

органи; 2) органи місцевого самоврядування; 3) громадські організації; 4) міжнародні організації.

На нашу думку, загалом, до таких органів та організацій відносяться: управління у справах сім'ї та молоді облдержадміністрацій та відповідні виконавчі органи міських рад; центри соціальних служб для сім'ї, дітей та молоді; служби у справах дітей; управління освіти і науки облдержадміністрацій та відповідні виконавчі органи міських рад; управління охорони здоров'я облдержадміністрацій та відповідні виконавчі органи міських рад; управління праці та соціального захисту населення облдержадміністрації та відповідні виконавчі органи міських рад; центри зайнятості; підрозділи Національної поліції України; підрозділи Служби безпеки України; підрозділи Державної прикордонної служби України; заклади охорони здоров'я; дошкільні, загальноосвітні, професійно-технічні, вищі та позашкільні навчальні заклади; громадські організації, що працюють у сфері надання допомоги особам, які постраждали від торгівлі людьми; міжнародні організації.

Підсумовуючи, слід зауважити, що ефективність розслідування кримінального провадження загалом, залежить від того, наскільки діяльність слідчого та взаємодіючих з ним органів відповідає особливостям злочину та обстановки, що складається під час розслідування. Така відповідність насамперед багато в чому визначається чітким уявленням про предмет доказування, встановлення якого, в свою чергу, є кінцевою метою розслідування.

**Список використаних джерел:**

1. Єдині звіти про кримінальні правопорушення за 2013-березень 2017 року. URL: <http://www.gp.gov.ua> (дата звернення 17.10.2017).

*Одержано 24.10.2017*

**УДК 65.012.8 + 004**

**Олександр Володимирович МАНЖАЙ,**

*кандидат юридичних наук, доцент, доцент кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ*

**ДИТЯЧИЙ ГРУМІНГ ТА ОКРЕМІ АСПЕКТИ  
ЙОГО ДОКУМЕНТУВАННЯ**

Одним з негативних явищ застосування інформаційних технологій з протиправною метою є дитячий грумінг, який може використовуватись для залучення неповнолітніх до тор-

гівлі дітьми, нелегальних обробок, таких як дитяча проституція або виробництво дитячої порнографії. Це поведінка характерна для педофільї [1, с. 49].

Онлайн ґрумери можуть бут розділені на дві групи. До першої належать ті, які працюють «виключно онлайн», у той час як друга група має на меті вчинення сексуального насильства не стільки в кіберпросторі як у фізичному світі. Працівники поліції нерідко використовують легендовані профілі дітей для приваблювання потенційних педофілів. При цьому аналіз відповідних поліцейських профілів засвідчив, що вони не містили стереотипних ознак вразливих до насильства дітей. Це вказує на те, що будь-яка дитина може стати жертвою онлайн-ґрумінга [2, с. 111, 117].

У 2017 році британського педофіла Пола Лейтона (Paul Leighton) було засуджено до 16 років позбавлення волі за зґвалтування в режимі онлайн. Він створив 30-40 несправжніх облікових записів Facebook для знайомства з дітьми. За допомогою соціальної мережі зловмисник спочатку вмовляв дітей надіслати йому фотографії інтимного характеру, після отримання яких шантажував дітей, змушуючи їх до вчинення сексуальних дій насильницького характеру. Так, 14-річного хлопця з Флориди (США) Лейтон змусив зґвалтувати 12 річну племінницю, 14-річну дівчину з Південної Дакоти (США) примусив до статевих актів зі своїм братом, які вони знімали для зловмисника на відео. В аналогічній ситуації опинилась і 13-річна дівчина з Теннессі (США). Загалом жертвами серійного педофіла стали більше ста осіб з різних країн [3].

З технічної точки зору під час документування ґрумінгу можна здійснювати:

- огляд веб-сайту;
- контроль за вчиненням злочину у формі спеціального слідчого експерименту із використанням апаратних та програмних засобів фіксації;
- тимчасовий доступ до речей і документів;
- зняття інформації з транспортних телекомунікаційних мереж;
- зняття інформації з електронних інформаційних систем.

Аналіз форм документування процесу огляду інформації, яка не має обмеження доступу встановленого її володільцем та зберігається в електронному вигляді, в різних регіонах України засвідчує, що існують два головних підходи в цьому питанні. Перший полягає у відповідному документуванні з викорис-

танням протоколу огляду. У другому випадку процес документування оформлюється протоколом негласної слідчої (розшукової) дії щодо зняття інформації з електронних інформаційних систем, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту, а тому не потребує дозволу слідчого судді (ч. 2 ст. 264 Кримінального процесуального кодексу України). Різниця в підходах пояснюється суперечностями щодо належності інформації в електронній формі до місцевості, приміщення, речей або документів, щодо яких можна здійснювати огляд (ч. 1 ст. 237 Кримінального процесуального кодексу України). Водночас більшість правоохоронних органів в регіонах все ж тяжіють до використання першого підходу – оформлення електронних доказів протоколом огляду.

**Список використаних джерел:**

1. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій (Проект): навчальний курс / [В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков]. К., 2015. 158 с.
2. Cybercrime and its victims / Edited by Elena Martellozzo, Emma A Jane. 2017. Routledge. 230 p.
3. British paedophile Paul Leighton jailed for 16 years for rape. URL: <https://www.theguardian.com/uk-news/2017/sep/04/british-paedophile-paul-leighton-jailed-for-16-years-for-rape> (дата звернення: 22.09.2017).

*Одержано 30.10.2017*

**УДК 343.13**

**Євгеній Олександрович НАЛИВАЙКО,**

*кандидат юридичних наук, викладач відділу підготовки прокурорів з нагляду за додержанням законів органами, які проводять оперативно-розшукову діяльність, дізнання та досудове слідство Національної академії прокуратури України*

**КРИМІНАЛІСТИЧНІ ТА ПРОЦЕСУАЛЬНІ ОСОБЛИВОСТІ У ЗЛОЧИНАХ ПОВ'ЯЗАНИХ ІЗ КІБЕРЗЛОЧИННІСТЮ**

На актуальність та необхідність теми вдосконалення боротьби з кіберзлочинністю вказує кількість злочинів у даній сфері яка постійно зростає.

Відповідно до принципів сучасного міжнародного кримінального права злочини з використанням комп'ютерних технологій (інакше «кіберзлочини») віднесені до злочинів міжнародного характеру. Перелік видів кіберзлочинів визначається