справ України від 12.10.2009 р. №436, затвердженого наказом Міністерства внутрішніх справ України.

Таким чином, як показує досвід інших країн організація роботи правоохоронних органів з використанням інформаційного забезпечення та постійного зв'язку з громадськістю впливає на підвищення ефективності роботи поліції та є дієвим засобом для розкриття, виявлення та попередження злочинів.

Використані джерела:

1. В федеральних органах власти внедряют специальные терминалы «Призма» для отслеживание активности в блогах и социальных сетях [Електронний ресурс]. - Режим доступу: http://bda-expert.com/2012/08/v-federalnyh-organah-vlasti-vnedryayut-specialnye-terminaly-prizma-dlya-otslezhivaniya-aktivnosti-v-blogah-i-socialnyh-setyah/

2. Колодяжний М. Г. Досвід Великої Британії у використанні громадськості щодо запобігання злочинності // Форум права., 2013., № 3. - С. 317–323.

Максимова М.К. – слухачка магістратури юридичного факультету;
Науковий керівник: Косиченко О.О.
доцент кафедри економічної та інформаційної безпеки, кандидат технічних наук
(Дніпропетровський державний університет внутрішніх справ).

ОСОБЛИВОСТІ КІБЕРПРОСТОРУ ЯК ОБ'ЄКТА КРИМІНАЛІСТИЧНОГО ДОСЛІДЖЕННЯ

Стрімкий розвиток комп'ютерних технологій зумовлює появу нових форм взаємодії між членами суспільства. Суспільство отримало доступ до безмежних інформаційних потоків, що призвело до розширення можливостей сучасної злочинності. Використання кіберпростору для вчинення злочинів привертає до нього увагу в криміналістичних дослідженнях.

Указ Президента України від 15 березня 2016 року «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 р. «Про стратегію кібербезпеки України» передбачає створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Законодавець вбачає в кіберпросторі певне середовище, в якому можуть бути вчинені кримінальні правопорушення та сформулював загальні завдання, пов'язані з забезпеченням безпеки функціонування і використання кіберпростору. Це зобов'язує суб'єктів сектору безпеки та оборони створити умови для забезпечення ефективної боротьби із кіберзлочинністю [1].

Кіберпростір є складовою частиною інформаційного простору і утворюється як за допомогою мережі Інтернет та безпосередньо у ній функціонує, а може бути автономною системою, не пов'язаною із глобальною мережею. Автор праці « Декларація незалежності кіберпростору» зазначив: «Електронний інформаційний простір має два рівні – обмін інформацією у формі програмних кодів, які створюють кіберпростір та віртуальне життя, створене внаслідок обміну інформацією між користувачами мережі [2]. Кіберпростір – це результат взаємодії між людьми шляхом обміну інформацією в електронній цифровій формі. Можна стверджувати, що кіберпростір як об'єкт криміналістичного дослідження має подвійну природу, а саме: технічну і соціальну.

Інтернет є основним, але не єдиним засобом створення кіберпростору. З урахуванням комп'ютерної складової електронного обліку інформацією, кіберпростір утворюють усі телекомунікаційні мережі, комп'ютерні системи й пристрої, що забезпечують передачу вихідної інформації іншим користувачам. Інформація в електронній цифровій формі, що має криміналістичне значення, за своєю фізичною природою є доступною безпосередньому сприйняттю через використання програмно-технічних засобів. Внаслідок знищення, копіювання, блокування, модифікації та іншого впливу на комп'ютерну інформацію шляхом доступу до неї утворюються певні відомості, які в криміналістиці називають інформаційними слідами. Носіями таких слідів є відповідні технічні засоби, а не матеріальні об'єкти чи свідомість людини, тому ці сліди ще називають віртуальними.

Віртуальні сліди є досить складним об'єктом для пізнавальної діяльності слідчого в рамках певного кримінального провадження. Такі сліди можуть зберігатися Інтернет - провайдерами або користувачами на певному матеріальному носії. З метою ефективного виявлення, фіксації та аналізу інформаційних слідів, які мають криміналістичне або доказове значення необхідно використовувати нові підходи у провадженні слідчих (розшукових) дій та належних слідчих дій, оскільки віртуальність кіберпростору забезпечує відносну конфіденційність інформації про особу злочинця та можливість впливати на свідомість певної категорії осіб. Це приваблює злочинців для використання кіберпростору в механізмі вчинення злочину [3].

Для дослідження кіберпростору слідчий може проводити огляд у ході якого описати технічне, програмне забезпечення, канали зв'язку із обов'язковим залученням спеціаліста. Матеріали фотозйомки, звукозапису, відеофіксації досліджуються як документі відповідно до ст. 99 Кримінального процесуального кодексу України (далі – КПК), у відповідній формі фіксуються і долучаються до матеріалів справи [4].

Кіберпростір як складову частину обстановки кримінального правопорушення можна дослідити за допомогою допити його учасників, наприклад, адміністратор групи у соціальній мережі може надати відомості щодо інформації, яка надсилалась користувачами групи, часу їх спілкування, моменту появи та реакції користувачів на відповідне повідомлення.

Доцільно також проводити негласні слідчі дії у формі зняття інформації з транспортних комунікаційних мереж та зняття інформації з електронних інформаційних систем, оскільки великий обсяг інформації у кіберпросторі передається за допомогою телекомунікаційних мереж та електронних систем.

Для дослідження кіберпростору слідчий призначає такі експертизи як: авторознавча, яка допомагає визначити автора і виконавця текстів та повідомлень у соціальних мережах; семантико – текстуальна експертиза писемного мовлення, яка досліджує зміст словосполучень, речень, текстів і виявляє висловлювання у формі публічних закликів до певних дій, наприклад, до участі у межових заворушеннях, терористичних актах; лінгвістична експертиза, яка досліджує мовленнєву діяльність в усній формі і зафіксовану у фоно або відеограмі; фототехнічна експертиза, яка допомагає ідентифікувати предмети, приміщення і ділянки місцевості на знімках; портретна експертиза для ідентифікації особи або трупа за фотознімком або відеозаписом.

Із комплексу інженерно-технічних експертиз може бути призначено експертизу комп'ютерної техніки і програмних продуктів та експертизу телекомунікаційних систем. Основними завданнями цих експертиз є характеристика параметрів інформаційних систем; робочий стан технічних засобів; встановлення фактів та способів передачі інформації [5].

Для оперативного виявлення злочинів, вчинених з використанням можливостей кіберпростору слід враховувати особливості вчинення злочину для його кримінально-правової кваліфікації; можливості, які створює кіберпростір для вчинення злочинів; вплив кіберпростору на методику розслідування окремих видів злочинів. У механізмі злочинної діяльності кіберпростір як обстановка злочину є передумовою швидкого досягнення злочинного результату в порівнянні з традиційною обстановкою.

Значні труднощі для розкриття та розслідування злочинів з використанням можливостей кіберпростору становить неможливість контролювати весь обсяг інформації в Інтернеті та соціальних мережах.

Визнання на державному рівні суверенного права регулювати комунікаційні можливості (наприклад, у Китаї, Ірані та деяких інших країнах) призводить до технічних помилок електронного зв'язку через надмірну завантаженість провайдерів. З одного боку, це зумовлює певні обмеження права на свободу слова, а з іншого – забезпечення державою належної правової охорони відносин у кіберпросторі,оскільки неузгодженість законів приваблюють злочинців. Адже правоохоронні органи стикаються з великою кількістю перешкод, коли під час розслідування встановлюють факт перебування під юрисдикцією іншої держави телекомунікаційної мережі, використаної для вчинення злочину, або власника інформаційного ресурсу, якого треба захищати від протиправного посягання [6].

За словами Крацберга М.: «Сама по собі технологія є ні гарною, ні поганою, але й нейтральною її не назвеш» [7]. Результати використання технологій залежать від мети суб'єкта їх застосування. Соціальні мережі створили безмежні можливості для об'єднання віддалених одна від одної осіб з метою діяльності організованих злочинних угрупувань. Організована злочинність активно використовує обстановку

кіберпростору для скоєння терористичних актів, незаконного обігу наркотичних засобів, піратства та інших кримінальних злочинів. Соціальні мережі стали масивом відомостей про реальне життя конкретної людини і ця база може бути використана для вчинення злочину.

Отже можна зробити висновок, що кіберпростір – це інформаційний простір взаємодії між людьми за допомогою електронних інформаційних технологій, обмін інформацією за допомогою яких здійснюється на основі системи стандартів, що пояснює технічну і соціальну природу кіберпростору.

Для досягнення злочинного результату використовуються такі особливості кіберпростору як дистанційність, що забезпечує транскордонну складову такої злочинної діяльності і викликає необхідність вирішення питань територіальної юрисдикції; оперативність дій щодо обробки інформації, що сприяє прискоренню або якісному приховуванню злочину; віртуальність, що ускладнює процес виявлення злочинця та дослідження інформаційних слідів; комунікативність, яка сприяє діяльності організованої злочинності як на національному, так і міжнародному рівнях; недосконаліть та наявність прогалин у законодавчій базі щодо забезпечення інформаційної безпеки та правової охорони відносин у кіберпросторі, що дав змогу уникати кримінальної відповідальності [8].

Тому враховуючи ці особливості потрібно застосовувати оновлені методи, прийоми та засоби з метою вирішення практичних завдань розслідування злочинної діяльності.

Використані джерела:

1. Рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про стратегію кібербезпеки України. Указ Президента України». [Електронний ресурс].- Режим доступу: www.rada.gov.ua
2. Шевченко Е.С., Михайлюченко Н.Н. Кіберпростір як елемент обстановки скоєння злочину /Е.С. Шевченко, Н.Н. Михайлюченко// Академічний юридичний журнал. – 2015.- №1.-С.53-54
3. Динту В.А. Місце кіберпростору в системі обстановки злочину/ В.А. Динту// Науковий вісник Херсонського Державного Університету. - 2016.- вип.2-Ф.3. – С.72-75
4. Кримінальний процесуальний кодекс України від 13.04.2012 р. станом на 18.10.2018 р. [Електронний ресурс].- Режим доступу: www.rada.gov.ua
5. Самойленко О.А. Природа кіберпростору як об'єкта криміналістичного дослідження / О.А. Самойленко// Криміналістика і судова експертиза.- 2018.- вип. 1.- С. 176-180
6. Бєлєнський В.П. Відповідальність за кіберзлочини за кримінальним правом США, Великої Британії та України (порівняльне – правове дослідження)/ В.П.Бєлєнський// Юридичні науки. – 2016.- вип.1- Г. 2.-С. 83-86
7. Волинець В.О. Віртуальна реальність: поняття та сутність /В.О.Волинець// Часопис Київського університету права. – 2014. –вип.30.-С. 35-37
8. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва /Д.В.Дубов//Вісник книжкової палати. - 2014.- вип. 2- С. 328-329