

кваліфікуючих ознак. Уважаємо, що це не тільки буде справедливо, але також стимулюватиме правоохоронні органи встановлювати ці інші ознаки, а не зупинятись лише на тій, що пов'язана із залученням дитини або дією проти неї.

Список бібліографічних посилань

1. Кулик С. Г. Кримінологічна характеристика та запобігання злочинам проти моральності : дис. ... канд. юрид. наук : спец. 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право». Запоріжжя, 2016. 266 с.

2. Генеральна прокуратура України : офіційний веб-сайт. URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=104402 (дата звернення: 17.10.2018).

3. Кримінальний кодекс України від 5 квіт. 2001 р. *Відомості Верховної Ради України*. 2001. № 25-26.

4. Про захист суспільної моралі : Закон України від 20 лист. 2003 р. *Відомості Верховної Ради України* від 02 квітня 2004 року, № 14.

Одержано 18.10.2018

УДК 343.97:004.056+65.012.8

Лариса Віталіївна ЗУБ,

начальник управління ювенальної превенції

Департаменту превентивної діяльності Національної поліції України;

Олексій Михайлович РВАЧОВ,

старший викладач кафедри кібербезпеки факультету № 4 (кіберполіції)

Харківського національного університету внутрішніх справ;

ORCID: <https://orcid.org/0000-0002-3500-9393>

СУЧАСНІ ЗАГРОЗИ СІМЕЙНИЙ ОНЛАЙН БЕЗПЕЦІ: КЛАСИФІКАЦІЯ ТА ПРОФІЛАКТИКА ВИНИКНЕННЯ

Сьогодні інформаційні технології та Інтернет в прямому і переносному сенсі вмонтовані і інтегровані в життя кожної людини і вже давно стали впливати практично на всі процеси її життєдіяльності.

Так за даними компанії «InMind Factum Group Ukraine» у II кварталі 2018 року в Україні Інтернетом користувалось хоча б 1 раз на місяць та частіше 65 % населення (особи віком від 15 років та старші). 67 % українських користувачів мають доступ до мережі Інтернет вдома.

При цьому серед жителів:

– міст з населенням більше 100 тис. чоловік 75 % регулярно користуються Інтернетом;

– міст з населенням менше 100 тис. чоловік – 65 % є користувачами Інтернету;

– сільської місцевості – тільки 53 % користувачів.

Серед українських жінок регулярно користуються Інтернетом 52 %, а серед чоловіків – тільки 48 %.

Серед населення регулярно користуються Інтернетом особи у віці:

- від 15 до 24 років – 94%;
- від 25 до 34 років – 94%;
- від 35 до 44 років – 84%;
- від 45 до 54 років – 66%;
- від 55 до 65 років – 44%;
- від 65 років та старші – 15%.

В Україні 99% учнів та студентів регулярно користуються Інтернетом.

За даними дослідження українські інтернет-користувачі отримують доступ до мережі за допомогою:

- мобільних телефонів або смартфонів – 57%;
- домашніх ноутбуків – 45%;
- стаціонарного домашнього комп'ютера – 39%;
- планшету – 15%;
- стаціонарного комп'ютера на роботі – 5%;
- ноутбука на роботі – 5%;
- комп'ютера в гостях – 2%;
- комп'ютера за місцем навчання – 1%;
- комп'ютера в інтернет-кафе – 1%.

З наведених даних чітко видно, що найбільше (57 %) українців користуються Інтернетом через персональні мобільні пристрої та вдома за допомогою комп'ютерної техніки, тобто у так званих «зоні відповідальності рідних та близьких людей. У великій частині випадків люди немолодого віку, які є безпосередньо або побічно користувачами Інтернету (від 55 до 65 років – 44 %) і (від 65 років і старші – 15 %) потребують опіки більш молодого і просунутого покоління [1].

Станом на серпень 2018 року до найпопулярніших серед українських користувачів програмних додатків (ТОП-10) для мобільних пристроїв на базі операційної системи Android відносяться:

1. Viber, яким користуються 90% користувачів.
2. Приват 24 – 66%.
3. Facebook Messenger – 50%.
4. Google Play – 50%.
5. Instagram – 48%.
6. OLX – 42%.
7. Facebook – 41%.
8. Skype – 27%.
9. Вконтакте — 26%.
10. AliExpress – 25%.

Як бачимо серед користувачів найбільш популярними є додатки для обміну повідомленнями та соціальні мережі.

Найбільш популярними соціальними комп'ютерними мережами серед українців є:

1. Facebook – 54%.
2. Вконтакте — 32%.

3. Instagram – 27%.
4. Однокласники — 18%.
5. Twitter – 12%.

До найбільш популярних маркетплейсів (платформи для електронної комерції) в Україні відносяться:

1. OLX – 45%.
2. Rozetka – 38%.
3. Prom.UA – 40%.
4. Aliexpress – 18%.
5. Zakupki.com – 6% [2].

Очевидно, що використання дітьми та дорослими сучасних інформаційних технологій і засобів комунікації несуть не тільки поліпшення і полегшення, але і створюють певні ризики і загрози, через те, що різного роду зловмисники теж використовують інформаційні технології для вчинення протиправної діяльності. Зазвичай, основною метою таких зловмисників є отримання доступу до конфіденційної і особистої інформації користувачів (наприклад, паролів, банківських і персональних даних) та її подальше незаконне використання або протиправна маніпуляція з нею.

За результатами аналізу наукової літератури та повідомлень у ЗМІ про правопорушення у сфері використання інформаційних технологій, був сформований певний перелік сучасних загроз, що можуть виникати під час користування дітьми та дорослими сучасними інформаційними технологіями, у тому числі під час користування глобальною мережею Інтернет.

Ці загрози можна класифікувати за певними ознаками наступним чином:

1. Крадіжка, а саме:
 - особистих даних користувачів (наприклад, для отримання кредитів, створення фейкових акаунтів);
 - логінів та паролів доступу до сайтів (наприклад, для розсилки спаму, шантажування);
 - реквізитів банківських платіжних карток (кардінг);
 - змісту листування;
 - фотографій та відеозаписів приватного характеру;
 - тощо.
2. Незаконне заволодіння коштами користувача:
 - 1) через фейкові сайти:
 - інтернет-магазинів;
 - поповнення рахунків мобільних телефонів;
 - переказу грошей;
 - участі в розіграші товарів;
 - 2) шахрайські оголошення про продаж товарів та послуг в мережі Інтернет;
 - 3) тощо.

3. Несанкціонований збір та розповсюдження конфіденційної інформації про дітей та дорослих.

4. Доступ дітей до небажаного або забороненого контенту, а саме:

– порнографії, в тому числі дитячої;

– агресивної лексики;

– так званого «позитивного досвіду» вживання алкоголю, тютюну та наркотиків;

– азартних ігор;

– інформації про статеве виховання;

– тощо.

5. Психічний розлади:

– інтернет-залежність (нав'язливе бажання «вийти до Інтернету»);

– захоплення онлайн комп'ютерними іграми;

– інтернет-шопоголізм (неконтрольовані покупки);

– тощо.

6. Маніпуляція свідомістю дітей та дорослих:

– пропаганда: небезпечних субкультур, екстремістської та антисоціальної поведінки;

– спонукання до суїцидів («групи смерті» у соцмережах);

– залучення в небезпечні квести, ігри та розваги (наприклад, «зацепери», «руфери»);

– тощо.

7. Селфоманія та лайкоманія, що призводять до:

– дурних вчинків та витівок;

– смертельним наслідкам через необережність.

8. Появи у дитини «в друзях» незнайомих дорослих (зазвичай педофіли або шантажисти), які знайомляться з дітьми для подальшого:

– грумінгу (втирання у довіру);

– секстингу (інтимне листування й пересилка фото інтимного характеру);

– булінгу (цькування та погрози для морального приниження);

8. Порушення правил мережевого етикету:

1) кібербулінг, у тому числі дітьми відносно інших дітей (залякування, цькування чи знущання через Інтернет);

2) тролінг (провокація співрозмовника на емоційну відповідь);

3) мобінг (цькування у колективі співробітника з метою його звільнення);

які можуть призвести до:

– психічним розладам;

– нападів зворотної агресії, у тому числі із застосуванням зброї;

– суїцидальних наслідків.

За даними громадської організації «Ла Страда Україна» з січня 2017 року по червень 2018 року на Національну дитячу «гарячу» лінію було здійснено 11 421 дзвінків щодо безпеки в інтернет-мережі. Всього звернулося 10 621 дітей та 800 дорослих.

Найчастіше на дитячу «гарячу» лінію зверталися із проблемними питаннями, що стосувалися:

- комп'ютерна та інтернет-залежність – 2 877 рази;
- секстинг – 2 627 рази;
- тролінг – 1 532 рази;
- фішинг – 1 207 рази;
- грумінг – 1 047 рази;
- смертельні квести в соціальних мережах – 919 рази;
- мобінг – 697 рази;
- кібербулінг – 398 рази;
- кардинг – 122 рази [3].

Як бачимо використання сучасних інформаційних технологій та засобів комунікації несуть не тільки покращення продуктивності праці, доступ до знань та культурної спадщини людства, але й створюють певні загрози. При цьому деякі з цих загроз більш актуальні для дорослих, деякі – для дітей, але є і такі, які становлять загрозу для всіх користувачів Інтернету незалежно від їх віку.

В сучасних державних та комерційних організаціях, закладах чи установах питаннями захисту від кіберзагроз працівників, клієнтів та відвідувачів, зазвичай, займаються працівники штатних відділів інформаційної безпеки. Але через те, що згідно наведених вище даних, більшість користувачів «виходять» до мережі Інтернет саме вдома або з власних мобільних пристроїв, необхідно більшу увагу приділяти безпечному користуванню Інтернетом саме вдома, а профілактичні заходи повинні бути спрямовані саме на поінформовання дітей та їх дорослих та рідних щодо загроз, з якими вони можуть зіткнутися під час використання мережі Інтернет.

На сьогодні в Україні на державному, регіональному та місцевому рівнях не ведеться комплексна робота щодо інформування населення про сучасні загрози, що можуть виникати під час користування дітьми та дорослими сучасними інформаційними технологіями.

Є необхідність формування у населення так званого «імунітету» до кіберзагроз за рахунок проведення «інформаційного щеплення», метою якого є запобігання чи зменшення отримання населенням віртуальних та реальних травм та втрат.

Даною проблемою необхідно займатися не тільки на рівні певного міста чи області, а взагалі всієї країни – виходити на загальнодержавний рівень.

Виникає потреба у розробці комплексної програми «“Інформаційне щеплення” для дітей та дорослих щодо безпечного використання сучасних інформаційних технологій», яка повинна включати, окрім інформування населення про наведені загрози, а також містити перелік дієвих механізмів протидії вищенаведеним сучасним загрозам.

Така програма повинна бути, в першу чергу, апробована на рівні певного населеного пункту, а в разі отримання позитивних результатів,

можна говорити про спробу запровадження такої програми на рівні всієї України.

Список бібліографічних посилань

1. Проникновение Интернета в Украине. Май 2018 // Factum Group Ukraine. URL: https://inau.ua/sites/default/files/file/1806/ui_factum_group_ii_kvartal_2018.pdf (дата звернення: 26.10.2018).

2. Opinion Software Media. Данные работы Панели, Сентябрь 2018 // Factum Group Ukraine. URL: https://inau.ua/sites/default/files/file/1810/top-25_saytiv_u_veresni_2018.pdf (дата звернення: 26.10.2018).

3. Аналіз дзвінків щодо небезпеки в інтернет-мережі: січень 2017 – червень 2018 // Національна дитяча «гаряча» лінія. URL: <https://www.facebook.com/childhotline.ukraine/photos/a.262018927286975/1083823491773177/> (дата звернення: 26.10.2018).

Одержано 27.10.2018

УДК 343.14+004

Віталій Геннадійович КОЛЕСНИК,

завідувач відділу досліджень у сфері інформаційних технологій

Харківського науково-дослідного експертно-криміналістичного центру МВС України

ПРОБЛЕМИ ЗАКРІПЛЕННЯ ПОНЯТЬ ТА ВИЗНАЧЕННЯ МІСЦЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ

Широке використання комп'ютерної техніки та новітніх засобів комунікацій у сучасному світі викликає необхідність правового регулювання використання таких джерел в процесі доказування.

Одразу слід зупинитись на проблемі, вирішенням якої займається цілий ряд науковців, а саме – проблемі закріплення понять та термінів. Досліджувані поняття є досить новими, але вже привернули увагу таких вчених, як О. Г. Григор'єв, С. В. Васильєв, М. А. Іванов, Н. А. Зігура, Г. В. Кудрявцева, П. П. Зайцев та інші.

Сьогодні одночасно існують та застосовуються два на перший погляд тотожних поняття – «електронний доказ» та «цифровий доказ». Крім цього в нормативно-правових актах та юридичному обігу також зустрічаються поняття: «електронний (цифровий) носій», «цифрова інформація», «комп'ютерна інформація», «комп'ютерні об'єкти». Таке широке коло термінів, понять та категорій створює суперечності та неузгодженості в діючому законодавстві та плутанину, насамперед під час прийняття процесуальних рішень.

Аналізуючи застосування цих термінів у сучасному законодавстві можна побачити, що наразі термін «електронний доказ» є переважним, а термін «цифровий» при цьому додається в окремих випадках або як тотожна заміна терміну «електронний», або як доповнення до нього. На думку автора ці поняття не можуть бути