УДК 343.54:004
DOI https://doi.org/10.32844/2618-1258.2019.4-2.29

ПОСТОЛ О.І.

ДОМАШНЄ НАСИЛЬСТВО ІЗ ЗАСТОСУВАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ: ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ

Стаття присвячена дослідженню питань виявлення домашнього насильства із застосуванням інформаційних технологій і його запобігання. На основі аналізу наукових праць і законодавства України виявлено проблемні питання у сфері запобігання та протидії домашньому насильству із застосуванням сучасних інформаційних технологій і запропоновано шляхи їх вирішення. У статті наведено статистичні дані щодо домашнього насильства та його наслідків для суспільства.

Зокрема, у статті визначено окремі аспекти застосування кривдниками сучасних інформаційних технологій під час вчинення домашнього насильства з метою контролю постраждалої особи. Розглянуто основні кроки забезпечення безпеки та конфіденційності мобільного пристрою, у т. ч. під час користування соціальними мережами та через додатки для спілкування. Проаналізовано позитивний закордонний досвід боротьби з домашнім насильством за допомогою інформаційних технологій, особливо в рамках забезпечення контролю за виконанням спеціальних заходів щодо протидії домашньому насильству, а саме термінового заборонного припису й обмежувального припису, що насамперед сприяло б забезпеченню захисту постраждалих осіб. Окрему увагу звернено на збирання та фіксування доказів вчинення домашнього насильства.

З огляду на відсутність згадувань у законодавстві щодо запобігання та протидії домашньому насильству, вчинення домашнього насильства із застосуванням інформаційних технологій і механізму виявлення домашнього насильства за допомогою інформаційних технологій, автором запропоновано виокремити вчинення домашнього насильства з використанням інформаційних технологій в окрему форму домашнього насильства «технологічне насильство».

Наголошено на необхідності проведення досліджень ефективності технологій у протидії домашньому насильству, а також вивчення питання забезпечення конфіденційності постраждалої особи.

Також наголошено на важливості підвищення обізнаності населення про те, як сучасні інформаційні технології можуть бути використані кривдником при вчиненні домашнього насильства, як захистити себе від таких дій і як забезпечити безпеку технологій, якими користується постраждала від домашнього насильства особа.

Ключові слова: *домашнє насильство, інформаційні технології, конфіденційність, мережі Інтернет, соціальні мережі, смартфон.*

The article is devoted to the study of the detection and prevention of domestic violence using information technology. On the basis of the analysis of scientific works and the legislation of Ukraine identified the problematic issues that exist in the field of prevention and counteraction to domestic violence with the use of modern information technologies and suggested ways to solve them. The article provides statistics on domestic violence and its consequences for society.

The article identifies certain aspects of the use of modern information technologies by the perpetrators of domestic violence in order to control the victim. The basic steps are taken to ensure the security and privacy of your mobile device, including when using social networks and through communication applications. Positive foreign experience in combating domestic violence through information technologies is analyzed, especially in the framework of control over the implementation of special measures to counter domestic violence, namely the urgent restraining order and restrictive prescription,

© ПОСТОЛ О.І. – ад'юнкт кафедри адміністративного правата адміністративного процесу (Одеський державний університет внутрішніх справ)

which would first of all help to ensure the protection of the victims. Particular attention has been paid to collecting and recording evidence of domestic violence.

Given the lack of mention in legislation on preventing and countering domestic violence, committing domestic violence with the use of information technology and the mechanism for detecting domestic violence through information technology, the author it is proposed to distinguish committing domestic violence with the use of information technology into a separate form of domestic violence, "technological violence".

It is emphasized that there is the need to research the effectiveness of technology in countering domestic violence, as well as the issue of ensuring the privacy of the victim.

It also emphasized the importance of raising public awareness of how current information technology can be used by the abuser to commit domestic violence, how to protect himself from such acts, and how to ensure the security of the technologies used by the victim of domestic violence.

Key words: *domestic violence, information technology, privacy, Internet, social networks, smartphone.*

Вступ. Домашнє насильство є одним із найпоширеніших порушень прав людини у світі, яке має руйнівний вплив на суспільство. Так, в Україні щороку від гендерно-зумовленого насильства, зокрема домашнього насильства, гине близько 600 жінок, внаслідок чого економіка держави втрачає 1,5 млн грн, окрім того 2,4 млн грн становлять економічні витрати внаслідок домашнього насильства. Слід зауважити, що 1,1 млн жінок на рік зазнають фізичного і сексуального насильства, та лише 15,9% із них звертаються за допомогою до правоохоронних органів [1].

Нині в нашій державі проблемі домашнього насильства приділяється значна увага. Прийняття Закону України «Про запобігання та протидію домашньому насильству» сприяло значним трансформаціям у сфері запобігання та протидії домашньому насильству. Основними напрямами реалізації законодавства у сфері запобігання та протидії домашньому насильству є: запобігання, ефективне реагування, надання допомоги та захисту постраждалим від домашнього насильства особам, належне розслідування фактів домашнього насильства та притягнення кривдників до відповідальності [2].

Однак звертає на себе увагу факт відсутності будь-яких згадувань у Законі про вчинення домашнього насильства із застосування сучасних інформаційних технологій і щодо інструментів протидії такому насильству. З погляду на факт розповсюдженості та доступності серед населення смартфонів і технологій відеонагляду загроза переслідування за допомогою сучасних технологій зростає, у зв'язку з чим виникає необхідність визначення такого поняття, як вчинення домашнього насильства із застосуванням інформаційних технологій і шляхів його запобігання і протидії.

Дослідженням проблеми домашнього насильства займалися вчені з різних галузей знань – адміністративного права, кримінального права, психології, соціології та ін.: О.М. Бандурка, А.Б. Блага, О.В. Бойко, Ф.К. Думко, М.В. Євсюкова, Т.В. Журавель, Я.М. Квітка, О.В. Ковальова, О.О. Лазаренко, К.Б. Левченко, О.В. Негодченко, О.М. Ткаленко, Г.О. Христова, Х.П. Ярмакі та ін. Однак практично відсутні наукові праці у цій сфері з боку науковців інформаційного права та кібербезпеки.

Постановка завдання. Мета статті полягає в тому щоб на основі аналізу наукових праць і законодавства України виявити проблемні питання та прогалиниу сфері запобігання та протидії домашньому насильству із застосуванням сучасних інформаційних технологій і запропонувати шляхи їх вирішення.

Результати дослідження. Домашнє насильство становить особливу модель поведінки кривдника, спрямовану на контроль і підтримку влади над членами своєї родини. Така поведінка включає в себе дії фізичного, психологічного, економічного та сексуального характеру для контролювання постраждалої особи. Сучасні технології ж у цьому процесі можуть надати нові можливості для кривдника для залякування і переслідування постраждалої особи.

Є велика кількість шпигунських програм та/або додатків із функцією відстеження, які доступні для завантаження, крім того, є і цілком законні додатки, що можуть бути неправомірно використані кривдником. Наприклад, додатки, призначені для пошуку загубленого телефону, можуть бути використані кривдником для відстеження місця перебування постраждалої особи. Також додатки, призначені для моніторингу використання Інтернету дитиною, містять посилання на те, як використовувати додаток для читання видалених повідомлень на смартфоні.

Важливо, що мережа Інтернет не лише надає кривднику можливість пошуку інформації щодо шляхів відстеження постраждалої особи, а також дозволяє кривднику знаходити інформацію,

за допомогою якої він має можливість знайти постраждалу особу. Наприклад, веб-сайти, блоги, соціальні мережі часто містять фотографії, імена, контакти та іншу інформацію про особу.

Кривдниками можуть бути використані мобільні телефони, смартфони, персональні комп'ютери, ноутбуки, системи фото- та відеофіксації, системи глобального позиціонування (GPS) та багато інших сучасних технологічних пристроїв [3].

До найпоширеніших правопорушень, пов'язаних із технологіями, можна віднести такі, як: переслідування або залякування шляхом відправки повідомлень; використання технології GPS з метою відстеження пересування особи; моніторинг дій і звичок особи через соціальні мережі.

Наприклад, мобільний телефон містить багато інформації про свого власника, тому важливо забезпечити безпеку та конфіденційність, особливо у разі, якщо кривдник використовує технології з метою переслідування або контролю постраждалої особи.

До основних кроків забезпечення безпеки та конфіденційності мобільного пристрою можна віднести:

По-перше, необхідно ввести пароль на мобільний телефон. Це перешкоджає тому, аби кривдник мав доступ до налаштувань небажаних програм або навіть встановлення шпигунського програмного забезпечення.

По-друге, необхідно перевіряти обліковий запис на смартфоні. Для власників Android – обліковий запис Google, для власників iPhone – обліковий запис iCloud. Ці облікові записи часто містять резервну копію телефону та залежно від налаштувань можуть містити конфіденційну інформацію, зокрема фотографії, контакти, нотатки та іншу особисту інформацію.

Важливо зазначити, що ці облікові записи можуть бути доступні і через інші телефони та комп'ютери. Тобто, якщо кривднику відомі ім'я користувача та пароль для облікового запису, він матиме можливість увійти до системи та переглянути інформацію, яка зберігається на телефоні постраждалої особи. Аби запобігти таким діям, необхідно переконатися, що ім'я користувача та пароль облікового запису нікому не відомі, крім того, перевірити наявність підключень інших пристроїв до облікового запису та за їх наявності видалити такі пристрої.

По-третє, важливо знати встановлені додатки на телефоні. Деякі з додатків використовують інформацію з телефону для роботи (наприклад, для додатку GoogleMaps, аби вказати напрямок, необхідно знати місце розташування користувача), інші додатки можуть ділитися інформацією на телефоні більш небезпечними способами. Тому, аби убезпечити витік інформації з телефону, необхідно: видалити додатки, які не використовуються, особливо якщо в них є права на доступ до даних; заборонити доступ до даних додаткам, які цього не потребують (наприклад, додатки з іграми, що не пов'язані з місцем розташування, не потребують інформації щодо місця розташування та не повинні її вимагати; встановити антишпигунські й антивірусні інструменти.

По-четверте, необхідно контролювати підключення до Wi-Fi і Bluetooth. Більшість смартфонів запитують підтвердження щодо підключення вперше до мережі Wi-Fi або пристрою Bluetooth, однак, якщо підключення відбулося один раз, воно автоматично підключатиметься знову, коли пристрій знаходитиметься в межах діапазону. Якщо це не захищена мережа Wi-Fi або пристрій Bluetooth, щодо якого є довіра (наприклад, коли особа має інший пристрій Bluetooth), після завершення підключення необхідно «забути» мережу Wi-Fi або пристрій Bluetooth.

Важливо зауважити, що найпростішим шляхом для кривдника дізнатися про життя постраждалої особи є соціальні мережі, які з роками набувають все більшої популярності. Сайти соціальних мереж, такі як Facebook, Instagram, Twitter дозволяють без ускладнень знаходити та стежити за людиною. Якщо в соціальних мережах використовуються облікові записи, то налаштування конфіденційності та налаштування автоматичного обміну даними можуть наражати постраждалу особу на ризик. Аби попередити доступ кривдника до сторінки соціальної мережі, важливо: використовувати налаштування конфіденційності аби контролювати, хто може бачити особисті дані; налаштувати параметри облікового запису, щоб заблокувати небажаних користувачів, які можуть переглядати сторінку; замінити зображення профілю з власного фото на більш загальне зображення; частіше змінювати пароль облікового запису (наприклад, кожні три місяці); у разі підозри перевірки соціальної мережі можливо створити обліковий запис із використанням анонімного імені й облікового запису електронної пошти.

Не менш важливим для постраждалої особи є конфіденційність спілкування. Найпоширенішими додатками для спілкування є Viber, Telegram, WhatsApp. Аби кривдник не мав можливості читати повідомлення, слід обирати зашифровані повідомлення. У зазначених додатках при використовуванні функції шифрування, навіть при зломі аккаунту читання чатів є неможливим.

Важливо, що у додатку Telegram можливо налаштувати повідомлення на «самознищення», які через певний проміжок часу самостійно видаляються.

Ватро уваги, що у США для постраждалих від домашнього насильства осіб було розроблено спеціальний додаток для iPhone і Android під назвою «AspireNews». У ньому можна знайти інформацію про організації, куди можна звернутися за допомогою. Крім того, цей додаток містить т. зв. «тривожну кнопку», при натисканні на яку в ситуації домашнього насильства відбувається оповіщення місцевих установ, котрі уповноважені запобігати і протидіяти домашньому насильству. Розробники цієї програми також включили до неї можливість аудіо- та відеофіксації конфліктної ситуації, що може використовуватися як докази для підтвердження провини кривдника.

Схожий додаток було розроблено в Індії, Нью-Делі під назвою «ICE» – це абревіатура від англійської «In case of emergency» (в екстрених випадках). Додаток допомагає його власникам встановити місцезнаходження і відправити сигнал SOS на кілька номерів телефонів, які вибирають самі користувачі [3].

Цікавим із погляду забезпечення безпеки для постраждалих осіб є сучасні технології, що застосовуються до кривдника в Австралії у випадках підвищеного ризику для життя постраждалих осіб. Так, кривдників можуть зобов'язати носити електронні GPS браслети. Постраждалі особи мають окремий прилад, який видає попереджувальний сигнал про наближення кривдника. Крім того, для постраждалих осіб розроблено «годинник безпеки 3G», що виглядає і функціонує як звичайний годинник, однак має аварійну кнопку, яка негайно підключається до Колл-центру, котрий надалі повідомляє поліцію.

Влада Штату Вікторія, що в Австралії, активно веде боротьбу з домашнім насильством, вчиненим із використанням інформаційних технологій. Стратегії, реалізовані для досягнення мети захисту постраждалих від домашнього насильства у власних будинках, включають встановлення камер відеонагляду у помешканні постраждалих осіб з метою запобігання порушенню заборонних та обмежувальних приписів кривдниками.

Позитивний закордонний досвід протидії домашньому насильству було б доцільно запровадити і в нашій державі, особливо в рамках забезпечення контролю за виконанням спеціальних заходів щодо протидії домашньому насильству, а саме термінового заборонного припису й обмежувального припису. Це сприяло б забезпеченню захисту постраждалих осіб і насамперед допомагало б працівникам поліції виконувати вимоги ст. 10 ЗУ «Про запобігання та протидію домашньому насильству», а саме у частині здійснення контролю за виконанням кривдниками спеціальних заходів протидії домашнього насильства протягом строку їх дії.

Слід зазначити, що під час розгляду у суді справ про адміністративні правопорушення про вчинення домашнього насильства судді відповідно до ст. 251 КУпАП [4] можуть вимагати доказів наявності адміністративного правопорушення, які, окрім пояснень потерпілої особи та свідків, включають показання технічних приладів і засобів. Це можуть бути фотографії, відеозаписи, текстові повідомлення, електронні листи, повідомлення в соціальних мережах. Ті самі вимоги пред'являються при прийнятті рішення по кримінальному провадженню щодо вчинення домашнього насильства. Відсутність доказової бази доволі часто призводить до повернення суддями матеріалів справ на доопрацювання органами поліції або до їх закриття у зв'язку з відсутністю факту правопорушення [5]. Тому для забезпечення доказової бази у випадках домашнього насильства доцільно за можливості фіксувати та зберегти все, що пов'язано з подією.

Наприклад, електронний лист містить IP-адресу, яка може допомогти визначити особистість відправника. Аби кривдник за умови доступу до облікового запису не мав можливості видалити електронний лист, його варто роздрукувати або зробити знімок екрану з вмістом, враховуючи заголовки. Важливо, що переадресовувати електронний лист не варто, оскільки він втратить ідентифікаційну інформацію, необхідну для доказу.

Якщо доказом вчинення домашнього насильства є текстове повідомлення, варто зробити фотографію такого повідомлення або знімок екрану з фіксуванням контакту відправника, аби довести, що повідомлення кривдника пов'язане з його номером телефону.

Аби зберегти докази переслідування в соціальних мережах, необхідно зробити фотографію або знімок екрану погроз або домагань на комп'ютері або іншому пристрої. Також співробітники поліції в рамках розгляду справи про вчинення домашнього насильства можуть відправити лист на веб-сайт компанії з проханням зберегти інформацію про обліковий запис.

Крім того, за можливості варто записувати телефонні розмови з кривдником з метою отримання доказу погроз або залякування. Однак варто перевірити, чи дозволяє пристрій записати телефонну розмову без повідомлення іншої сторони. Важливо фіксувати дату та час телефонних дзвінків.

З огляду на висвітлене слід зауважити, що, хоча в національному законодавстві є певні норми, які захищають постраждалих осіб від незаконного втручання технологій у їх особисте життя, однак, а ні в Законі України «Про запобігання та протидію домашнього насильства», а ні в інших нормативних актах у сфері запобігання та протидії домашньому насильству не містяться визначення вчинення домашнього насильства з використанням сучасних технологій.

Домашнє насильство, вчинене із застосуванням інформаційних технологій, можна було б віднести до психологічного насильства, яке в Законі визначено як форма домашнього насильства, що включає словесні образи, погрози, у т. ч. щодо третіх осіб, приниження, переслідування, залякування, інші діяння, спрямовані на обмеження волевиявлення особи, контроль у репродуктивній сфері, якщо такі дії або бездіяльність викликали у постраждалої особи побоювання за свою безпеку чи безпеку третіх осіб, спричинили емоційну невпевненість, нездатність захистити себе або завдали шкоди психічному здоров'ю особи.

Однак домашнє насильство, вчинене із застосування інформаційних технологій, може підпадати під економічну форму домашнього насильства, а саме у частині позбавлення або контролю коштів, а також під сексуальну форму домашнього насильства, наприклад, шляхом розповсюдження фотографій сексуального характеру, та навіть під фізичну форму домашнього насильства у частині незаконного позбавлення волі, що стає можливим завдяки новітнім технологіям «розумного будинку».

Тому, на нашу думку, необхідним є виокремлення домашнього насильства, вчиненого з використанням інформаційних технологій, в окрему форму домашнього насильства – «технологічне насильство», що значно полегшило б його ідентифікацію.

Висновки. Підсумовуючи, слід зазначити, що для боротьби з домашнім насильством необхідні подальші наукові дослідження ефективності технологій у сфері запобігання та протидії домашньому насильству. Важливе подальше вивчення питання конфіденційності, яке має першочергове значення для постраждалої особи. Крім того, самі технології потребують більш досконалого дослідження для переконання, що вони не дозволяють витоку конфіденційної інформації широкому колу осіб, наприклад, через Веб-картографію або форуми в Інтернеті. Однак, незважаючи на прогалини щодо конфіденційності та безпеки, технології можуть позитивно впливати на постраждалих від домашнього насильства осіб шляхом доступу до ресурсів та інформації стосовно можливостей отримання послуг і захисту.

Тому важливо підвищувати обізнаність населення про те, як сучасні інформаційні технології можуть бути використані кривдником при вчиненні домашнього насильства, як захистити себе від таких дій і як забезпечити безпеку технологій, якими користується постраждала від домашнього насильства особа.

Список використаних джерел:

1. Дослідження «Економічні наслідки насильства щодо жінок в Україні»: UNFPA Представництво Фонду ООН у галузі народонаселення в Україні.URL: http://ukraine.unfpa.org/sites/default/files/pubpdf/Infographics_UR_1.pdf.

2. Про запобігання та протидію домашньому насильству : Закон України від 07.12.2017 № 2229-19. URL: http://zakon3.rada.gov.ua/laws/ show/2229-19.

3. Постол О.І. Сучасні інформаційні технології як засіб вчинення домашнього насильства. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2018. № 4 (97). С. 163–168.

4. Кодекс України про адміністративні правопорушення : Кодекс від 07.12.1984 № 8073-X. URL: http://zakon3.rada.gov.ua/laws/show/80731-10.

5. Постол Е.И., Ковалева Е.В. Административная ответственность за совершение домашнего насилия. *Международный научно-практический журнал «Legeasi viata»*. 2019. № 5/2. С. 83–87.