв'язок тощо. Тут варто пізнати сутність таких категорій, як протоколи Інтернету, система адресації (формати IP і DNS), канали зв'язку між її мережами, система передачі інформації (вузли або маршрутизаторами (router)), способи підключення (сеанс: програма–телефонна лінія–модем, підключений в одну з мереж Інтернет, або окрема телефон-

на лінія, цифрова телефонна лінія, цифровий канал зв'язку, радіоканал за допомогою радіомодема, супутниковий зв'язок), ресурси мережі: новини, електронна пошта, вебінари, протоколи передачі файлів, системи пошуку, всесвітня павутина (URL-адреса, Web-сторінка, формат HTML, Web-сервер, Web-сайт), форуми, блоги та чати, розмови за принципом телефону.

Актуальними є питання програмного забезпечення персонального комп'ютера слідчого для роботи в Інтернеті за допомогою сучасних програм-клієнтів і його постійного оновлення для тих відділів, які розслідують злочини у сфері електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Але сучасний стан розвитку інформаційних технологій у сфері електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, що дає змогу на високому рівні з великою точністю дослідити переміщення інтернет-користувача по мережі (місце, час, тривалість тощо), відвідування сайтів (час, тривалість, рух по розділах, скачування тощо), рух коштів на платіжних рахунках (кількість, отримувач, вартість), спілкування (соціальні мережі, форуми, обговорення, будь-які відмітки тощо) як у межах певної країни, так і в усьому світі, у свою чергу, має як позитивні аспекти так і негативні.

Варто дослідити ці аспекти більш детально, відповідно до діяльності правоохоронних органів.

Позитивні аспекти:

1. Пошук інформації, документів і будь-яких даних, необхідних для забезпечення професійної діяльності, з диференціацією слідчого за часом, місцем, мовою тощо.

2. Пошук орієнтуючої інформації щодо фізичних і юридичних осіб, їх кола знайомих, клієнтів.

3. Контроль за професійною діяльністю фізичної та юридичної особи за допомогою мережі Інтернет у межах кримінального провадження [1; 2; 3; 4; 8; 9].

4. Функціонування форумів, чатів, ICQ, які дають змогу мільйонам людей спілкуватися, ділитися інформацією про себе й оточуючих (безкоштовне, швидке джерело обміну будь-якими даними, що є доступними для слідчого).

5. Віртуальне відвідування за допомогою спеціальних програм ділянок, приміщень, вулиць тощо (наприклад, відтворення в пам'яті свідка злочинної події за допомогою Google Maps, Яндекс-карт тощо).

6. Форма демонстрації колегам, суспільству та ЗМІ результатів діяльності структурного підрозділу правоохоронного органу на його офіційному сайті тощо.

7. Проведення нарад, навчальних занять, семінарів у форматі відео конференцій/вебінарів з великою кількістю учасників.

8. Доступ до різноманітної літератури на спеціалізованих сайтах найбільших бібліотек світу, якими може скористатися будь-який слідчий у будь-якому місці й у будь-який час.

9. Використання програм, що забезпечують зв'язок та інші можливості у віртуальному світі (програмне забезпечення, електронний зв'язок, Google документи, Google диск, календарі тощо). Кожна програма вирішує певне коло завдань.

10. Підвищення рівня освітніх знань слідчого за допомогою спеціальних програм та вдосконалення вже набутих навичок тощо.

11. Постійний доступ до всіх новин (як широкої, так і вузької тематики), крім цього, і до новин минулих років, що не є менш важливим у розслідуванні злочинів минулих років.

12. Користування послугами телефонного зв'язку через Інтернет.

13. Інше…

Отже, на сьогодні за допомогою мережі Інтернет можна робити практично все, але й це ще не все. Ми з надією дивимося в майбутнє, і розробники нам у відповідь майже кожного дня запускають для користувачів нову програму, технологію або технічний засіб. А правоохоронні органи, у свою чергу, будучи активним користувачем міжнародної мережі Інтернет, можуть ефективно застосовувати його технологічні й інші можливості в боротьбі зі злочинністю. І от саме тут стикаємося зі специфічними негативними аспектами цього інформаційно-комунікаційного буму, як-от:

1. Тривала робота за комп'ютером погано впливає на фізичний стан людини. Усе це з часом позначається на багатьох системах організму (вищої нервової, ендокринної, репродуктивної, імунної тощо).

2. Інтернет – ілюзія вседозволеності та безкарності. Саме тут існують різні сайти наркоманів, найманих убивць, самогубців, крадіїв, терористів.

3. Через Інтернет можна придбати зброю, наркотичні й сильнодіючі засоби та інші заборонені засоби. Крім цього, можна навчитися самому всі ці речі виготовляти.

4. Інтернет – найбільше джерело розповсюдження порнографії, наклепів, образ, екстремістських закликів.

5. Порушення авторських та інших інтелектуальних прав в офлайні (торгівля контрафактними дисками й програмами, послуги інсталяторів, які не мають прав на програмне забезпечення тощо).

6. Онлайн-шахрайство. Функціонування фіктивних Інтернет магазинів (торгівля); псевдосайтів благодійних і релігійних організацій, громадських та політичних партій і рухів (пожертвування, внески); сайтів із проханням про матеріальну допомогу під різні історії: хвороба, катастрофа, жахлива доля; фіктивних шлюбних агентств; фіктивних банків та інвестиційних фондів з обіцянками великих процентів по депозитах; фіктивних сайтів щодо працевлаштування з обов'язковим «вступним фіксованим внеском». Також шахрайські дії щодо Інтернет-трафіка й шахрайство в онлайн-іграх.

7. Спам-розсилки. Розсилка в Інтернет-мережі: пропозиції щодо придбання програм, які дають змогу економити або збільшувати кошти на рахунку тощо; шкідливі програми; заклики до вчинення екстремістських і терористичних дій; прохання щодо надання грошової допомоги хворим, обездоленим, знівеченим тощо.

8. DoS-атаки. В Інтернеті орудують спеціалісти, які створюють програми, що руйнують усе на своєму шляху задля задоволення власного самолюбства.

9. Дефейс. Злочинець змінює зовнішній вигляд веб-сайта потерпілого різними способами, частіше тільки першу сторінку, але іноді й інші (потерпілий – фізична або юридична особа).

10. Функціонування RBL – спеціальних чорних списків (база даних IP-адресов), спрямована на протидію розсилці спаму й на захист від спаму, які основані на протоколі DNS.

11. Фішинг – виманювання під різними приводами в потерпілих їх персональних і конфіденційних даних, які надалі використовуються в злочинній діяльності (види: вішинг, фармінг).

12. Кіберсквотинг – перепродаж доменних імен, тобто придбання доменного імені з метою його недоброякісного використання чи з метою завадити його доброякісному використанню законним власником.

13. Кардерство – отримання даних банківської карти, включаючи пароль. Способи реалізації цих даних: придбання товарів в Інтернет-магазинах; розрахунки за Інтернет-послуги; фіктивне придбання товарів в Інтернет-магазинах або фіктивний розрахунок за Інтернет-послуги; гра в Інтернет-казино; зняття коштів з рахунків тощо.

14. Шкідливе програмне забезпечення: троянські програми та їх підвиди (ransomware, черва, троянець тощо); програми, що впроваджують відкрито або приховано на персональний комп'ютер несанкціоновану рекламу; програми, які слугують для підвищення привілеїв користувача й приховання його дій; програми, що програмують знищення будь-якої інформації в будь-який час з дотриманням певним вимог або/чи їх виконанням.

15. Функціонування трьох найбільш розповсюджених груп дій, які надають можливість спостерігати за діяльністю в мережі Інтернет, можуть бути виконані програмними закладками: копіювання інформації користувача комп'ютерної системи, що знаходиться в ОП або зовнішній пам'яті цієї чи підключеної до неї комп'ютерної системи; зміни в алгоритмах функціонування системних, прикладних і службових програм; нав'язування певних режимів роботи. Саме потенціал цих груп використовують спецслужби багатьох країн для своєї розвідувальної діяльності (СОРМ, ЕШЕЛОН, PRISM).

16. Незаконний контроль за життям мільйонів людей, виток інформації в будь-якій формі, працездатність систем спостереження, які дають змогу отримати доступ до особистої пошти та списку сайтів будь-якого користувача (наприклад, перехоплення мережевих з'єднань і пакетів, паролів (кейлогер), звернень браузера до сайтів за допомогою HTTP Proxy або розширень браузера, експорт усіх даних із сервісів тощо).

17. Існування в Інтернет мережі платіжних систем, що надають можливість провести незаконні транзакції великих сум, введення та виведення коштів, у тому числі анонімних (так звані «кримінальні платежі»).

18. Кібервійна – це інформаційна війна, без учинення бойових дій, використання вогнепальної зброї або іншого її виду, де зброєю є спеціально оброблені та підготовлені дані.

19. Замкненість у мережі Інтернет інформації в централізованих базах даних, що належать обмеженому колу осіб, які ними володіють.

20. Інше.

Висновки. Ці аспекти можна й варто досліджувати. Але головне, що варто підкреслити, це те, що з плином дуже короткого проміжку часу Інтернет мережа посіла першорядне місце в діяльності слідчого й саме вона надає йому безліч можливостей для розвитку, оперативності, швидкості. І як будь-який елемент матеріального світу, він має як позитивні аспекти, так і негативні, навіть можна говорити про наявність ще й нейтральних. Однак складові цих аспектів завжди залежатимуть від багатьох суб'єктивних та об'єктивних факторів, які ми і збираємося дослідити в подальшій діяльності.

Список використаної літератури

1. Андреев Б.В. Расследование преступлений в сфере компьютерной информации / Б.В. Андреев, П.Н. Пак, В.П. Хорст. – М. : Юрлитинформ, 2001. – 152 с.

2. Комп'ютерна злочинність : [навчальний посібник] / [П.Д. Біленчук, Б.В. Романюк, В.С. Цимбалюк]. – К. : Атіка, 2002. – 240 с.

3. Вехов В.Б. Расследование преступлений в сфере компьютерной информации : [учебно-методическое пособие] / В.Б. Вехов, А.Ф. Родин. – Волгоград : ВА МВД России, 2004. – 164 с.

4. Крилов В.В. Информационные компьютерные преступления : [учебное и практическое пособие] / В.В. Крилов. – М. : ИНФРА-М : Норма, 1997. – 276 с.

5. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ / В.А. Мещеряков. – Воронеж : Воронежский государственный университет, 2001. – 176 с.

6. Усов А.И. Судебно-экспертное исследование компьютерных средств и систем: основы методического обеспечения : [учебное пособие] // под ред. Е.Р. Россинской. – М. : Экзамен : Право и закон, 2003. – 368 с.

7. Цехан Д.М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ : [монографія] / Д.М. Цехан. – Одесса : Юридична література, 2011. – 214 с.

8. Використання оперативно-технічних засобів у протидії злочинам, що вчиняються у сфері нових інформаційних технологій : [монографія] / [І.Ф. Хараберюш, В.Я. Мацюк, В.А. Некрасов, О.І. Хараберюш]. – К. : КНТ, 2007. – 196 с.

9. Федоров В.И. Компьютерные преступления: выявление, расследование и профилактика / В.И. Федоров // Законность. – 1994. – № 6. – С. 44.