УДК 004.056.55

Фернега Є.І.
Шелепало Г.В.

КІБЕРБУЛІНГ ТА МЕТОДИ ПРОТИДІЇ ЙОМУ

Вінницький Національний Технічний Університет

Анотація

В даній статті розглянуто питання актуальності кібербулінгу. Наведено всі відомі методи його протидії на сьогодні, а також плани розвитку протидії в майбутньому.

Ключові слова: Кібербулінг, психологія, менталітет, цифровий розвиток, маніпулювання.

Abstract

This article discusses the relevance of cyberbullying. All known methods of its counteraction for today, and also plans of development of counteraction in the future are resulted.

Key words: Cyberbullying, psychology, mentality, digital development, manipulation.

Вступ

Актуальність проблеми кібербулінгу безпосередньо залежить від рівня розвитку цифрових технологій. Він може проходити в соціальних мережах, в додатках для обміну повідомленнями, на ігрових платформах і мобільних телефонах. Це повторювані епізоди, мета яких - налякати, розсердити або зганьбити тих, кого переслідують. На сьогодні не існує жодних заборон збоку закону щодо кібербулінгу. В даній статті розглядається питання виявлення та боротьби з інтернет-цькуванням.

Дослідження

Кібербулінг – це булінг із застосуванням цифрових технологій. Він може відбуватися в соціальних мережах, платформах обміну повідомленнями (месенджерах), ігрових платформах та мобільних телефонах. Це неодноразова поведінка, спрямована на залякування, провокування гніву чи приниження тих, проти кого він спрямований.

Для булінгу характерні такі ознаки [1]:

- Поширення неправдивої інформації або розміщення непристойних фотографій кого-небудь в соціальних мережах;
- Систематичність(повторюваність) діяння;
- Відправка ображаючих повідомлень або погроз через платформи обміну повідомленнями;
- Наявність сторони - кривдник (булер), потерпілій (жертва булінгу), спостерігачі (за наявність);
- Видача себе за іншу особу і відправка непристойних повідомлень від його імені.
- Дії або бездіяльність кривдника, наслідком якого є запобігання психічній та / або фізичної шкоди, приниження, страх, тривога, підпорядкування потерпілого інтересам кривдника та / або спричинення соціальної ізоляції потерпілого.

Окрім того варто розуміти відмінність між булінгом та кібербулінгом, зокрема відмінність зумовлюються особливостями інтернет-середовища: анонімністю, можливістю підмінити ідентичність, охоплювати велику аудиторію одночасно, (особливо дієво для поширення пліток), здатність тероризувати та тримати у напрузі жертву будь-де і будь-коли. Поміж того кібербулінг являється формую психологічного насильства.

На сьогодні кібербулінг має наступні типи [4]:

- Перепалка (флеймінг) - обмін короткими гнівними та запальними репліками між учасниками, з використанням комунікаційних технологій (як правило, на форумах та в чатах);
- Нападки (домагання) – регулярні висловлювання образливого характеру на адресу жертви (багато СМС-повідомлень, постійні дзвінки), що перевантажують персональні канали комунікації;
- Наклеп - поширення неправдивої, принизливої інформації;
- Самозванство - використання особистих даних жертви (логіни, паролі до акаунтів в мережах, блогах) з метою здійснення від її імені негативної комунікації;

• Публічне розголошення особистої інформації - поширення особистої інформації, наприклад шляхом публікування інтимних фотографій, фінансової інформації, роду діяльності з метою образи чи шантажу;

• Ошуканство - виманювання конфіденційної особистої інформації для власних цілей або передачі іншим особам;

• Відчуження (острокізм, ізоляція)- он-лайн відчуження в будь-яких типах середовищ, де використовується захист паролями, формується список небажаної пошти або список друзів;

• Кіберпереслідування - використання мобільного зв'язку або електронної пошти. Хулігани можуть тривалій час переслідувати свою жертву, створюючи брудний образ приниженого характеру або шантажуючи будь-які таємні факти.

• Хепіслепінг – реальні напади, які знімаються на відео для розміщення в Інтернеті, що можуть привести до летальних наслідків;

• Секстинг – обмін власними фото / відео / текстовими матеріалами інтимного характеру, із застосуванням сучасних засобів зв'язку (мобільні телефони, електронна пошта, соціальні мережі).

• Онлайн-грумінг – побудова в мережі інтернет дорослим або групою дорослих осіб довірливих стосунків із дитиною (підлітком) із метою отримання її інтимних фото/відео та подальшим її шантажуванням про розповсюдження цих фото.

Міжнародно-правова діяльність, спрямована на протидію кібербулінгу, має певні перешкоди в особливості через недостатньо розроблену законодавчу базу стосовно цеї галузі. Однак на даний момент, процес боротьби поділений на 3 основні напрямки: підвищення рівня безпеки інтернет-платформ, робота над законодавством, а також навчання громадян безпечній, адекватній і невіктимній поведінці в мережі. Деякі країни вже практикують кримінальну та цивільну відповідальність за даний злочин. Особливстю інтернет-цькування є те, що людина карається не державою, а натовпом людей в мережі. Таким чином за для швидкої та якісної самостійної боротьби з кібербулінгом варто знати послідовність дій.

Насамперед потрібно зібрати певні матеріали, що являються доказами інтернет-цькування: скріншоти листування, ображаючих, або недостовірних постів в соціальних мережах, посилання на фейкові акаунти, запис погроз або цькування в голосових повідомленнях. Надалі, варто захистити свої особисті дані, а саме перевести свій акаунт в мережі в приватний режим, якщо відомо хто саме вас цькує, то заблокувати даного користувача, або добавити в чорний список. Наступним кроком є звернення до адміністрації додатку в якому здійснюється кібербулінг, якщо відомо хто саме це робить, адміністратор заблокує обліковий запис користувача, у випадку анонімного кібербулінгу, буде відбуватись постійний моніторинг повідомлень, та в разі наявності можливостей підозрілих акаунтів. В особливих випадках, коли кібербулінг переходить межу цівільного кодексу, та застосовується в якості погроз життю або вимаганню грошей, варто звернутись по допомогу у відповідні правоохоронні органи влади.[2]

Якщо ж людина стала жертвою Кібербулінгу, важливо вчасно це розпізнати.

Серед основних ознак [3]:

• Часті зміни настрою;

• Нервові відповіді на питання;

• Спропи уникати спілкування з друзями, колегами, знайомими, рідними і т.д.;

• Пропустити школу, університет, роботу і т.д.;

• Видалення профілів з соціальних мереж.

На сьогодні ведеться активна протидія кібербулінгу: в школах створюють додаткові уроки для освідомлення дітей в даній галузі та мінімальній можливості протидіяти, створюються відповідні додатки для різних пристроїв за для відслідкування ознак кібербулінгу (програми батьківського контролю в тому числі), проведення спеціальних курсів для ознайомлення з протидії цькуванню, підготовлення відповідних законопроектів щодо кібербулінгу. Окрім того, за статистикою близько 70% кібербулінгу застосовується проти підлітків, значну частину потерпілих становить жіноча стать. Однак 50% підлітків не звертаються по допомогу у відповідні організації та навіть до рідних, саме тому на даний момент уже існують спеціальні цілодобово-працюючий сайти та оператори для допомоги людям, стосовно яких застосовувався кібербулінг.

Дослідження Kaspersky Lab та незалежного агентства B2B International розповсюдили 10 простих порад для убезпечення від можливих наслідків кібербулінгу [5]:

1) Залишайтеся спокійними. В такій ситуації не варто гарячкуватись та метушитись;

2) Не відповідайте. Дуже важливо не вступати в розмову з кібербулером, адже цього вони й намагаються досягти;

3) Робіть скріншоти. Знімки прояву цькування можуть бути корисними в подальшій протидії;

4) Поділіться своїми переживаннями з іншими. Якщо після даної ситуації, ви відчуваєте себе незадовільно, варто з кимось поговорити;

5) Заблокуйте кібербулера. Одразу потрібно заблокувати кривдника та внести до «чорного списку», щоб він не зміг з вами зв'язатись;

6) Подайте скаргу. Як уже згадувалось раніше, в подібних ситуаціях варто звертатись до адміністрації соціальної мережі, аби вони прийняли відповідні міри;

7) Протидійде діям кривдника. Якщо ви знайомі з кібербулером в реальному житті, варто йому наказати припинити свою діяльність;

8) Не бійтесь вживати рішучих засобів. Якщо вас атакують інтернет-кривдники, не варто бездіяти. В таких випадках варто діяти, іноді навіть одна дія може відштовхнути кібербулера;

9) Змініть налаштування приватності. Варто переконатись, що до вашого профілю немають доступу інші користувачі;

10) Перегляньте список друзів, аби запевнетись у відсутності підозрілих користувачів;

За думкою статистичного відділу ООН, саме подібне вирішення питання, забезпечить зменшення проценту населення потерпілих від інтернет-цькування, та збільшисть спроможність населення коректно та оперативно протидіяти подібним діям.

Висновок

Підвівши підсумки дослідженої теми, слідує, що головними причинами стрімкого поширення кібербулінгу є: відсутність етикети спілкування між відомими особами (за якими спостерігають більшість населення, в тому числі і підлітки, які беруть з подібних людей приклад), нерегулювання державою контенту в мережі, реальний булінг, що переходить на простори мережі, а також цифровий розвиток, що вносить найбільший вклад в даний вид свавілля. Паралельно розвитку причин кібербулінгу, розвиваються шляхи розв'язання даної проблеми. На даний момент гіганти соціальних мереж «Facebook» та «ВКонтакте» мають спеціалізовані центри запобігання інтернет-цькуванню, що в дійсності єдина зброя проти кібербулінгу на даний момент.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кібербулінг – що це та як це зупинити? [Електронний ресурс] / С.Лівінгстон, А. Серд, М. Агбай, С. Блайт // Unicef. – 2019. – Режим доступу до ресурсу: https://www.unicef.org/ukraine/cyberbulling.
2. Авганов С. Кібербулінгу. Або трохи про інтернет-цькування [Електронний ресурс] / Сергій Авганов // Online Zakon. – 2019. – Режим доступу до ресурсу: https://online.zakon.kz/Document/?doc_id=37000746#pos=68;-67.
3. Методи протидії кібербулінгу [Електронний ресурс] // eset. – 2020. – Режим доступу до ресурсу: https://eset.ua/ru/blog/view/34/kak-predotvratit-kiberbulling-sovety-roditelyam.
4. Турубара К. Кібербулінг: що це, яким він буває та як від нього захистити свою дитину [Електронний ресурс] / Катерина Турубара // Telegraph. – 2019. – Режим доступу до ресурсу: https://www.telegraf.in.ua/kremenchug/10082081-kberbulng-scho-ce-yakim-vn-buvaye-ta-yak-vd-nogo-zahistiti-svoyu-ditinu.html.
5. Як боротися з Буллінг в мережі? [Електронний ресурс] // Epicentrk. – 2019. – Режим доступу до ресурсу: https://epicentrk.ua/articles/kak-borotsya-s-bullingom-v-seti-lang-yak-borotisya-z-bulingom-v-merezhi.html.

Фернега Євгеній Іванович – студент групи КІТС-19б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail evgeniyfernega@gmail.com .

Науковий керівник: ***Шелепало Галина Василівна*** – кандидат фіз.-мат. наук, доцент кафедри ЗІ ВНТУ.

Fernega Yevheniy Ivanovych – student of KITS-19b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail evgeniyfernega@gmail.com .

Supervisor: ***Shelepalo Halyna Vasylivna*** – candidate of Physical and Mathematical Sciences, Associate Professor of the Department of IS VNTU.