002.6:343.971

ХАХАНОВСЬКИЙ В.Г., *доктор юридичних наук, доцент,*
професор кафедри інформаційних технологій
Національної академії внутрішніх справ

ЗАПОБІГАННЯ ТА ПРОТИДІЯ ТОРГІВЛІ ЛЮДЬМИ В МЕРЕЖІ ІНТЕРНЕТ

Анотація. *Про запобігання та протидію торгівлі людьми в мережі Інтернет.*
Ключові слова*: кіберзлочинність, віртуальна педофілія, безпека дітей, мережа Інтернет.*

Аннотация. *О предупреждении и противодействии торговли людьми в сети Интернет.*
Ключевые слова*: киберпреступность, виртуальная педофилия, безопасность детей, сеть Интернет .*

Summary. *On preventing and couteraction of human trafficking in the Internet.*
Keywords*: cybercrime, virtual pedophilia, child safety, the Internet.*

Постановка проблеми. Сьогодні у світі до глобальної мережі Інтернет має доступ близько трьох мільярдів осіб. Виявляється, що 17 % користувачів Інтернету в Європі мешкають у чотирьох країнах – Білорусії, Росії, Молдові та Україні. Росія за таким показником в Європі знаходиться на другому, а Україна – на дев’ятому місці.

Велика користь від використання Інтернету всім людством, а також дітьми та підлітками сьогодні ні у кого не викликає сумнівів. Можливості спілкування і доступу до інформації, а також до культурних цінностей; доступ до всесвітньої бібліотеки, розвиток дистанційних форм навчання з використанням інформаційно-телекомунікаційних систем і технологій – це далеко не повний перелік тих переваг, що надає глобальна мережа Інтернет.

Разом з тим, існують й негативні властивості Інтернету, а саме: поширення вірусів, екстремістської інформації, порнографічної продукції,шахрайство тощо. З метою боротьби з такими негативними явищами у правоохоронних органах країн світу створені відповідні підрозділи, утворюються національні та загальноєвропейська платформи сигналізації кіберзлочинів, організуються різні мережі зв’язку у режимі реального часу, розробляються нормативно-правові акти щодо міжнародного співробітництва правоохоронців, їх співпраці з провайдерами; обов’язків останніх (щодо надання необхідних даних, фільтрації певних ресурсів, зокрема, обмеження доступу до дитячої порнографії тощо).

Проблемам боротьби з кіберзлочинністю присвятили свої наукові публікації вітчизняні та зарубіжні автори, зокрема: В.М. Бутузов, В.Б. Вєхов, В.Д. Гавловский, В.О. Голубєв, В.Є. Козлов, А.Б. Кочарян, Е.В. Рижков, Б.В. Романюк, В.С. Цимбалюк, І.Р. Шинкаренко, В.П. Шеломенцев, Н.Г. Шурухнов та ін. (див., зокрема, [1 – 6]). Разом з тим, здебільшого вказаними та іншими авторами проблеми боротьби з кіберзлочинністю розглядалися фрагментарно або стосувалися певного аспекту проблеми.

Метою статті є розгляд однієї з найважливіших проблем сучасності – безпеки дітей у глобальній мережі Інтернет.

Виклад основних положень. Сьогодні у світі близько половини всіх дітей проводить в Інтернет від однієї до трьох години на день, а кожна десята дитина – від п’яти до десяти годин на день. Безконтрольність роботи дітей в мережі Інтернет може призвести до отримання ними шкідливої інформації. Адже підлітки мають можливість спілкуватися в чатах з незнайомими людьми, купувати різні товари тощо. Тому діти потребують відповідного захисту від інформації шкідливого та агресивного характеру, яка, на жаль, існує в Інтернеті [7].

Одним із способів забезпечення безпеки дітей в Інтернеті є блокування доступу чи фільтрація негативної інформації оператором зв’язку. Правильним було б, щоб батьки слідкували за тим, чим займаються їх діти в Інтернеті, встановлювали межі і визначали, в якій мірі підростаючому поколінню можна користуватися новим інформаційним середовищем. Так, в межах послуги “Батьківський контроль” дорослі можуть накладати обмеження на використання мережі Інтернет дітьми, самостійно вирішуючи, чи треба вмикати фільтрацію контента [8].

Фахівці стверджують, що мережа Інтернет містить більш ніж 30 млрд. сторінок з порнографічними матеріалами, а провайдери вважають, що ефективно закрити доступ до порносайтів без закриття значної кількості сегментів Інтернету неможливо. У всьому світі та у нашій країні спостерігається збільшення сексуальних злочинів проти дітей саме з використанням Інтернету. Половина таких злочинів вчиняється у соціальних мережах. Педофіли обмінюються дитячою порнографією за допомогою технологій P2P, “торентів”, через електронну пошту; заманюють дітей до віртуальних контактів через сайти знайомств; ведуть з ними розмови за допомогою комунікаційної системи Skype тощо.

Ю.М. Горвиць у проблемі безпеки дітей в мережі Інтернет виділяє програмно-технічний і соціально-культурний аспекти. Перший аспект забезпечується шляхом застосування спеціальних технічних та програмних засобів для огородження дітей від небажаного впливу інформаційного середовища.

Психологи відзначають, що педофілія є найбільш поширеним та найтяжким серед статевих відхилень. Кожен рік у світі вчиняються сотні тисяч дитячих зґвалтувань, багато з них відбувається й віртуально, а у такому випадку знайти винних чи довести факт розбещення достатньо складно [9].

Для порушення кримінальної справи необхідна заява потерпілих. Як правило, із заявою щодо протиправних дій проти дитини до правоохоронних органів звертаються її батьки. Дитину, наприклад, дочку, опитують у присутності матері. Батьки можуть надати журнал розмов, проведених між дитиною та підозрюваним (скажімо, через комунікатор Skype).

Часто педофіли ставлять ультиматум дитині, щоб вона знайшла контакти зі своїми друзями й однокласниками, щоб вони теж підключалися до непристойних дій перед веб-камерою. Надалі педофіл може погрожувати дитині фізичним насильством, побиттям. Дитина може отримати психічний шок, вона дуже налякала і після цього часто розповідає про все своїм батькам. Зокрема, існує сайт “jivotno.com”, який пропонує цікаві ігри для маленьких дітей і призначений для спілкування дітей від 7 до 14 років. На сайті можна розміщати фотографії, публікації на загальний чат, обмінюватися особистими повідомленнями. Цей сайт був зареєстрований на 29-річного І.Л., який видавав себе за хлопчика. Їм було розміщено багато об’яв, звернень до дівчаток від 8 до 13 років з непристойними пропозиціями. Загалом профіль педофіла налічував 510 контактів. Він також створив профіль на іншому популярному сайті знайомств, де представлявся як 13-річний хлопчик. Адміністратор сайту надав всі необхідні дані: адреси електронної пошти, журнал розмов з жертвами, IP-адреси.

На іншому популярному сайті педофіл представлявся 14-річним, який шукає подругу 14-16 років. Адміністратор сайту надав необхідні відомості (про записи поштової скриньки, входу в акаунт, контакти на цьому сайті знайомств).

Всі дані, представлені адміністраторами сайтів, засвідчили, що доступні дві IP-адреси адресного простору двох постачальників Інтернету з м. Пловдива. Одну IP-адресу було надано за договором на ім’я сестри педофіла за адресою, де вона жила разом з його сім’єю. Інша IP-адреса належала комп’ютеру в Інтернет-клубі,

розташованому недалеко від місця мешкання педофіла. За словами адміністратора клуба, 29-річний І.Л. кожного дня відвідував клуб з 19 до 24 години. Адміністратор та відвідувачі клуба бачили, що він спілкується в Інтернет з маленькими дітьми і спонукає їх до непристойних дій перед веб-камерою. Адміністратор клуба кілька разів попереджав, що викличе правоохоронців. Через декілька днів І.Л. було заарештовано за комп’ютером в Інтернет-клубі, де було вилучено два жорстких диски від комп’ютера, які він використовував. Під час обшуку квартири затриманого були також вилучені три комп’ютерні системи, знайдено більш ніж п’ять тисяч порнографічних зображень дітей.

У подальшому були проведені відповідні допити підозрюваного, потерпілих та свідків, призначено медичну, психіатричну, комп’ютерно-технічну, художню судові експертизи [10 – 12].

Існує декілька способів виявлення педофілів у мережі Інтернет. Одним із найбільш поширених є метод, який полягає у тому, що особа видає себе у соціальній мережі за малолітню дитину. Така “ловля на живця” спрацьовує досить часто, але навіть наявність доказів у вигляді відповідних скриншотів і лог-файлів не дозволяє у нашій державі притягати до кримінальної відповідальності педофіла за так званий “грумінг” (залицяння, пристування до дитини в Інтернет з ціллю входження до неї у довіру).

Другий метод, який вважають найефективнішим, полягає у спілкуванні правоохоронця у мережі, вдаючи себе за педофіла. Для цього треба знати лексичні та сленгові особливості, що застосовуються педофілами. Надалі складається власний психологічний портрет в очах оточуючого середовища, вивчаються доступні списки користувачів форуму та виявляються серед них ті, хто вказав у своєму профілі e-mail чи номер ICQ. Потім встановлюються персональні дані користувача.

Знайомство може відбуватися у тематичних чатах або соціальних мережах. Так, на відомому сайті “Mail.ru” існує система чатів, які поділяються на різні тематичні кімнати. В одній з них спілкуються педофіли-одиночки. Чат відкритий, але спілкування педофілів там відбувається непомітно.

Існує декілька сайтів, які ведуть нібито борці з педофілами. Насправді ж вони належать саме останнім. Поруч з кожним учасником відображена адреса електронної пошти, тому встановити таких осіб нескладно.

Сьогодні існує низка спеціалізованих програмних засобів для здійснення контролю доступу до контенту на стороні користувача, зокрема “ParentalControl” та “KidsControl”. Подібні системи засновані на наявності набору фільтрів, налаштованих на негативні матеріали (нецензурна лексика, насилля тощо), що дозволяє вибирати різні параметри фільтрації для власної дитини.

В Одеській національній академії зв’язку ім. О.С. Попова було розроблено метод блокування і автоматичної заборони доступу до сайтів з порнографічними зображеннями і відеофільмами, який заснований на концепції контекстного пошуку зображень за зразком. Метод передбачає створення дворівневої бази зображень – зразків людської шкіри. Попередній аналіз завантажених браузером зображень для виявлення тих, які можуть бути порнографічними, здійснюється шляхом вилучення з цих зображень дескрипторів домінантного кольору і подальшого контекстного пошуку таких зображень у базі. В процесі аналізу відбувається квантування статичних зображень чи опорних кадрів відеопотоку для зменшення кольорової надлишковості. Надалі визначається частина тілесних кольорів та приймається рішення про блокування сайту.

Соціальна безкоштовна послуга “Батьківський контроль” надається програмою “Київстар” “Безпека дітей в Інтернеті”. Така послуга дозволяє відвідувати гарантовано безпечні сайти (нині їх 44), які схвалені Інститутом психології ім. Костюка.

В Росії та Молдові вирішили боротися з педофілами як у багатьох країнах світу – методом примусової хімічної кастрації. Такий закон набрав чинності в Росії у лютому 2012 р. В РФ також вирішується питання щодо посилення покарання для педофілів-рецидивістів, включаючи довічне ув’язнення. В Молдові такий закон набере чинність з 1 червня 2012 р.

У 2011 р. Верховною Радою України розглядався законопроект про примусову хімічну кастрацію педофілів, але не набрав потрібних голосів. Разом з тим, у лютому 2012 р. Верховна Рада підтримала законопроект щодо посилення відповідальності за злочини проти статевої свободи і статевої недоторканності особи. Відповідно до змін, внесених до Кримінального кодексу України, тепер за зґвалтування малолітніх передбачене покарання у виді довічного позбавлення волі.

Висновки.

Отже, глобальна мережа Інтернет, крім низки позитивних якостей, має негативні прояви, одним з яких є торгівля людьми та дитяча порнографія. Такі прояви потребують адекватного реагування з боку держави та суспільства.

Особлива роль у запобіганні та протидії проявам педофілії у віртуальному просторі належить правоохоронним органам. Працівники підрозділів по боротьбі з кіберзлочинністю разом з працівниками підрозділів по боротьбі із злочинністю в сфері торгівлі людьми повинні вміти документувати та розкривати такі злочини. Тому при підготовці фахівців з нової спеціалізації “Протидія кіберзлочинності” у Національній академії внутрішніх справ в рамках спеціалізованих навчальних дисциплін передбачено вивчення нової теми з відпрацюванням певних навичок у віртуальному просторі.

Використана література

1. Бутузов В.М. Документування злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку при проведенні дослідчої перевірки : наук. практ. посіб. / В.М. Бутузов, В.Д. Гавловский, Л.П. Скалозуб та ін. ; за заг. ред. Л.П. Скалозуба, І.В. Бондаренка. – К. : Вид. Дім “Аванпост-Прим”, 2010. – 245 с.

2. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. – М. : Горячая линия. – Телеком, 2002. – 336 с.

3. Хахановський В.Г. Киберзлочинність : застосування сучасних технологій при вчиненні злочинів – проблеми досудового розслідування та міжнародної співпраці / В. Г. Хахановський // Правова інформатика. – № 1 (13). – 2007. – С. 65 – 70.

4. Рыжков Э.В. Кадровое обеспечение борьбы с компьютерной преступностью / Э.В. Рыжков // Международное сотрудничество в борьбе с компьютерной преступностью: проблемы и пути их решения : матер. міжнар. наук.-практ. конф. – Донецьк, 2007. – С. 276 – 279.

5. Хахановський В.Г. Проблема підготовки кадрів з протидії кіберзлочинності / В. Г. Хахановський // Митна справа. – 2011. – № 2 (74). – Ч. 2. – С. 305 – 307.

6. Кочарян А.Б. Виховання культури користувача Інтернет. Безпека у всесвітній мережі : навч.-метод. посіб. / А.Б. Кочарян, Н.І. Гущина. – К. : Інститут інноваційних технологій і змісту освіти, 2011. – 100 с.

7. – Режим доступу : //www. mincom.gov.az

8. – Режим доступу : //www.edu.gov.az

9. – Режим доступу : //www.obozrevatel.com

10. – Режим доступу : //www.ua.partnersinlearningnetwork.com

11. – Режим доступу : //www.onlandia.org.ua/pages/UNESCO_research_whitepaper

12. – Режим доступу : //www.sputnikmedia.net/news/854.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~