Похил Олександра Ігорівна
курсант факультету підготовки фахівців
для органів досудового розслідування ДДУВС

Науковий керівник –
доцент кафедри ОРД та СТ,
к.ю.н., доц. ***Санакоєв Д.Б.***

ЗАГАЛЬНА ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Комп'ютери, комп'ютерні мережі, комп'ютерна інформація є складовими життя сучасної людини. В останні роки в Україні значно зросла кількість Інтернет-користувачів, адже підключення до глобальної мережі стало доступним та зручним. Популярність Інтернету невипадкова, адже він забезпечує цілодобовий доступ до величезної кількості інформації, швидку передачу даних, можливість проведення банківських, торгових, біржових операцій, переказ коштів і багато іншого. Для багатьох людей він став цілим світом, віртуальним світом. Як і в реальному світі, так і у віртуальному, де панує комп'ютерна інформація, трапляються злочини та кіберзлочини, суспільно-небезпечність та масштабність яких з року в рік стрімко зростає.

Термін «кіберзлочинність» поки що в жодному з нормативно-правових актів чітко не визначений. У 2001 р. Радою Європи було прийнято Конвенцію про кіберзлочинність[1], яку Україна ратифікувала лише чотирма роками пізніше, у 2005 р., але і там небуло чіткого визначення даного терміну. Але пропри це поняття широко використовується в лексиконі працівників правоохоронних органів не лише України, а й Європи. Слід зауважити, що український законодавець приділяє значну увагу цій проблемі у Кримінальному кодексі України (далі – КК України), вперше передбачив самостійний розділ для цих злочинів – розд. XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»; двічі положення цього розділу змінювалися та доповнювалися, а отже, це свідчить про актуальність цієї проблеми в українському суспільстві [2].

Кіберзлочини вчиняються за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, а також проти комп'ютерних систем, комп'ютерних даних. Таким чином, електронно-обчислювальна техніка може виступати як засобом вчинення злочину, так і предметом злочину.

На сьогодні найбільш розповсюдженою є класифікація кіберзлочинів на два види: агресивні та неагресивні. До першої групи належать кібертероризм, погроза фізичної розправи, кіберпереслідування, дитяча порнографія (створення порнографічних матеріалів, виготовлених із зображенням дітей). Друга

група включає кіберкрадіжку, кібершпигунство, розповсюдження спаму та вірусних програм[3].

Напевне, однією з найгостріших проблем запобігання цій категорії злочинів є їхня висока латентність, на яку суттєво впливає низька кваліфікація працівників правоохоронних органів, недостатня технічна оснащеність відповідних підрозділів національної поліції. Науково-технічний прогрес не стоїть на місці, з року в рік все більш освоюються та вдосконалюються комп'ютерні програми та технології. Кіберзлочинці, здебільшого, є людьми високоінтелектуальними та обізнаними, через це вони винаходять нові способи вчинення злочинів набагато швидше, ніж створюються ефективні системи безпеки.

Так, проаналізувавши статистичні дані за 2014–2016 рр. на сайті Генеральної прокуратури України, ми маємо такі показники: за 2014 р. до ЄРДР було внесено 418 кримінальних правопорушень за розд. XVI КК України, за 2015 рік – 556 та лише у період з грудня по вересень 2016 р. в Україні вже 736 зареєстрованих випадків [4]. Таким чином, статистичні дані вказують на збільшення кількості злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Саме задля того аби запобігти кіберзлочинності в Україні у 2012 р. було створено Управління боротьби з кіберзлочинністю, який пізніше, в рамках реформи міліції в Національну поліцію, у 2015 році було створено Департамент кіберполіції, основними завданнями якої є запобігання, виявлення, припинення злочинів, пов'язаних із використанням інформаційних технологій та систем.

З огляду на те, що динаміка кіберзлочинності стрімко зростає не лише в нашій державі, але й в усьому світі, необхідно вживати активних заходів запобігання цій проблемі. Так, Україна ратифікувала Конвенцію Ради Європи про кіберзлочинність від 23 листопада 2001 р., що забезпечує регіональні стандарти протидії комп'ютерним злочинам, співробітництва та транскордонної координації діяльності правоохоронних органів. Цей акт уможливлює не тільки перейняття досвіду діяльності відповідних правоохоронних органів інших країн, але й проведення спільних операцій, запрошення висококваліфікованих фахівців. Нещодавно було створено Департамент кіберполіції Національної поліції України, на який покладається забезпечення реалізації державної політики щодо запобігання кримінальним правопорушенням, підготовка, учинення або приховування яких передбачає використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку [5, с. 88; 3, с. 169].

Отже, сучасне запобігання кіберзлочинності знаходиться у перебігу інституціоналізації – з'являються спеціальні суб'єкти запобіжної діяльності, формуються правові норми боротьби з кіберзлочинцями. У цьому контексті надзвичайно важливим є використання знань соціальних наук, зокрема кри-

мінології, що уможливлює ефективну координацію зусиль національних та міжнародних установ боротьби з кіберзлочинністю, надає знання про ціну кіберзлочинності та її актуальні тенденції.

1.Конвенція про кіберзлочинність [Електронний ресурс].- Режим доступу: http://zakon3.rada.gov.ua/laws/show/994_575.

2. Довбиш М. Кіберзлочинність в Україні. 2013 рік [Електронний ресурс]. – Режим доступу: https://www.science-community.org/uk/node/16132.

3.Іванченко О.Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні /Актуальні проблеми вітчизняної юриспруденції, С. 137.

4. Статистична інформація. Єдиний звіт кримінальних правопорушень [Електронний ресурс]. – Режим доступу: http://www.gp.gov.ua/ua/stat.html..

5. Дмитрієв А. А. Роль органів Національної поліції України у сфері протидії організованій злочинності / А. А. Дмитрієв // Форум права. – 2016. – №1. – С. 86–92.

Синько Євген Віталійович
курсант факультету підготовки фахівців
для підрозділів кримінальної поліції ДДУВС

Науковий керівник –
старший викладач кафедри
ОРД та СТ, к.ю.н. ***Кисельов А.О.***

ВЗАЄМОДІЯ СЛІДЧИХ З ПРАЦІВНИКАМИ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ ПІД ЧАС ПРОВЕДЕННЯ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

Після вчинення протиправного діяння, працівники Національної поліції здійснюють певні дії, які спрямовані на розкриття цього злочину та розшуку осіб, що його вчинили. Такі дії мають гласний та негласний характер. Проведення таких дій покладається на слідчі підрозділи Національної поліції України, але при їх проведенні залучаються й оперативні підрозділи.

Актуальність цієї теми полягає в тому, що оперативні підрозділи не можуть діяти самостійно при проведенні негласних слідчих (розшукових) дій, що з одного боку підвищує контроль за їх виконанням, а з іншого боку робить залежними працівників оперативних підрозділів від рішень слідчого.

Раніше дану тему вивчали такі науковці як: О.В. Керевич, Є.В. Лизогубенко, К.В. Смахтин та інші.

Згідно чинного Кримінального процесуального кодексу України(далі КПК України), оперативних підрозділів (крім підрозділу детективів, підрозділу внутрішнього контролю Національного антикорупційного бюро України) не мають права здійснювати процесуальні дії у кримінальному провадженні за власною ініціативою або звертатися з клопотаннями до слідчого судді чи прокуро-