УДК 343.1
DOI https://doi.org/10.32844/2618-1258.2022.4.41

ТАРАСЕНКО О.С.

ВІКТИМОЛОГІЧНІ ЗАХОДИ ЗАПОБІГАННЯ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ, ПОВ'ЯЗАНИМ З ОБІГОМ ПРОТИПРАВНОГО КОНТЕНТУ В МЕРЕЖІ ІНТЕРНЕТ

VICTIMOLOGICAL MEASURES TO PREVENT CRIMINAL CIRCULATION OFFENSES ILLEGAL CONTENT ON THE INTERNET

У статті надані пропозиції щодо заходів віктимологічного запобігання для користувачів мережі Інтернет, запровадження яких зменшить ризик стати жертвою кримінального правопорушення, пов'язаного з обігом протиправного контенту в мережі Інтернет, а саме спрямованих на: захист комп'ютера чи аналогічного пристрою; забезпечення захисту особистої інформації в мережі Інтернет; захисту від шахрайства в мережі Інтернет; безпечної поведінки дітей. Розглянуті особливості віктимологічної поведінки, на підставі чого розроблено ряд заходів метою яких є запобігання кримінальним правопорушенням на індивідуальному рівні. Зазначається, що особливістю вчинення кримінальних правопорушень, пов'язаним з обігом протиправного контенту в мережі Інтернет, є те, що їх жертви як правило не знають в обличчя осіб, які вчинили щодо них суспільно-небезпечне діяння; такі діяння часто є «автоматизованим», тобто воно вчиняється за допомогою комп'ютерних технологій і протягом короткого періоду часу, що прискорює швидкість та кількість вчинення; особа, яка його вчиняє може перебувати з жертвою у різних місцях та в будь-який час незалежно від зовнішніх факторів – злочинця та жертву можуть розділяти тисячі кілометрів, навіть країни та континенти, а також різні національні юрисдикції; використання сервісів переадресації, які одночасно зберігають конфіденційність особистих дій на пристрої (наприклад, VPN-сервісів) не дозволяє встановити моделі їх розповсюдження географічно та демографічно, як це робиться для інших кримінальних правопорушень. Зроблено висновок, що значна кількість кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, вчиняється за рахунок неуважної та безпечної поведінки безпосередньо користувачів мережі Інтернет, які дозволяють їм стати жертвою. Також навіть наявності сучасних безпекових систем, якими користуються юридичні особи, не гарантує їх захист від окремих видів кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет. Разом з тим, щоб мінімізувати можливість стати жертвою кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, розроблено рекомендації, які повинні на постійній основі доводитись Департаментом кіберполіції Національної поліції користувачам мережі Інтернет. Акцентовано на необхідності посилення роботи Департаменту кіберполіції Національної поліції в частині протидії та попередження булінгу (цькуванню) в закладах освіти та щодо дітей.

***Ключові слова**: протиправний контент, Інтернет, запобігання, віктимологічне запобігання, дитина.*

The article provides proposals for victim prevention measures for Internet users, the introduction of which will reduce the risk of becoming a victim of criminal offenses related to the circulation of illegal content on the Internet, namely, aimed at: protecting the computer or similar device; ensuring the protection of personal information on the Internet; protection against fraud on the Internet; safe behavior of children. Peculiarities of

© ТАРАСЕНКО О.С. – доктор юридичних наук, доцент, професор кафедри оперативно-розшукової діяльності (Національна академія внутрішніх справ)

victimological behavior are considered, on the basis of which a number of measures have been developed aimed at preventing criminal offenses at the individual level. It is noted that the peculiarity of committing criminal offenses related to the circulation of illegal content on the Internet is that their victims usually do not know the faces of those who committed a socially dangerous act against them; such actions are often "automated", ie they are committed with the help of computer technology and for a short period of time, which accelerates the speed and amount of commission; the perpetrator can be with the victim in different places and at any time, regardless of external factors – the perpetrator and the victim can be separated by thousands of kilometers, even countries and continents, as well as different national jurisdictions; The use of forwarding services, which at the same time maintain the confidentiality of personal actions on the device (for example, VPN services) does not allow to establish models of their distribution geographically and demographically, as is done for other criminal offenses. It is concluded that a significant number of criminal offenses related to the circulation of illegal content on the Internet are committed due to careless and safe behavior directly by Internet users, which allows them to become victims. Also, even the availability of modern security systems used by legal entities does not guarantee their protection against certain types of criminal offenses related to the circulation of illegal content on the Internet. At the same time, in order to minimize the possibility of becoming a victim of criminal offenses related to the circulation of illegal content on the Internet, recommendations have been developed that should be constantly communicated by the Cyber Police Department of the National Police to Internet users. Emphasis is placed on the need to strengthen the work of the Cyber Police Department of the National Police in combating and preventing bullying (harassment) in educational institutions and against children.

Key words: *illegal content, Internet, prevention, victimological prevention, child.*

Зі стрімким розвитком технологій людство наприкінці минулого століття вступило в еру комп'ютерів, і тепер майже кожний у своєму повсякденному житті мусить використовувати обчислювальні машини для полегшення життя. Інформаційні технології активно просуваються світом, і вже сьогодні жоден технологічний процес, фінансова операція або передача даних неможливі без комп'ютерних мереж. Масове включення електронно-обчислювальних машин до всіх сфер діяльності суттєво полегшили життя, водночас воно несе в собі безліч проблем. Перекладаючи частину своїх обов'язків на машину, людина не завжди розуміє ступінь ризику та відповідальності, що виникають у зв'язку з цим.

За даними щорічного звіту Федерального бюро розслідувань США, у 2020 р. надійшло майже 800 тис. скарг з приводу різних кіберінцидентів − це на 69 % більше, ніж у 2019 р. П'ятий рік поспіль ФБР фіксує зростання кількості злочинів і все більші грошові втрати. У 2020 р. жертви повідомили про втрату коштів на суму понад 4,2 млрд доларів. За даними ФБР, особливо активізувалися атаки за допомогою програм-вимагачів. У 2020 р. таких злочинів стало більше на 225 %, а збитки зросли до 29 млн доларів [1].

У загальному розумінні віктимізація як процес включає сукупність явищ, серед яких нарощування віктимності певної частини суспільства, різних соціальних груп населення та великої кількості людей; масове поширення виявів віктимності в основних сферах суспільного життя (побуті, сім'ї, дозвіллі, трудовій діяльності); включення людей з підвищеною віктимністю в систему криміногенних відносин з особами, схильними до вчинення кримінальних правопорушень; участь потенційних жертв у формуванні мотивації злочинної поведінки та створенні ситуацій, що полегшують реалізацію намірів і досягнення злочинного результату; віктимізованість певної частини населення; посткримінальна поведінка жертв кримінальних правопорушень; вплив контингенту жертв злочинів на злочинність і криміналізацію суспільства [2, с. 93].

Віктимізація пов'язана з формуванням індивідуальної та групової віктимності, збільшенням частки віктимізованих осіб у структурі населення, а також з наслідками злочинності, а саме: утворенням контингенту жертв кримінальних правопорушень як зареєстрованих, так і латентних [2; 3].

Проведений аналіз способів вчинення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, засвідчив, що їх жертви, як правило, не знають в обличчя осіб, які вчинили щодо них суспільно-небезпечне діяння; такі діяння часто є «автоматизованими», тобто вони вчиняються за допомогою комп'ютерних технологій і протягом короткого періоду часу, що прискорює швидкість вчинення, і, відповідно, їх кількість; особливістю

вчинення кримінального правопорушення, пов'язаного з обігом протиправного контенту в мережі Інтернет, є те, що особа, яка його вчиняє, не може перебувати з жертвою у будь-якому місці та в будь-який час незалежно від зовнішніх факторів – злочинця та жертву можуть розділяти тисячі кілометрів, навіть країни та континенти; використання сервісів переадресації, які одночасно зберігають конфіденційність особистих дій на пристрої (наприклад, VPN-сервісів), не дозволяє встановити моделі їх розповсюдження географічно та демографічно, як це робиться для інших злочинів [4, с. 435].

Визначаючи особливості жертви кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, необхідно також відмітити, що найчастіше від них страждає молодь, оскільки саме вона активно використовує WI-FI та користується соціальними мережами. При цьому важливо звернути увагу на те, що зазвичай при здійсненні своїх дій молодь нехтує елементарними заходами безпеки, наприклад, дотриманням вимог інформаційної безпеки, встановленням різноманітних паролів, до того ж відмінних один від одного, ненаданням своїх паролів, номерів карток невідомим або сумнівним особам, або ж встановлення антивірусного програмного забезпечення. Практика показує, що з кожним днем масштаб кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, невпинно зростає, при цьому потерпілі особи рідко повідомляють про неправомірні дії щодо себе [5, с. 161].

Що стосується юридичних осіб, то вони також значною мірою стають жертвами кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, але вже більш професійних злочинців і навіть організованих угруповань, які спеціалізуються саме на таких протиправних діяннях, а в окремих випадках навіть за підтримки спеціальних служб. Наприклад, хакерська група Electrum причетна до атаки на енергосистему компанії «Укренерго» в грудні 2016 р., йдеться у звіті фахівців з інформаційної безпеки Dragos. За даними дослідників, ця група безпосередньо пов'язана з хакерською групою SandwormTeam, яку неодноразово звинувачували в роботі на російські спецслужби [6].

Дослідження засвідчують, що кожен з нас може стати жертвою кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, через власну віктимність. Б. М. Головкін зазначає, за різних обставин жертвами кримінальних правопорушень можуть стати будь-які особи, незалежно від статі, віку, національності, соціального становища, рівня доходів, місця проживання. Між тим практика показує неоднаковий рівень уразливості людей перед злочинними посяганнями. Це пов'язано не тільки з соціально-демографічними відмінностями населення, але й з несприятливими середовищними умовами проживання та небезпечною поведінкою за конкретних обставин [7].

У зв'язку з неповнотою вітчизняних статистичних даних для встановлення повної віктимологічної характеристики жертв кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, необхідно звернутися до зарубіжних досліджень. Так, за даними Національного бюро боротьби з шахрайством у Великобританії, сформовано такі основні характеристики жертви кіберзлочину:

– на частку фізичних осіб припадає 85 % усіх кіберзлочинів, тоді як на юридичних осіб усього 13 %;

– близько 24 % жертв кіберзлочинності були визначені як потенційно вразливі (тобто такі, що стають або можуть стати жертвами повторно);

– жертвами схильні бути особи віком від 15 до 49 років;

– чоловіки схильні втрачати від кіберзлочинності в 3 рази більше, ніж жінки;

– збиток від крадіжки інтелектуальної власності та конфіденційної ділової інформації є найбільш важливою категорією збитку;

– жінки у 6 разів частіше стають жертвами шахрайства від Інтернет-магазинів, ніж чоловіки [8].

Виходячи з цього, погойдуємося з Д. О. Шагірмановим, який підкреслює, що жертвою кіберзлочину може стати будь-яка особа, проте на індивідуальному рівні можна виокремити такі типи жертв кіберзлочинів:

– випадкова жертва – коли особа стає такою внаслідок збігу обставин;

– жертва з незначним ступенем ризику – віктимність виникла під впливом конкретної несприятливої ситуації;

– жертва з підвищеним ступенем ризику;

– жертва з високим ступенем ризику – особа, морально-соціальна деформація якої не відрізняється від правопорушників [9, с. 242].

Таким чином, суб'єктами віктимізації внаслідок кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, є користувачі комп'ютерів, які здійснюють вихід у мережу Інтернет, у зв'язку з чим внаслідок небезпечної поведінки, події й ситуації вони можуть стати жертвами злочинів. Факторами віктимізації визнається сукупність негативних явищ і подій у суспільстві та житті людей, що детермінують підвищену уразливість певної частини населення, зумовлюють злочинні форми поведінки, полегшують і сприяють заподіянню шкоди різним соціальним суб'єктам, обраним у ролі жертви злочинних посягань. Умовами віктимізації є небезпечна поведінка, події й ситуації, що забезпечують реалізацію злочинних посягань, підвищена віктимність осіб, які користуються мережею Інтернет без дотриманням відповідних заходів безпечного поводження [10, с. 211].

Завдяки захисту комп'ютера можна уникнути впливу зловмисного програмного забезпечення та прямих спроб злому з метою викрадення особистої інформації з домашнього комп'ютера фізичної особи. Тому віктимологічні заходи повинні бути запроваджені в декількох напрямах з метою зменшення ризику під час роботи в Інтернеті на домашньому комп'ютері, та повинні бути спрямовані на:

а) захист комп'ютера (використання брандмауера Windows, вбудований та автоматично ввімкнутий брандмауер; оновлення програмного забезпечення обов'язково повинно здійснюватися в автоматичному режимі, що дасть змогу програмному забезпеченню комп'ютера своєчасно реагувати на виявлені ризики. З цією метою повинно бути увімкнуто оновлення в Windows Update, щоб постійно оновлювати Windows, Microsoft Office та інші програми Microsoft. Також потрібно увімкнути автоматичне оновлення для програмного забезпечення сторонніх розробників, особливо браузерів, Adobe Acrobat Reader та інших програм, що регулярно використовуються; під час роботи на комп'ютері має бути обов'язково встановлене антивірусне програмне забезпечення, при цьому його ліцензійна та актуальна версія, яка повинна бути поставлена на автоматичне оновлення та ін.) [11];

б) забезпечення захисту особистої інформації в мережі Інтернет залежить від можливості контролювати як обсяг особистої інформації, яку ви надаєте, так і осіб, які мають доступ до такої інформації. З метою зменшення ризиків використання особистої інформації у протиправних цілях необхідно: переглянути настройки і параметри вебсайту задля визначення користувачів, які зможуть бачити інтернет-профіль чи фотографії, переглядати публікації і залишати коментарі, а також способів, за допомогою яких люди зможуть віднайти, з подальшим блокуванням небажаного доступу з боку інших користувачів; переглянути параметри конфіденційності для улюблених соціальних мереж, щоб переконатися у відображенні саме того об'єму інформації, яким бажає особа ділитися [11];

в) захист від шахрайства в мережі Інтернет. З цією метою необхідно: запобігати встановленню зловмисного програмного забезпечення і здійснити його видалення в разі виявлення на комп'ютері чи носіях інформації; активізувати в домашньому комп'ютері Центр безпеки Захисник Windows у Windows 8 або попередніх версіях Windows 10, що дасть змогу в реальному часі виявляти зловмисні програми, попереджати та виправляти їх з хмарним захистом; не відкривати підозрілі електронні листи, які стверджують, що особа повинна негайно клацнути, зателефонувати або відкрити вкладення, а також відправлення, які надходять вперше від незнайомих відправників, а також загальні привітання, у яких електронний лист починається із загального повідомлення «Шановний пане або мадам»; підозрілі посилання або неочікувані вкладення. Якщо ви підозрюєте, що повідомлення електронної пошти шахрайське, не відкривайте жодних посилань або вкладень, які ви бачите. Натомість наведіть вказівник миші на посилання, але не клацайте його, щоб побачити, чи збігається адреса введеного в повідомленні посилання. У наведеному нижче прикладі після наведення вказівника миші на посилання відображається справжня вебадреса в полі з жовтим фоном. Користувачеві необхідно звертати увагу на те, що рядок з IP-адресою зовсім не схожий на вебадресу компанії; якщо у листі особу просять розкрити конфіденційні дані, необхідно переконатися, що URL-адреса вебсторінки починається з «HTTPS», а не просто з «HTTP». Буква «S» означає «secure» (безпечно), тобто підключення за такою адресою є захищеним. Разом з тим це не дає гарантії, що вебсайт є законним, проте більшість законних вебсайтів використовують саме протокол HTTPS в силу його більшої безпеки. При цьому навіть законні вебсайти, які використовують протокол HTTP, уразливі перед атаками хакерів та ін. [12].

Важливе значення для запобігання вчинення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, щодо дітей є дотримання ними та їхніми батьками відповідних правил безпечного поводження в мережі Інтернет. Вказане обумовлене

багатьма причинами. Так, за даними міжнародного дослідницького проєкту ESPAD, у 2019 р. лише 6,7 % опитаних підлітків в Україні не користувалися соціальними мережам. Майже 45 % підлітків проводять у соціальних мережах до 3 годин на день, а ще приблизно 50 % – 4 та більше годин [13]. Також проведені дослідження засвідчують, що 24 % дітей віком 7−11 років зустрічались з друзями, з якими познайомились через Інтернет. Інші 24 % дуже б хотіли це зробити. Більшість дітей ішла на зустріч з друзями, але 25 % були одні (незважаючи на такий малий вік). У 58 % випадків зустріч з «другом» була неприємним сюрпризом, тому що діти зрозуміли, що їх віртуальний друг брехав про себе. Підлітки були здивовані при зустрічі з тими, з ким мали зв'язки по Інтернету в 48 % і шоковані в 28 % [14].

Працівники Департаменту кіберполіції (ДКП) Національної поліції повинні розміщати як на своїй вебсторінці правила безпеки в мережі Інтернет для дітей, так і доводити їх до відома з використанням інших ресурсів, наприклад, ці правила повинні розповідатись учням навчальних закладів під час освітньої діяльності. Так, буклет для дітей має доносити наступні правила їхньої поведінки в мережі Інтернет: нікому без дозволу батьків не повідомляти особисту інформацію: домашню адресу, номер свого мобільного або домашнього телефону, робочу адресу батьків, їхній номер телефону, назву й адресу та місцезнаходження своєї школи; не допускати розміщення на обліковому записі чи своїй сторінці фотокартки, на яких дитина оголена або у нижній білизні чи піжамі; не посилати свої фотографії чи іншу інформацію незнайомим особам без дозволу батьків; не відправляти незнайомим особам свої фото електронною або звичайною поштою; якщо знайдете якусь інформацію, що турбує, дитина має негайно сповістити про це батьків; ніколи не погоджуватися на зустріч з людиною, з якою знайомишся в мережі Інтернет; нікому, навіть друзям, не повідомляти пароль до своєї Інтернет-сторінки; якщо дитина все ж таки спілкується з незнайомцем, вона не повинна ніколи повідомляти про те, що вона знаходиться одна дома, або що сама перебуває перед комп'ютером; не обговорювати з незнайомцями теми, які неприємні дитині, або яких вона соромиться; не показувати навіть друзям перед веб-камерою своє тіло або якісь його частини, не робити те, що не подобається; не відповідати на питання, які стосуються особистого життя дитини або її тіла; не розповідати багато про своїх друзів, знайомих та родину, особливо, видавати їхні таємниці; не відповідати на невиховані й грубі листи; розробити з батьками правила користування Інтернетом; не заходити на аморальні сайти і не порушувати без згоди батьків ці правила; не давати нікому крім батьків свої паролі, навіть найближчим друзям; не робити протизаконних вчинків і речей в Інтернеті; не шкодити і не заважати іншим користувачам; не відправляти поштою та не передавати через когось свої особисті речі співрозмовнику по Інтернету [15].

Крім вказаних рекомендацій, доцільно запроваджувати у практичну діяльність підрозділів ДКП Національної поліції й інші інформаційні матеріали з метою формування безпечної поведінки дітей в мережі Інтернет, зокрема, які розміщені на офіційному сайті Міністерства освіти і науки України [13].

Останніми роками звичні нам речі, зокрема зустрічі, спілкування, переходять в онлайн. Пов'язані з пандемією обмеження зробили ще більш затребуваним Інтернет та інші можливості цифрового простору. Це змушує прискорити вироблення рішень із забезпечення прав людини, зокрема прав дитини, в цифровому середовищі. Булінг, що в цифровому середовищі набув часточки кібер-, є одним з ризиків для прав дитини. Охоплення інцидентами суттєво більшої від традиційного булінгу аудиторії та часто анонімність тих, хто вчиняє цькування, справляє значний негативний вплив на благополуччя дітей [15].

Представниця ЮНІСЕФ в Україні Лотта Сильвандер зазначає, що в Україні близько 50 % підлітків були жертвами кібербулінгу. «Кожна третя дитина прогулювала школу через кібербулінг. 75 % підлітків у анонімному опитуванні підтвердили те, що Instagram, TikTok та Snapchat є основними соціальними платформами для цькування» [16].

Тому вироблення віктимологічних заходів попередження та протидії онлайн-цькуванню є важливим компонентом ДКП Національної поліції. З цією метою необхідно впроваджувати серед дітей відповідні рекомендації з попередження та протидії в дитячому середовищі кібербулінгу [13], зокрема на платформі Prometheus можна пройти безкоштовний онлайн-курс «Протидія та попередження булінгу (цькуванню) в закладах освіти», що був створений за ініціативи Міністерства освіти і науки України.

Підводячи підсумки зазначимо, що значна кількість кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, вчиняється за рахунок неуважної та безпечної поведінки безпосередньо користувачів мережі Інтернет, які дозволяють їм стати

жертвою. Також навіть наявності сучасних безпекових систем, якими користуються юридичні особи, не гарантує їх захист від окремих видів кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет. Разом з тим, щоб мінімізувати можливість стати жертвою кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, розроблено рекомендації, які повинні на постійній основі доводитись ДКП Національної поліції користувачам мережі Інтернет. Акцентовано на необхідності посилення роботи ДКП Національної поліції в частині протидії та попередження булінгу (цькуванню) в закладах освіти та щодо дітей.

Список використаних джерел:

1. ФБР: більше $4 млрд збитків від кіберзлочинів в 2020. URL: https://spilno.org/news/fbr-bilshe-4-mlrd-zbytkiv-vid-kiberzlochyniv-v-2020.

2. Головкін Б. М. Кримінологічне поняття віктимізації. *Науковий вісник Міжнародного гуманітарного університету*. *Серія: Юриспруденція*. Одеса, 2015. Вип. 15, т. 2. С. 93–94.

3. Головкін Б. М. Віктимізація населення в Україні: стан, детермінанти, запобігання. *Теорія і практика правознавства*. 2014. Вип. 2. URL: http://nbuv.gov.ua/UJRN/tipp_2014_2_33

4. Юртаєва К. В. Визначення місця вчинення злочинів з використанням комп'ютерних технологій. *Форум права*. 2009. № 2. С. 435.

5. Горбенко А. В. Як стають жертвою кіберзлочинів. *Злочинці і жертви злочинів: матеріали* XX Всеукр. наук. конф. з кримінології для студентів, аспірантів та молодих вчених (м. Харків, 16 листоп. 2020 р.). Харків, 2020. С. 161.

6. Атака на енергомережі в Києві 2016 року: експерти знайшли зв'язок хакерів з РФ. URL: https://www.ukrinform.ua/rubric-technology/2246440-ataka-na-energomerezi-v-kievi-2016-roku-eksperti-znajsli-zvazok-hakeriv-z-rf.html.

7. Головкін Б. М. Як стають жертвами злочинів. *Проблеми законності*. Вип. 136. 2017. С. 162. URL: http://nbuv.gov.ua/ UJRN/Pz_2017_136_19.

8. Cyber Crime – Victimology Analysis : February 2016 / National Fraud Intelligence Burea. *City of London Police – National Policing Lead For Fraud.* 2010. P. 3. URL: https://www.cityoflondon.police.uk/news-and-appeals/Documents/Victimology%20Analysis-latest.pdf

9. Шагірманов Д. О. Деякі питання віктимологічного запобігання кіберзлочинності. *Теорія і практика віктимології*: матеріали Всеукр. конф. для студ., аспірантів, ад'юнктів, здобувачів, присвяченої 50-річчю з дня заснування кафедри кримінології та кримінально-виконавчого права (м. Харків, 12 листоп. 2015 р.) / за ред. А. П. Гетьмана, Б. М. Головкіна. Х.: НЮУ ім. Я. Мудрого, 2015. С. 242.

10. Тарасенко О. С. Теорія та практика протидії кримінальним правопорушенням, пов'язаних з обігом протиправного контенту в мережі Інтернет: *монографія*. Одеса : Видавничий дім «Гельветика», 2021. 432 с.

11. Захист комп'ютера вдома. URL: https://support.microsoft.com/uk-ua/windows/; Захист конфіденційності в Інтернеті. URL: https://support.microsoft.com/uk-ua/windows/.

12. Анатомія кіберзлочину: ключові тренди 2020 року. *Експертний центр прав людини* (30 квіт. 2020 р.). URL: https://ecpl.com.ua/news/anatomiia-kiber-zlochynu/.

13. Безпека дітей в інтернеті. *Офіц. сайт Міністерства освіти і науки України*. URL: https://mon.gov.ua/ua/osvita/pozashkilna-osvita/vihovna-robota-ta-zahist-prav-ditini/bezpeka-ditej-v-interneti.

14. 10 золотих правил безпеки в Інтернеті для дітей. URL: http://school118.edu.kh.ua/vihovna_robota/propaganda_zdorovogo_sposobu_zhittya/10_zolotih_pravil_bezpeki_v_interneti/.

15. Попередження та протидія кібергбулінгу в дитячому середовищі України. URL: https://cyber.bullyingstop.org.ua/storage/media-archives/cyberbuling_виправл15-10_compressed.pdf.

16. Презентовано чат-бот «Кіберпес» для допомоги у боротьбі з кібербулінгом. URL: https://www.kmu.gov.ua/news/prezentovano-chat-bot-kiberpes-dlya-dopomogi-u-borotbi-z-kiberbulingom.