

Харкевич Олексій Олександрович,
здобувач наукової лабораторії з проблем
досудового розслідування Національної
академії внутрішніх справ

МЕРЕЖА ІНТЕРНЕТ ЯК СЕРЕДОВИЩЕ ВЧИНЕННЯ ОКРЕМИХ ВИДІВ ЗЛОЧИНІВ МІЖНАРОДНИМИ ЗЛОЧИННИМИ ОРГАНІЗАЦІЯМИ

Широке використання мережі Інтернет для оптимізації та автоматизації процесів у всіх без винятку сферах життєдіяльності призвело до нівелювання кордонів і глобалізації економіки та інформаційно-телекомунікаційної інфраструктури держав.

Разом з цим, мережа Інтернет активно використовується міжнародними злочинними організаціями як засіб вчинення злочину. Сьогодні підшукування або пристосування засобів знарядь, підшукування співучасників або змова на вчинення окремих злочинів не потребує безпосередньої присутності злочинця на території, де він буде вважатися закінченим. Новітні інформаційні технології дозволяють учасникам транснаціональної злочинної організації забезпечувати свою анонімність в умовах незначного ризику, а це надає їм можливість залучати все більше людей до злочинної діяльності. Тому на сучасному етапі актуальним є питання протидії транснаціональній організованій злочинності, яка вчиняється з використанням мережі Інтернет.

Інформаційні технології викликали появу нових умов, котрі використовуються організованими злочинними групами для скоєння злочинів на національному, міжнародному і транснаціональному рівнях. Злочинні об'єднання, окремі «фахівці» кримінального бізнесу у повну міру використовують новітні технології для «відмивання» грошей, здобутих злочинним шляхом, несанкціонованого доступу до інформаційних систем тощо [1]. Особливості цього виду злочинності полягає у:

- відносній комфортності, тобто готування та скоєння злочину здійснюється практично на «робочому місці»;
- доступності – у зв'язку з тенденцією постійного зниження цін на комп'ютерну техніку;

– географії скоєння злочинів, яка є досить широкою, але враховуючи те, що основна кількість комп'ютерів розташована у великих населених пунктах, то саме на них і припадає «левова частка» злочинності;

– віддаленості об'єкту злочинних посягань – він може знаходитись за тисячі кіло- метрів від місця скоєння злочину; – складності виявлення, фіксації і вилучення криміналістично значущої інформації (слідової картини злочину) при виконанні слідчих дій для використання її як речовий доказ тощо.

Відповідно до оцінок експертів, злочинність у мережі Інтернет здатна нанести збитки, які можливо порівняти з обсягом крадіжки виробів мистецтва в усьому світі. За даними ООН, збитки, які наносить така злочинність, можна порівняти з доходами від протизаконного обігу наркотиків і зброї. Крім того, дана злочинність виступає стримуючим фактором розвитку конкуренто-спроможності економіки країн світу, в тому числі й України, оскільки покупці, підприємства та банки з пересторогою використовують нові технології – Інтернет-послуги [2, с. 338–339]. Така ситуація спричинена розширенням транснаціональними злочинними організаціями масштабів своєї діяльності завдяки використанню мережі Інтернет. Зокрема, на думку зарубіжних експертів, кількість неліцензійних сайтів у мережі Інтернет наразі більш ніж у десять разів перевищує ліцензійні. Значна кількість сайтів сьогодні працюють тільки в «Чорному Інтернеті», а також використовують Інтернет як спосіб розрахунку віртуальною валютою чи електронними грошима. Як зазначає голова Європейського центру по боротьбі з кіберзлочинністю Трулс Ертінг: «Майже вся організована злочинність отримує прибуток у реальному світі за допомогою використання «віртуального світу». Гроші, як правило, відмиваються в три етапи: розміщення (завантаження) – розшарування (класифікація, диференціація) та інтеграція. Гроші за допомогою мережі Інтернет постійно перебувають в обігу як усередині країни, так і між державами [3].

Крім того, дослідження RandCorporation показало, що завдяки піратським сайтам злочинці заробляють навіть від такого легітимного доходу, як реклама, більш ніж 220 млн дол. США на рік. За оцінками експертів, організовані злочинні групи мають близько 4–5 млрд дол. США прибутку від продажу контрафактних компакт-дисків. Також RandCorporation

опублікувала доповідь щодо вивчення зв'язку між піратством, організованою злочинністю та тероризмом. Так, у даній доповіді містилися переконливі матеріали щодо широкого, географічно розподіленого і постійного зв'язку між кінопіратством та організованою злочинністю, а також докази того, що терористичні групи, такі як Хезболла, використовували доходи від піратства фільмів для фінансування своєї діяльності [4].

Список використаних джерел

1. Кіберзлочинність в Україні: перспективи протидії [Електронний ресурс]. – Режим доступу: http://kpk.org.ua/2007/02/05/kberzlochinnst_v_ukran_perspektivi_protid.html.
2. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби [Електронний ресурс] // Н. В. Савчук. – 2009. – С. 338–342. – Режим доступу: http://tppe.econom.univ.kiev.ua/data/2009_19/zb1_9_48.pdf.
3. Cybercrime: getting paid and getting away with it / [Electronic resource]. – Mode of access : <http://www.globalinitiative.net/cybercrimegetting-paid-and-getting-away-with-it/>.
4. Entertainment piracy: fair game, or organized crime? / [Electronic resource]. – Mode of access : <http://www.globalinitiative.net/online-piracy/>.