фіксується. Якщо наші дані потрапляють в чужі руки, ми фактично не можемо контролювати їх використання.

Сфери застосування блокчейна. Сутність «ланцюга блоків» як загальнодоступною, розподіленої і 100% достовірної бази даних робить застосування блокчейн дуже привабливим для компаній, що працюють в різних областях. В даний час вже існує ряд розширень для розробки бізнес-додатків на блокчейн, що забезпечують: безпечне адміністрування мереж, що виключає хакерські атаки MIM (Man-in-the-Middle, що означає «людина посередині») і знімає проблему централізованого адміністрування; зберігання цифрових сертифікатів, що робить повністю захищеним доступ користувачів до сайтів (зокрема, виключаючи перехоплення паролів); безпечні двосторонні угоди; фіксацію часу розміщення документів, що дозволяє вирішувати питання патентування, авторського права; систему DNS (Domain Name System), невразливу для DDOS-атак (Distributed Denial of Service – attacks), та інше.

Висновок. Наша особиста інформація в даний час зосереджена в Інтернеті і в базах даних компаній, тобто по суті контролюється кількома гравцями. Можна очікувати, що такі темпи зростання обсягів створюваних і зібраних даних і далі будуть послаблювати захист нашої особистої інформації. Рішення із застосуванням технології блокчейн або засновані на принципах цієї технології можуть допомогти знизити загрозу конфіденційності, дозволяючи нам при цьому прискорити вчинення транзакцій, поліпшити сервіс і використовувати найбільш ефективні алгоритми штучного інтелекту.

Список бібліографічних посилань

1. Ray S. How Blockchains Will Enable Privacy // Towards Data Science. Mar 3, 2018. URL: https://towardsdatascience.com/how-blockchains-will-enable-privacy-1522a846bf65 (дата звернення: 28.10.2018).

Одержано 30.10.2018

УДК 159.923

Олена Сергіївна КРУПИЧ,
студентка групи ПБП-16-6 навчально-наукового інституту права Національного університету державної фіскальної служби України;
Ірина Василівна ПИЛИПІВ,
студентка групи ПБП-16-6 навчально-наукового інституту права Національного університету державної фіскальної служби України;
Микола Васильович КОВАЛЬ,
кандидат юридичних наук, професор,
професор кафедри адміністративного права і процесу та митної справи Національного університету державної фіскальної служби України;

КІБЕРБУЛІНГ ЯК ЗАГРОЗА XXI СТОЛІТТЯ: ОСОБЛИВОСТІ ТА ЗАХОДИ БОРОТЬБИ

Сучасне суспільство неможливо уявити без інтернет ресурсів, які несуть чималий вклад до соціалізації суспільства, яка передбачає

трансформацію у всі сфери життя суспільства. Однією з них є комунікація – процес спілкування та взаємодії людей у соціумі. Поряд з позитивними сторонами такої тенденції соціалізації прослідковуються негативні аспекти. Одним з таких є нова форма жорстокості у віртуальному середовищі – вплив через засоби масової інформації на людину, суспільство, державу, яка отримала назву кібербулінг [1, с. 1]. Тому наразі постала нагальна проблема вирішити та стабілізувати вплив медіа на психіку людини.

Вивченням даної віртуальної проблеми з наукової точки зору займалися як вітизняні, так і зарубіжні вчені: Н. Алексєєва, Г. Олпорт, М. Грінченко, К. Девіс, А. Третьякова, Л. Тьорстоун, Б. Лускін, А. Мелях, Г. Солдатова, Д. Смірнов, А. Шелонг та інші.

Кібербулінг або інтернет-мобінг – це сучасна форма агресії, яка набула поширення з появою мобільних телефонів, інтернету. Будь-які її форми мають на меті дошкулити, нашкодити чи принизити людину дистанційно, без фізичного насильства. «Зброєю» булера стають соціальні мережі, форуми, чати, мобільні телефони тощо [1, с. 2].

Така форма цькування набирає все більших обертів. Часто люди, і зокрема діти не знають, як можна захиститися від кібербулінгу. Більш того, батьки самі часто не розуміють, як себе поводити і яким чином захистити дитину.

Причин кібербулінгу як інтренет-агресії чимало, вона може бути вмотивованою чи непередбачуваною. У реальності чи в інтернеті практично однаково розкриваються стосунки «агресор-жертва». Механізм їх взаємодії фактично ідентичний. Так само часто ворожнеча з реального світу переходить у віртуальний. В інтернеті дуже просто бути анонімним, що підвищує шанси стати жертвою знущання, бо анонімність передбачає безкарність. Залякування може відбуватися з будь-якої точки планети.

Аналіз наукової літератури дозволив виділити нам наступні способи поведінки, які характерні для кібербулінгу, відображають переважну більшість різновидів негативного впливу в інтернет-просторі:

– суперечки, або флеймінг – обмін короткими гнівними і запальними репліками між двома чи більше учасниками, використовуючи комунікаційні технології. Частіш за все розгортається в «публічних» місцях Інтернету, на чатах, форумах, дискусійних групах, інколи перетворюється в затяжну війну. На перший погляд, флеймінг – це боротьба між рівними, але в певних умовах вона теж може перетворитися на нерівноправний психологічний терор [2, с. 93];

– напади, постійні виснажливі атаки – найчастіше це залучення повторюваних образливих повідомлень, спрямованих на жертву (наприклад, сотні смс-повідомлень на мобільний телефон, постійні дзвінки) з перевантаженням персональних каналів комунікації. У чатах чи на форумах (місця розмов у інтернеті) напади теж трапляються, в онлайн-іграх напади найчастіше використовують гріфери – група

гравців, які за мету ставлять не перемогу в певній грі, а руйнацію ігрового досвіду інших учасників.

– обмовлення, зведення наклепів – розповсюдження принизливої неправдивої інформації з використанням комп'ютерних технологій. Жертвами можуть ставати не тільки окремі підлітки, трапляється розсилка списків (наприклад, «хто є хто», або «хто з ким спить» в класі, школі), створюються спеціальні «книги для критики», в яких розміщуються жарти про однокласників, де також можуть розміщуватись наклепи, перетворюючи гумор на техніку «списку групи ненависті», з якого вибираються мішені для тренування власної злоби, зливання роздратування, переносу агресії тощо [3];

– самозванство, втілення в певну особу – переслідувач позиціонує себе як жертву, використовуючи її пароль доступу до її акаунту в соціальних мережах, блогу, пошти, системи миттєвих повідомлень тощо, а потім здійснює негативну комунікацію. Організація «хвилі зворотних зв'язків» відбувається, коли з адреси жертви без її відому відправляються ганебні провокаційні листи її друзям і близьким за адресною книгою, а потім розгублена жертва не очікувано отримує гнівні відповіді. Особливо небезпечним є використання імперсоналізації проти людей, включених до «списку груп ненависті», адже наражає на реальну небезпеку їхнє життя;

– ошуканство, видурювання конфіденційної інформації та її розповсюдження – отримання персональної інформації в міжособовій комунікації і передача її (текстів, фото, відео) в публічну зону Інтернету або поштою тим, кому вона була призначена [4, с. 132];

– кіберпереслідування – це дії з прихованого вистежування переслідуваних і тих, хто пересувається без діла поруч, зазвичай зроблені непомітно, анонімно, з метою організації злочинних дій на кшталт спроб згвалтування, фізичного насильства, побиття. Відстежуючи через Інтернет необережних користувачів, злочинець отримує інформацію про час, місце і всі необхідні умови здійснення майбутнього нападу

– хепіслепінг – відносно новий вид кібербулінгу, який починався в англійському метро, де підлітки прогулюючись пероном раптом ляскали один одного, в той час як інший учасник знімав цю дію на мобільну камеру. В подальшому за будь-якими відеороликами, в яких записано реальні напади, закріпилась назва хепіслепінг [5, с. 255].

Вбачаючи на зазначені способи потрібно наголосити, що кібертероризм в молодіжному середовищі має свої особливості:

– молодь починає спілкуватися між собою частіше і приховано від дорослих, а спілкування у всесвітній мережі Інтернет, позбавляє дорослих здійснювати контроль;

– швидке і багатоадресне розповсюдження інформації;

– частіше кіберпреслідувачі знають, кого вони переслідують, а їх жертви не завжди знають, хто переслідує їх та інші [6].

Також, як свідчить практика, жертви кібернасильства, як і жертви інших форм насильства, приховують факти кібербулінгу по відношенню до себе через, наприклад, страх переслідувачів, та батьків, які можуть обмежити доступ до мобільного телефону, Інтернету.

На сьогодні злочини, що пов`язані з кібернасильством, мають чи не найгіршу статистику розкриття, це пов`язано з тим, що органам поліції не завжди вдається довести, що певні негативні наслідки спричинила саме агресія у віртуальному світі.

З метою запобігання кібербулінгу нами пропонується:

– бути уважним при передачі інформації про себе, особливо неперевіреним джерелам;

– завжди критично оцінювати інформацію, яку пропонує «всесвітня мережа». Варто пам`ятати, що не вся інформація є достовірною і часто потребує порівнянню з іншими джерелами тієї ж тематики

– ніколи не використовувати однакові чи схожі паролі доступу до мережі, PIN-коди та тому подібне.

Як висновок можна зазначити, що при дотримуванні хоча б цих трьох правил ризик зіткнутися з кібербулінгом у рази зменшиться і людина буде більше захищена від загроз, які спричиняє кібербулінг.

Список бібліографічних посилань

1. Найдьонова Л. А. Кібербулінг або віртуальна агресія: способи розпізнання і захист дитини : методичні рекомендації / Упоряд. В. О. Снігульська. К. : Редакції загально педагогічних газет, 2014. 96 с.

2. Кулик Є. В., Дайнека Н. М. Кібербуллінг як педагогічна проблема. *Вісник Чернігівського державного педагогічного університету*. Серія: Педагогічні науки. 2010. Вип. 80. С. 141.

3. Schellong A. Breaking down the threat of cyber terrorism URL: http://blogs.csc.com/ 2016/02/04/breaking-down-the-threat-of-cyber-terrorism (дата звернення: 30.10.2018).

4. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К. : ДУТ, 2015. 288 с.

5. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системноструктурний аналіз) : монографія. К. : КИТ, 2010. 408 с.

6. Davis K. Why Cybercrime is so Hard to investigate // Computer Crime Research Center. December 29, 2015. URL: http://www.crime-research.org/ articles/ 4002/ (дата звернення: 30.10.2018).

Одержано 01.11.2018