Одеський державний університет внутрішніх справ
Кафедра кібербезпеки та інформаційного забезпечення
Факультет підготовки фахівців для підрозділів кримінальної поліції

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

International scientific-practical conference
"Cybersecurity in Ukraine: Legal and Organization Issues"

Матеріали
Міжнародної науково-практичної конференції
19 листопада 2021 року

Одеса 2021

Рекомендовано до друку рішенням кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ
(протокол № від грудня 2021 року)

Всі матеріали надані в авторській редакції та виражають
персональну позицію учасника конференції

Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук.
К38 практ. конф., м. Одеса, 26 листопада 2020 р. Одеса : ОДУВС, 2021. _____ с.
ISBN 678-717-7020

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжнародну науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 19 листопада 2021 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов'язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем, технологій та інформаційно-аналітична діяльність правоохоронних підрозділів у боротьбі з злочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали всеукраїнської науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад'юнктам), слухачам магістратури, студентам та курсантам вищих навчальних закладів.

«ВИХОВАТЕЛЬ БЕЗПЕКИ» – ДІЄВИЙ МЕХАНІЗМ ПРОТИДІЇ КІБЕРБУЛІНГУ

Сіфоров О.І.
доцент кафедри кібербезпеки та інформаційного забезпечення ОДУВС, к.тех.н, доцент,
Гонтаренко Н.В.
студентка 2-го курсу ОПП «Кримінальний аналіз» освітній ступінь магістр ОДУВС

На сьогоднішній день велика увага суспільства приділяється поведінці підлітків у мережі Інтернет. Це обумовлено тим фактом, що найактивнішими користувачами є саме діти шкільного віку. З кожним роком кількість користувачів збільшується. Інтернет у сьогоденні став невід'ємною частиною життя сучасних дітей, їхнім найближчим оточенням та джерелом знань. Особливо в останні роки у зв'язку з розповсюдженням у всьому світі коронавірусної інфекції виникла необхідність переходу очного навчання дітей на дистанційне, що обумовлює більше проведення часу в мережі Інтернет, користування різними ресурсами, програмними продуктами, подовжує та урізноманітнює спілкування в соцмережах, ігрових платформах. Враховуючи це, до дітей може бути застосована новітня форма агресії, на яку дуже легко потрапити у мережі Інтернет. Це явище не залежить від місця знаходження агресора чи жертви та може мати різні прояви і носить назву кібербулінг.

Розглянувши його види та проаналізувавши ступінь обізнаності підлітків про існування імовірних загроз в мережі Інтернет, чи ставали вони самі вже жертвами, можна запропонувати програмно-аналітичний комплекс заходів, який допоміг би запобігти нанесенню шкоди емоційному та фізичному здоров'ю, створити належні умови для звернення дітей по допомогу і як результат знизити статистичні показники кібербулінгу у підлітковому середовищі.

Вивчаючи поняття кібербулінгу можна визначити, що науковці мають різні підходи до його трактування, тож розглянемо варіанти тлумачення даного поняття:

П.Сміт трактує кібербулінг як агресивні, навмисні дії, що здійснюються групою або окремою особою з використанням електронних форм комунікаціїї, повторно чи з плином часу проти жертви, яка не може захистити себе.

С.Монкс вважає, що кібербулінг – це насильницьки, принизливі або загрозливі дії однієї дитини на адресу іншої за допомогою електронних засобів зв язку, таких як стільниковий телефон, веб-сайти, соціальні мережі, інтернет-групи.

М. Фадєєва вбачає, що кібербулінг – це агресивна поведінка певної особи, найчастіше підлітка, яка здійснюється проти конкретної дитини (жертви) засобами електронної комунікації.

Узагальнюючи підходи науковців можна дійти висновку, що кібербулінг – це умисні дії, що скоюються однією особою або групою осіб відносно іншої особи, посередництвом електронних засобів комунікації, з метою надання шкоди, що можуть здійснюватися напряму або анонімізовано і можуть призвести до низки негативних наслідків в результаті створення ситуації напруження, тиску, залякування, переслідування [1].

Науковці виокремлюють вісім основних типів поведінки, притаманних для кібербулінгу:

1) Перепалки (флеймінг), які полягають в обміні стислими гнівними й запальними репліками між двома чи більше учасниками шляхом використання комунікаційних технологій. Здебільшого вони розгортаються в чатах, форумах, дискусійних групах.

2) Напади, постійні виснажливі атаки – переважно це використання багаторазових повторюваних образливих повідомлень, спрямованих на жертву.

3) Обмовлення, зведення наклепів – розповсюдження принизливої неправдивої інформації з використанням комп'ютерних технологій. Це можуть бути відео, фото або текстові повідомлення в образливій формі по відношенню до жертви.

4) Самозванство, перевтілення в певну особу – переслідувач використовуючи пароль доступу жертви до будь якого її акаунту в соціальних мережах, блогу, пошти тощо, а потім здійснює негативну комунікацію компрометуючи жертву.

5) Шахрайство – неправомірне одержання конфіденційної персональної інформації та її подальше розповсюдження (текст, фото, відео, аудіо) у відкритий Інтернет.

6) Ізоляція – онлайн відчуження, яке можливе в будь-яких типах середовищ, де використовують захист паролями, формують списки небажаних членів групи.

7) Кіберпереслідування – це приховане вистежування через Інтернет необережних користувачів, злочинець отримує інформацію про час, місце та всі необхідні умови здійснення майбутнього нападу.

8) Хепіслепінг – порівняно новий вид кібербулінгу, який започатковано в англійському метро, де підлітки, прогулюючись пероном, раптово ляскали один одного, а інший учасник знімав це на мобільну камеру [2].

Щодо сприйняття дітьми кібербулінгу в Україні та різних його проявів, джерелами виступають різні опитування. Можна навести результати одного з них, а саме проведене Лабораторією психології масової комунікації та медіаосвіти Інституту соціальної та політичної психології НАПН України в травні-червні 2018 року серед старшокласників (1439 учнів з 18 областей України). Дослідження показало, що в рейтингу форм кібербулінгу першу позицію має розповсюдження неправдивої інформації, з чим стикався майже кожен п'ятий підліток (21,4%). З викраданням персональних даних і використання іншими акаунтів від імені опитаних (самозванство) зіштовхувалось 19,8%. Залякувань та погроз завдати шкоди зазнавали 15,6% підлітків, а знущань, образ, приниження та психологічного терору – 14% опитаних [3].

Отже проблема онлайн-цькувань потребує прийняття певних рішень, які б сприяли запобіганню такого виду злочинності у кіберпросторі. Напевно, кращим варіантом було б ситуацію попереджати, ніж з нею боротися, а за для цього підхід до запобігання має бути комплексним.

З одного боку, це міри, які приймаються самими власниками соціальних мереж. Наприклад, Instagram та Facebook у своїй боротьбі з кібербулінгом використовуют технології, за яких люди можуть увімкнути налаштування, що використовує технологію штучного інтелекту, щоб автоматично фільтрувати та приховувати коментарі, які засмучують або цькують користувачів. Функція «Обмежити» – це інструмент, що надає можливість цільового захисту свого акаунту, але при цьому у користувача залишається можливість слідкувати за кривдником. Кожна соціальна платформа пропонує різні інструменти, які дозволяють обмежити тих, хто може коментувати або переглядати публікації чи хто може автоматично ставати другом, а також повідомляти про випадки булінгу. Багато з них передбачають прості кроки для того, щоб заблокувати користувача, припинити отримувати сповіщень від нього/неї або поскаржитися на кібербулінг. Тому вважається доцільним навчити користуватися цими інструментами [4].

З іншого боку виявляється, що існує слабка обізнаність підлітків у небезпеках, які існують на сьогодення в мережі Інтернет, а отже і відсутність знань стосовно того, як допомогти собі, як захиститися від кривдників в кіберпросторі, куди звертатися по допомогу. За для вирішення цього питання потребується створення певних комплексних програм допомоги та просвітництва на базі самих шкіл, призначення відповідальних, незалежних осіб, шкільних «гарячих ліній» та консультативних чатів.

Два міністерства, а саме: МОН та МВС України опрацьовують проект «Вихователь безпеки». Це будуть не поліцейські, а вихователі, які пройдуть відповідний відбір і навчання на базі навчальних закладів системи МВС. Вони будуть розуміти специфіку роботи з дітьми орієнтуватися в тих проблемах, які сьогодні є, в тому числі в законодавчій площині, а також орієнтуватися на міжнародні практики протидії кібербулінгу. Питання побудови для них програмно-аналітичних комплексів, які дозволять вчасно обрати та запустити дієвий механізм протидії кібербулінгу по кожному окремому випадку на сьогодні є дуже актуальним та затребуваним.

Література:

1. Міхєєва О.Ю. Кібербулінг як соціально-педагогічна проблема. http://molodyvcheny.in.ua/files/journal/2018/11/60.pdf
2. Землянко М.С., Наливайко Л.Р. Поняття та особливості кібербулінгу https://er.dduvs.in.ua/bitstream/123456789/5772/1/44.pdf

3. Попередження та протидія Кібербулінгу в дитячому середовищі України 2020. Аналітичний огляд. Команда правозахисного департаменту ГО «Докудейз». с.15. https://cyber.bullyingstop.org.ua/storage/media-archives/cyberbuling_preview_5-10.pdf?fbclid=IwAR2LzoPNfsaZrpI5fBJJwA5V9js-B-kT46VzY6mFk4LV_Qr9RLiz-CvYC5I
4. https://www.unicef.org/ukraine/cyberbulling