DOI (Issue): https: //doi.org/10.36486/np.2020.1(47) Issue 1(47) 2020

УДК 343.9:004.738.5-053.6

Лубенець Ірина Григорівна,
кандидат юридичних наук, провідний науковий співробітник
ДНДІ МВС України, м. Київ, Україна
ORCID ID 0000-0003-2597-0356
Толочко Галина Василівна,
старший науковий співробітник ДНДІ МВС України, м. Київ, Україна
ORCID ID 0000-0003-2913-9439
Наумова Ірина В'ячеславівна,
старший науковий співробітник ДНДІ МВС України, м. Київ, Україна
ORCID ID 0000-0002-6643-0375

ІНТЕРНЕТ-РИЗИКИ ТА ЗАГРОЗИ ЩОДО НЕПОВНОЛІТНІХ КОРИСТУВАЧІВ: КРИМІНОЛОГІЧНИЙ АСПЕКТ[1]

Стаття присвячена комплексному аналізу ризиків та загроз, джерелом яких є сучасні засоби комунікації та мережа Інтернет. Метою дослідження є встановлення певних аспектів уразливості дитини в інформаційній сфері, а також з'ясування рівня обізнаності школярів щодо безпеки в мережі Інтернет.

У статті перелічені основні особливості та найбільш поширені види злочинів та інших антисуспільних діянь, що вчиняються в мережі Інтернет або з її використанням. Особлива небезпека таких діянь полягає в тому, що часто жертвами стають неповнолітні інтернет-користувачі, адже вони є найактивнішими користувачами Інтернету та інших засобів комунікації.

Ключові слова: *Інтернет, інтернет-ризики, користувачі, неповнолітні, діти, ґаджети, кібернасильство, інтернет-шахрайство, порнографія, "групи смерті".*

На сьогодні злочини, а також протиправні, антисуспільні діяння, що вчиняються з використанням сучасних засобів комунікації та мережі Інтернет, – це актуальна проблема, з якою зіштовхнулися всі країни у XXI столітті, яка має тенденцію до збільшення як за своїми масштабами, так і за рівнем спричиненої шкоди. Отже, назване явище заслуговує на особливу увагу серед науковців.

Слід зазначити, що дослідженню кіберзлочинності (комп'ютерної злочинності) та її похідних присвятили свої роботи різні науковці, зокрема: В.А. Ліпкан, О.О. Тихомиров, О.М. Пфо, М.А. Погорецький, В.П. Шеломенцев, О.С. Алавердов, Ю.М. Батурін, А.В. Войцехівський, В.Б. Вєхова, В.О. Голубєв, М.Д. Діхтяренко, Т.Л. Тропіна, Б.Х. Толеубеков, Т.М. Барабаш, Р.С. Бєлкін, С.Д. Бражник, С.Ю. Битко, В.В. Воробйов, Н.Л. Волкова, Л.В. Борисова, А.Ф. Волобуєв, М.Т. Дзюба, Я.М. Жарков, Р.А. Калюжний, А.М. Кузьменко, В.К. Лисиченко, П.А. Лупінська, М.І. Онищук, С.В. Слинько, В.П. Філонов та інші.

[1] Закінчення в наступному номері.

DOI (Article): https: //doi.org/10.36486/np.2020.1(47)

Злочини, вчинені в мережі Інтернет або з її використанням (кіберзлочини), інші антисуспільні діяння (не криміналізовані дії, які спричинюють шкоду особі – спам, кібербулінг тощо), що вчиняються з використанням сучасних засобів комунікації (наприклад, мобільних телефонів, планшетів, інших сучасних ґаджетів) – це явища, які виникли у процесі еволюції комп'ютерних та інформаційних технологій. Тобто жертвою зазначених вище протиправних діянь може бути будь-яка людина, що користується сучасними засобами комунікації або мережею Інтернет. Особлива небезпека таких діянь полягає в тому, що часто їх жертвами стають неповнолітні, бо, як зазначалося вище, вони є найактивнішими користувачами Інтернету та інших засобів комунікації. Слід наголосити, що більше 70 % батьків не знають, які сайти відвідують їх діти.

Однією з основних характеристик інтернет-злочинності є висока латентність як природна, так і штучна, що виникає через небажання потерпілих повідомляти про злочини правоохоронним органам. Офіційна статистика правоохоронних органів не відображає реальної картини стану правопорушень, що вчиняються в мережі Інтернет, або за її допомогою, як на рівні держави, так і на загальносвітовому рівні. Для оцінювання стану такого виду злочинності необхідно використовувати інші способи одержання даних, такі як інтерв'ювання, фокусні групи, огляди, а також метод "реєстрації звернень" – віктимологічний метод, що полягає у збиранні відомостей про злочини від потерпілих. Використання цих методів поряд з аналізом офіційної статистики дає змогу дослідити справжні масштаби інтернет-злочинності та її тенденції з урахуванням злочинів, що залишилися незареєстрованими правоохоронними органами.

Основними особливостями злочинів та інших антисуспільних діянь, що вчиняються в мережі Інтернет або з її використанням, є такі:

– відносна комфортність, тобто готування та скоєння злочину здійснюється практично не відходячи від "робочого місця";

– доступність, зумовлена тенденцією постійного зниження цін на комп'ютерну техніку та засоби комунікації;

– віддаленість об'єкта злочинних посягань, який може перебувати за тисячі кілометрів від місця скоєння злочину;

– велика множинність кіберзлочинів, яка полягає в тому, що суб'єкт злочину за допомогою комп'ютерних технологій протягом короткого періоду часу може вчинити декілька тисяч протиправних діянь;

– складність виявлення, фіксації і вилучення криміналістично-значущої інформації (слідової картини злочину) при виконанні слідчих дій для використання її як речового доказу і т. ін.;

– велика швидкість вчинення кіберзлочинів, які відбуваються практично миттєво і тому потребують швидкої реакції у відповідь;

– постійне оновлення форм та способів вчинення кіберзлочинів, яке здійснюється на тлі вдосконалення інформаційних технологій. Це вкрай ускладнює визначення ступеня та географії поширеності зазначених злочинів, прогнозування тенденцій змін її параметрів [1, с. 130].

На сьогодні найпоширенішими видами кіберзлочинів та інших протиправних діянь, що вчиняються в мережі Інтернет або з її використанням, є: розповсюдження

порнографії (у тому числі дитячої), шахрайство (фітинг), наркозлочинність, схиляння до самогубства шляхом психологічного впливу, секстинг (інтимне листування), шантаж, грумінг (входження в довіру до дитини з метою подальшої особистої зустрічі для вступу в сексуальні відносини, експлуатації чи шантажу), а також кібернасильство (кібербулінг), пропаганда насильства та жорстокості, некриміналізований спам тощо.

Наркозлочинність в мережі Інтернет. Революція в галузі інформаційних технологій призвела до того, що в сучасний період проблема розповсюдження наркотиків у світі дедалі частіше перетинається з можливостями сучасних технологій, у тому числі Інтернету, за допомогою якого у будь-яку точку світу можна надіслати інформацію про купівлю-продаж наркотиків, про нові розробки у виготовленні, культивації, їх транспортуванні тощо. Мережа Інтернет дає можливість встановлювати контакти між виробниками наркотиків, їх продавцями та клієнтами з географічних пунктів значно віддалених один від одного. Глобальна інформаційна мережа дозволяє також особам, зацікавленим у поширенні наркоманії, залучати користувачів Інтернету до вживання наркотиків безпосередньо і популяризувати субкультури, пов'язані з вживанням наркотиків. Слід підкреслити, що неповнолітні особи складають основну соціальну групу, в якій постійно пропагується вживання наркотичних засобів, зростає кількість їх споживачів та розповсюджувачів.

Слід зазначити, що офіційна статистика щодо наркозлочинності в мережі Інтернет у цей час відсутня. За результатами соціологічного опитування "Куріння, вживання алкоголю та наркотичних речовин серед підлітків, які навчаються: поширення й тенденції в Україні", проведеного ГО "Український інститут соціальних досліджень імені Олександра Яременка" у 2019 році в межах міжнародного проєкту "Європейське опитування учнів щодо вживання алкоголю та інших наркотичних речовин", частка підлітків, які вживали наркотики, склала 18 %, причому серед дівчат вона зросла в 1,5 рази у порівнянні з 2015 роком. 8,7 % підлітків пробували марихуану, а 9,2 % вживали інгалянти. Поширеність полінаркоманії (вживання двох і більше шкідливих речовин) серед усіх опитаних становить 4,2 % [2].

Раніше підлітки отримували доступ до наркотиків через наркопритони, а на сьогодні за допомогою Інтернету можна знайти та купити будь-які наркотичні препарати та отримати їх через систему "закладок". У цей час найбільш зручним і поширеним способом пошуку інформації про наркотики є запити через пошукові системи (такі як Google, Мета тощо). Дослідження посилань, знайдених за допомогою зазначених вище пошукових систем, свідчать про те, що потрапити на пронаркотичні сайти нескладно.

За результатами анкетування учнів закладів загальної середньої освіти м. Києва та Київської області, майже кожний четвертий з опитаних нами школярів (24,4 %) зіштовхувався з пропозицією придбати алкоголь чи наркотики. До речі, хлопцям удвічі частіше надходять такі пропозиції, ніж дівчатам (61,6% проти 37,1% відповідно)[2].

[2] Дослідження проводилось у Державному науково-дослідному інституті МВС України. Воно спрямоване на встановлення сучасних шляхів запобігання злочинам та іншим антисуспільним діянням щодо неповнолітніх, які вчиняються з використанням сучасних засобів комунікації та мережі Інтернет. Усього опитано 787 учнів 6–11 класів (вік опитуваних – 11–17 років, серед респондентів – 427 (54,3 %) хлопців та 347 (44,1 %) дівчат).

Інтернет-шахрайство. До найбільш поширених в Інтернеті видів шахрайства належать:

– *фальшиві рахунки на оплату з Інтернет-магазинів або інші повідомлення* – підроблені рахунки, що розсилаються по e-mail, містять посилання на шкідливі програми. Одержувач, який відкрив рахунок, миттєво стає жертвою зловмисних дій. Суб'єктом посягання, як і потерпілим, може бути будь-яка особа (неповнолітні в тому числі);

– *шахрайський Інтернет-магазин* або продаж неіснуючого товару за допомогою сайтів для безкоштовних приватних оголошень. Ця схема схожа на схему, за якою діють фірми-однодневки. Шахрай відкриває такий магазин (або розміщує оголошення), за вигідними цінами пропонує товар. Приймається передоплата, шахрай зникає, привласнивши гроші. Суб'єктом скоєння злочину як і потерпілим також може бути особа будь-якого віку. Головна умова – доступ до мереж Інтернет. Неповнолітні можуть бути жертвами в тому випадку, якщо у них є власні кошти для здійснення інтернет-купівель;

– *фітинг* – вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказування або обміну валюти, Інтернет-магазинів. Шахраї використовують усілякі виверти, які найчастіше змушують користувачів самостійно розкрити конфіденційні дані – наприклад, посилаючи електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в Інтернеті, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів. Потерпілими від такого виду злочину майже завжди виступають дорослі.

Однак, схожою схемою шахрайства, яка використовується часто до неповнолітніх, є ***соціальний інжиніринг.*** Цей термін в останні роки вживається для позначення дій, в ході яких під виглядом довірливого інтернет-спілкування дитина повідомляє зловмиснику інформацію конфіденційного характеру (доходи батьків, адреса, розпорядок дня, наявність сигналізації в домі, номери карток та ін.).

Нерідко, встановлюючи будь-які додатки, користувачі не звертають уваги на дозволи доступу, які будуть надаватися розробникам або власникам цього додатку, що дає можливість шахраям скористатися можливістю безперешкодного доступу до фото, особистих даних власника мобільного телефону;

– *крадіжка послуг* – правопорушення з отримання несанкціонованого доступу до будь-якої системи, щоб безкоштовно скористатись її послугами. Прикладом цього виду шахрайства є фоунфрейкинг, тобто використання комп'ютера для проникнення в комунікаційну телефонну систему та незаконне використання послуг з надання міжнародного телефонного зв'язку;

– *підроблені сайти благодійних фондів* або смс-повідомлення з проханням про фінансову допомогу або неіснуючий виграш. "Збираємо на протези для бійців АТО!", "Допоможіть жертвам урагану Катріна"!, "Ви виграли авто", "Ви не отримали свій приз" тощо. Особливо актуальними такі методи відбирання грошових коштів стають у святковий сезон, коли відвідувачі мережі більш охоче розлучаються з грошима, а також сильнішою є жага користувачів до швидкого збагачення;

– *Інтернет-кардинг* – використання даних з чужої банківської картки для здійснення всіляких операцій у мережі з метою отримання грошей. Жертві

надсилається повідомлення від "служби безпеки" банку або надходить дзвінок від "працівника" банку нібито оновити дані (підвищити ступінь захисту банківського рахунку тощо) та вимагають назвати номер картки, пароль, кодове слово тощо.

Слід вказати, що 16 % опитаних працівниками Державного науково-дослідного інституту МВС України школярів повідомили, що відносно них здійснювались шахрайські дії або крадіжка коштів за допомогою Інтернету.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Європіна І.В. Види протиправних діянь у сфері новітніх інформаційних технологій. Вісник Академії адвокатури України. 2010. № 3(19). С. 129–136.

2. Українські підлітки стали менше курити, проте вживання алкоголю, доступ до наркотичних речовин та залежність від соціальних мереж зростають. *UNICEF*.URL: https://www.unicef.org/ukraine/uk/espad2019 (дата звернення: 18.11.2019).

REFERENCES

1. *Yevropina I.V.* (2010) Vydy protypravnykh diian u sferi novitnikh informatsiinykh tekhnolohii. "Types of illegal activity in the field of the latest information technologies". Bulletin of the Academy of Advocates of Ukraine 3(19), P. 129–136 [in Ukrainian].

2. Ukrainski pidlitky staly menshe kuryty, prote vzhyvannia alkoholiu, dostup do narkotychnykh rechovyn ta zalezhnist vid sotsialnykh merezh zrostaiut. "Ukrainian teenagers have begun to smoke less, but alcohol consumption, access to drugs and dependence on social networks are growing". UNICEF. URL: https://www.unicef.org/ukraine/uk/espad2019 (date of application: 18.11.2019) [in Ukrainian].

UDC 343.9:004.738.5-053.6

Lubenets Iryna,
Candidate of Juridical Sciences, Leading Researcher,
State Reserch Institute MIA Ukraine, Kyiv, Ukraine
ORCID ID 0000-0003-2597-0356
Tolochko Halyna,
Senior Researcher, State Reserch Institute MIA Ukraine, Kyiv, Ukraine
ORCID ID 0000-0003-2913-9439
Naumova Iryna,
Senior Researcher, State Reserch Institute MIA Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-6643-0375

INTERNET RISKS AND THREATS TO MINOR USERS: CRIMINOLOGICAL ASPECT

A variety of means of communication and the Internet are an integral part of the life of modern society in general and children in particular. In turn, the information environment has significant potential for the development and self-realization of a child's personality. Using the resources of open digital repositories of libraries, museums, sites of an educational, cognitive and entertaining nature, modern schoolchildren are able to download digitized books, music, photographs, etc. Thanks to modern technical means, children communicate with friends and have a rest. That is, the means of

communication and the Internet for them is part of life, and the virtual world is a means of socialization.

Since the Internet has become as accessible as the telephone, studying its impact on minors is a pressing issue today. On the one hand, it is a means of increasing erudition and communication skills, and on the other hand, it is a situation of increased risk of facing some threats of the virtual world from cyber-violence and fraud to the distribution of narcotic substances and the propensity to commit suicide.

This article is devoted to a comprehensive analysis of risks and threats, the source of which is modern means of communication and the Internet. The aim of the study is to establish certain aspects of the vulnerability of the child in the information sphere, as well as to determine the level of awareness of schoolchildren about safety on the Internet.

The article lists the main features and the most common types of crimes and other antisocial acts committed on the Internet or with its use. A particular danger of such acts is that often underage Internet users become victims, because they are the most active users of the Internet and other means of communication. In this regard, there is a need for further investigation of this problem from a criminological point of view to clarify the causes and conditions of the above crimes and antisocial actions, which, in turn, will help to increase the effectiveness of their prevention measures.

Keywords: Internet, Internet risks, users, minors, children, gadgets, cyber violence, Internet fraud, pornography, “death groups”.

Отримано 20.02.2020