О. А. Самойленко,
к. ю. н., доцент, доцент кафедри криміналістики
Національного Університету «Одеська юридична академія».

ДО ПИТАННЯ ПРОТИДІЇ СУЧАСНІЙ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ У КІБЕРПРОСТОРІ

Нині соціальні мережі створили безмежні можливості для об'єднання віддалених одна від одної (часто безпосередньо не знайомих) осіб з метою спільної злочинної діяльності – у кримінологічному сенсі, для ефективної діяльності утворених організованих злочинних угруповань – у криміналістичному. Адже скоєння терористичних актів, контрабанда, незаконний обіг наркотичних засобів, поширення порнографії; піратства та інших транснаціональних злочинів потребує технічного, матеріального й організаційного супроводження, що повною мірою забезпечують можливості кіберпростору. Тому організована злочинність активно використовує обстановку кіберпростіру для досягнення злочинної мети.

Питанням виявлення й розслідування злочинів, вчинених організованими групами у сфері інформаційних (комп'ютерних) технологій, присвятили свою увагу П. Д. Біленчук, В. Б. Вєхов, Ю. В. Гаврилін, В. О. Голубєв, М. В. Гуцалюк, О. І. Котляревський, Л. П. Паламарчук, М. В. Салтевський, В. С. Цимбалюк та багатьох інших науковців. При цьому більшість з них придавали глибокому криміналістичному аналізу комп'ютерні злочини або кібертероризм. Проте можна константувати, що для організованих груп саме у кіберпросторі існують необмежені можливості для вчинення злочинів іншої кримінально-правової кваліфікації.

За офіційними даними Генеральної прокуратури України на території України у 2014 році було зареєстровано 418 кримінальних проваджень за ознаками лише злочинів у сфері використання ЕОМ (комп'ютерів), систем і комп'ютерних мереж; у 2015 році –556; у 2016 році – 818 [1]. Це свідчить про необхідність підвищення ефективності розслідування таких злочинів та необхідність впровадження нових способів протидії організованої злочинності у кіберпросторі.

Сучасний користувач комп'ютерних мереж має можливість здійснювати різноманітні дії в модельованому комп'ютером електронному просторі в реальному часі (наприклад, під час комп'ютерних ігор у мережі, спілкування в соціальних мережах). Ці дії створюють так звану «віртуальну реальність» або «реальну вертуальність». Це система, в якій реальність як така (матеріальне або символічне існування людей) повністю занурена у віртуальні образи, вигаданий світ, у якому зображення не просто перебуває на екрані, через який передається досвід, але й саме стає досвідом [2, с.22; 3, с.351].

У сучасних словниках поняття «віртуальна реальність» подано у вузькому й широкому сенсі [4; 5]. У вузькому розумінні – це ті ігрові або необхідні в технічному плані «штучні реальності», які виникають унаслідок впливу комп'ютера на свідомість, коли, наприклад, на людину одягають «електронні окуляри» й «електронні рукавички». У широкому – це будь-які змінені стани свідомості, як-от: шизофренічні марення, наркотичне чи алкогольне сп'яніння, гіпнотичний стан, ігроманія. Шляхом використання різних комп'ютерних аудіовізуальних технологій людина може реалізовувати свою комунікативну функцію, контактувати не лише з іншими людьми, а й зі штучними персонажами, створеними іншими особами, з метою використання цих образів для подальшого вчинення злочину. Тож, віртуальність – це одна з ознак кіберпростору, особливість, яка приваблює злочинців для його використання в механізмі вчинення злочину.

Цю ж ознаку – віртуальність кібепростору – вдало можна використовувати й для протидії відповідній злочинності. Розуміючи можливості кожного Інтернет-ресурсу і вміючи використовувати їх у своїх інтересах, для правоохоронців набагато більше шансів успішно протидіяти організованій злочинності, вчасно повідомляти користувачів мережі про сучасні способи вчинення злочинів у мережі, поширювати іншу важливу для слідства інформацію серед мільонів людей.

Сучасне реформування в Україні правоохоронних органів призвело до створення підрозділів боротьби з кіберзлочинністю. На підставі Постанови Кабінету Міністрів «Про утворення територіального органу Національної поліції» від 13 жовтня 2015 року за № 831 створено Департамент кіберполіції. Наказом Національної поліції від 10 листопаду 2015 року № 85 було затверджено Положення про Департамент кіберполіції Національної поліції України, проведено атестацію відповідних співробітників.

Цій департамент має відповідний Інтернет-ресурс, зокрема свій сайт, сторінки у соціальних мережах facebook та twitter. Останні насьогодні налічують відповідно 7511 та 1100 тільки зареєстрованих читачів. Через вказані Інтернет-ресурси кіберполіцейські України також дають можливість користувачам мережі у режимі зворотного зв'язку повідомити про вчинений злочин, перевірити підозрілий сайт (url-адресу ресурсу), номер телефону чи реквізити банківської карточки. Цінність наведеного для протидії сучасній організованій злочинності у кібепросторі не викликає сумніву.

Але функції існуючих насьогодні Інтернет-ресурсів кіберполіції України дозволяють попередити вчинення злочинів у кібепросторі стосовно осіб, які слідкують за новаціями у правоохоронній сфері та є обережними користувачами мережі. Виникає питання щодо необізнаних користувачів, а також суб'єктів відносин у мережі, що часто стають об'єктом

злочинних посягань у мережі (кібератак різноманітних сервісів, банків, підприємств у певній сфері діяльності тощо). Тут можна звернути увагу на практику поліцейських інших держав у протидії кібезлочинам.

У 2001 році Федеральне бюро розслідувань США розпочало програму запобігання комп'ютерних злочинів Infra Guard, розроблену центром із захисту національної інфраструктури (Національний центр захисту інфраструктури) [6]. Однією з цілей програми є створення захищеної від вторгнення ззовні мережі для обміну інформацією між компаніями та органами забезпечення правопорядку про здійснені атаки та надання відомостей, які можуть попередити такі зазіхання. Однак деякі експерти вважають, що контроль з боку ФБР спричиняє недоступність інформації іншим учасникам. Це зумовлює появу інших подібних програм. Так, американські комп'ютерні корпорації Miscrosoft, Oracle, AT&T, Intel та 15 інших компаній створили центр обміну інформацією по боротьбі з комп'ютерною злочинністю (Information Technology Information Sharing and Analysis Center).

Такі програми та центри можна назвати по-суті криміналістичними засобами профілактики організованої кібезлочинності. Нажаль в Україні таких мереж не застосовують, хоча є реальна необхідність у цьому. Адже, хакер, що дії в складі організованої групи, доволі нечасто потрапляє в поле зору кримінального судочинства, оскільки для вчинення злочину використовує нетиповий, постійно вдосконалюваний, специфічний набір операцій у комп'ютерних мережах. Організований характер злочину забезпечує якісне його приховування, особливо з врахуванням транскордонної складової такої злочинної діяльності.

На прикінці зазначимо, у питаннях протидії сучасній організованій кіберзлочинності особливого значення набуває сама мережа Інтернет. Одна з особливих її ознак, така як віртуальність, дає можливість використовувати Інтернет-ресурси, комп'ютерні програми та системи, віртуальні центри у механізмі протидії злочинам, вчиненим організованими групами.

Література:

1. Статистика ГП України [Електронний ресурс] // Режим доступу : http://www.gp.gov.ua/ua/stst2011.html?dir_id=111482&libid=100820

2. Кормич Б. А. Інформаційне право : підручник / Б. А. Кормич. – Харків : БУРУН і К°, 2011. – 334 с.

3. Кастельс М. Информационная эпоха: экономика, общество, культура : пер. с англ. / М. Кастельс; под науч. ред. О. И. Шкаратана. – М. : ГУ ВМЭ, 2000. – 606 с.

4. Heim M. The Metaphysics of Virtual Reality // Virtual Reality: Theory, Practiceand Promise / M. Heim ; Ed. S. K. Helsel, J. P. Roth. – Westport, London : Meckler,1991. – P. 27–33.

5. Носов Н. А. Словарь виртуальных терминов / Н. А. Носов // Труды лаборатории виртуалистики. Труды Центра профориентации. Вып. 7. – М. : Путь, 2000. – 69 с.

6. Infra Guard [Електронний ресурс] // Режим доступу : https://www.youtube.com/watch?v=8pobZWHnplc

Д. В. Собко,
Студент 2-го курсу факультету №2
ННІЗДН Одеського державного
університету внутрішніх справ
П. В. Романько,
к. ю. н., доцент кафедри
адміністративної діяльності ОВС та
економічної безпеки Одеського державного
університету внутрішніх справ

ЩОДО ПРАВОВОГО РЕГУЛЮВАННЯ ФІНАНСОВОГО МОНІТОРИНГУ В НОТАРІАЛЬНІЙ ДІЯЛЬНОСТІ В УКРАЇНІ

Для з'ясування поняття і змісту правового регулювання фінансового моніторингу в нотаріальній діяльності слід насамперед звернутися до доктринальних положень адміністративного права.

Відтак у теорії права під правовим регулюванням розуміють здійснення за допомогою системи правових засобів (юридичних норм, правовідносин, індивідуальних приписів та ін.) результативного нормативно-організаційного впливу на суспільні відносини з метою їх упорядкування, охорони, розвитку відповідно до суспільних потреб чинного соціального устрою [1, с. 210].

У свою чергу в юридичній енциклопедії правове регулювання визначається як здійснюваний державою за допомогою всіх юридичних засобів владний вплив на суспільні відносини з метою їх упорядкування, закріплення, охорони й розвитку, а також вплив на поведінку та свідомість громадян через проголошення їхніх прав та обов'язків, установлення певних дозволів і заборон, затвердження певних правових актів тощо [4, с. 369].

Як справедливо зауважує А. Коренєв, правове регулювання – це процес послідовного використання адміністративно-правових засобів для досягнення цілей регулювання поведінки учасників суспільних відносин [3, с. 60].

Як бачимо, між вищезазначеними дефініціями вчених з приводу правового регулювання суттєвих відмінностей немає. Усі вони виділяють у визначенні правового регулювання два обов'язкових елементи: владний