УДК 004.056.5: 342.922/951 DOI: 10.26565/2519-2310-2020-1-02

ДОСЛІДЖЕННЯ ЯВИЩА КІБЕРБУЛІНГУ ТА АНАЛІЗ ШЛЯХІВ ПРОТИДІЇ ЙОГО ПРОЯВАМ

Валерія Гайкова, Сергій Малахов

Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна
valeriagaikova98@gmail.com, mailgate@meta.ua

Рецензент: Володимир Хома, д.т.н., проф., Опольський політехнічний Університет, Ополе, Польща
xoma@wp.pl

Надійшло: Березень 2020.

Анотація: *В роботі досліджено основні характеристики Інтернет-травлі (кібертравлі або кібербулінгу). Розглянуті основні особливості проявів цього явища. Виконано аналіз існуючих видів кібербулінгу і їх окремих характеристик. Розглянуто приклади законодавчих актів різних країн щодо протидії кібербулінгу. За результатами огляду наявної нормативно-правової бази різних країн, зроблений висновок про істотний дефіцит відповідних норм законів. Підкреслено, що в сучасному світі жертвою Інтернет-травлі може стати будь-хто. При цьому, ризик стати жертвою кібербулінгу практично не залежить від будь яких факторів (наприклад, фінансового становища жертви, її віку, статі, соціального стану та ін.). Відзначено, що комунікації, які здійснюється в кіберпросторі надають користувачам можливість заздалегідь та ретельно вибирати інформацію про себе, яку вони хочуть оприлюднити. У більшості випадків це сприяє тому, що люди демонструють тільки свої «позитивні» сторони (наприклад, при спілкування в чатах). В результаті цього у мережевих співрозмовників часто виникають помилкові взаємні симпатії, внаслідок чого вони необачно вступають в довірчі відносини. Таким чином відбувається ідеалізація партнера по мережевої комунікації, та будь-яка його інформація починає сприйматися набагато більш чуйно, аніж при прямій «фізичній» комунікації. Цей ефект з «успіхом» використовується при проведенні акцій кібербулінгу, коли одна людина спочатку викликає максимальну довіру іншого, а потім різко змінює тактику спілкування, стаючи немотивовано віроломним і агресивним. Підкреслено, що явище кібербулінгу є дуже недооціненим і тому являє собою серйозну проблему.*

Виконано короткий огляд існуючих технологій і засобів протидії цьому явищу. Проведено порівняння їх ефективності. Систематизовано критерії, яким повинна відповідати сучасна і ефективна технологія протидії кібербулінгу. Представлені приклади вдалої реалізації захисту користувачів у деяких найбільш популярних соціальних мережах. Акцентовано увагу на тому, що для протидії кібербулінгу, в теперішній час, в переважній більшості випадків, використовують технології захисту на основі обмежень. Головна мета відповідних засобів захисту полягає у тому, щоб максимально локалізувати небажаний контент (з точки зору існування ознак кібербулінгу).

За результатами роботи стверджується, що і в подальшому кібербулінг буде тільки поширюватись. Це обумовлено постійним збільшенням чисельності користувачів нових мережевих сервісів та онлайн майданчиків для спілкування. Висловлено думку, що для активної протидії та ефективного захисту від кібербулінгу потрібно впровадження комплексних організаційно-технічних заходів. На завершенні запропонована загальна оцінка подальшого розвитку кібербулінгу і шляхів вдосконалення відповідних інструментів протидії.

Ключевые слова: *булінг; кібербулінг; соціальна мережа; інформаційна безпека; контент; захист; технологія; мережева безпека.*

1 Вступ

Наш час характеризується стрімким та багатовекторним розвитком інформаційно-комунікаційних технологій, що суттєво змінює характер виробничих, соціально-політичних і морально-етичних відносин, які, в своїй сукупності, формують нові критерії норм поведінки не тільки у сучасному суспільстві, а й у кіберпросторі. Такі речі як смартфон і комп'ютер стали невід'ємною частиною буденного життя сучасної людини. Інтеграція всіх існуючих пристроїв в єдине інформаційне середовище, за рахунок використання глобальної мережі Інтернет, надання функцій мобільності її абонентам та практично безперервний зв'язок, фактично створили нову реальність. Ця реальність спроможна надати людству нову якість життя але, з іншого боку, несе в собі і нові загрози, та фактори ризику нових форматів, і змісту. Так, наприклад, наразі Інтернет використовується майже у всіх сферах життя сучасної людини: - для роботи, навчання, розваг, забезпечення побутових потреб, підтримання соціальних контактів і багато чого іншого. Проте, поряд з великою кількістю позитивних сторін, нові інформаційні технології (ІТ- технології) мають і свої, приховані від непідготовленої людини,

загрози [1]. В цьому сенсі, однією з найгостріших проблем, яка пов'язана з широким використанням нових можливостей ІТ-технологій, є загроза потенційного зіткнення людини (*користувача будь якого онлайн сервісу або пристрою, що має з'єднання з мережею*) з агресивними нападками окремих представників мережевої спільноти, що називають кібербулінгом.

Кібербулінг – це форма залякування, яке відбувається, в тому числі, за рахунок можливостей Інтернет технологій, та використання різних електронних пристроїв (смартфонів, планшетів тощо). Кібербулінг може реалізуватися за допомогою соціальних мереж, електронної пошти, додатків для обмінну миттєвими повідомленнями, текстових повідомлень, форумів, комп'ютерних ігор та багато чого іншого. Принциповим є те, що будь-яке онлайн середовище, яке дозволяє обмінюватися даними, може стати технічною платформою для здійснення Інтернет-травлі [2].

Свого найбільшого поширення кібербулінг набув у молоді, але не слід вважати, що жертвою Інтернет-травлі можуть бути лише представники молодого покоління. В сучасному світі жертвою Інтернет-травлі може стати будь-хто, і це не залежить а ні від фінансового статку, а ні від віку, а ні від статі, соціального стану та іншого.

Актуальність даної роботи обумовлена тим, що по мірі поширення новітніх віртуальних сервісів та комунікаційних технологій, явище кібербулінгу теж набуває все більших масштабів та форм його проявів. Його наслідки можуть бути найрізноманітніші, від тяжкої психічної травми конкретної людини до порушення поточного балансу відносин (*виробничих, соціальних, культурних та ін.*) в рамках цілих соціальних груп або окремих співтовариств. Тому знати цю проблематику та володіти відповідними знаннями щодо можливостей протидії цьому явищу, є важливим напрямком фахових компетенцій сучасних фахівців з інформаційної безпеки (ІБ).

2 Основні визначення і характеристики кібербулінгу

В наслідок стрімкого розвитку ІТ-технологій безліч, раніше звичних явищ, в теперішній час, набувають нових форм та масштабів можливих наслідків. Це стосується і питань еволюції прояву взаємної людської агресії, яка існує у віртуальному просторі, і як наслідок, формування певних поведінкових норм мережевої етики, котрі тісно пов'язані з проблематикою протидії можливим наслідкам мережевої агресії та віртуального маніпулювання особистістю.

Булінг (*тобто знущання*) [3] – різновид насильства; навмисне, що не носить характеру самозахисту і не є санкціонованим нормативно-правовими актами держави, довготривале (*повторюване*) фізичне чи психологічне насильство з боку індивіда чи групи, які мають певні переваги (*фізичні, психологічні, адміністративні тощо*) стосовно індивіда, і що відбувається переважно в організованих колективах з певною особистою метою (*наприклад, бажання заслужити авторитет у бажаних осіб і т.і.*).

Булінг був проблемою з найдавніших часів. Хоч більшість людей і намагається жити у цивілізованому, мирному суспільстві, але, нажаль, є люди, які хочуть виплеснути свою агресію на того, хто слабший за них. З часом тривіальний булінг у реальному житті переріс у нове явище, яке називається кібербулінг. Тобто знущання у віртуальному світі.

2.1 Джерела походження явища булінгу

Практично неможливо точно сказати коли люди почали проявляти психологічну агресію один до одного. Термін булінг не був публічно визнаний доти, поки відома англійська газета не зробила статтю з даною темою. У 1862 році, через сімдесяти двох років публікацій щотижнева газета «*The Times*» написала свою першу розповідь про булінг [4]. У той час булінг сприймався багатьма як нормальна поведінка. Проте, після того як це явище стало більш поширеним, воно стало привертати до себе все більше уваги дослідників, які хотіли дізнатись більше про ймовірні причини, мотиви та можливі наслідки.

Найбільш значущий момент (*в історичному сенсі*) булінга був у середині 70-х років минулого століття. Професор психології *Dan Olweus* першим провів інтенсивне дослідження явища булінгу серед учнів, використовуючи при цьому свої особисті методи дослідження. Слід

зазначити, що зусилля Олвеуса справили великий вплив на зменшення рівня шкільного насилля та допомогли підвищити безпеку учнів у школі [5].

Розглядаючи явище булінгу принципово важливо підкреслити, що знущання можуть траплятися у різному віці, у різних місцях, у різних соціальних та техногенних середовищах, та як свідчить реальність, з використанням різноманітних технологічних здобутків.

Хоч кожен окремий випадок булінгу по своєму унікальний, у більшості ситуацій є три породжуючи фактори [6]:

1. *Намір*. Випадкова образа, скоріш за все, не є булінгом. Ті, хто знущаються свідомо, добре розуміють, що саме роблять вони, і тому шкода буде навмисною;
2. *Дисбаланс влади*. У більшості випадків кривдник має більшу владу. І зовсім не означає, що кривдник обов'язково більше або сильніше за жертву. Він може, наприклад, займати більш високий пост на роботі, або бути вихідцем з багатої родини тощо;
3. *Повторювання*. Одноразовий образливий вчинок по відношенню до людини не є булінгом. Булінг це навмисна дія, яка згодом буде систематично повторюватись.

Повертаючись до історії слід відмітити, що наприкінці 90-х років XX-го сторіччя наслідки залякування досягли свого піку [7] і прийняли ще один негативний еволюційний поворот. Завдяки поширення доступу до мережі Інтернет, багато підлітків почали використовувати кіберпростір як майданчик для булінгу [5]. Враховуючи те, що в сучасному світі переважна більшість людей для спілкування та роботи використовують дуже широкий спектр різних гаджетів, то явище кібербулінгу набуло нових якостей, поширилось у віртуальному світі і стало великою проблемою, яка безпосередньо впливає не тільки на характер взаємовідносин людей в сучасному мережевому просторі, але і в їх реальному житті.

Офіційний науковий термін «кібербулінг» ввів канадський педагог *Bill Belsey*. Згідно його тлумачення, кібербулінг – це навмисна, повторювана ворожа поведінка окремих осіб чи груп, маючих намір спричинити шкоду іншим, використовуючи при цьому інформаційні і комунікаційні технології [8]. В сучасному розумінні кібербулінг став поширеним явищем у середині 2000-х років, коли звичайні смартфони, як інтегрований засіб мобільних комунікацій, набули популярності та стали повсякденним компонентом сучасного життя.

2.1.1 Особливості та мотивації кібербулінгу

Як було зазначено вище, кібербулінг – особливий вид Інтернет комунікації. Серед головних особливостей [9] даного типу комунікацій слід виділити наступні:

- *Безперервність*. Комунікація в мережі Інтернет (*надалі мережі*) майже не має обмежень за часом: - користувачі можуть у будь-який час «вийти» з діалогу, та в будь-який час його продовжити;
- *Мультіконтентність*. Користувачам мережі надаються багаточисельні інструменти і засоби спілкування: - текст, графічні зображення, фото- й відеоматеріали, аудіо контент і тому подібне;
- *Анонімність*. Один з ключових факторів кібербулінгу. Будь-яка людина може реєструватись в мережі під будь-яким неіснуючим образом (*віртуальним аватаром*), який приховує реальну особистість. Це дозволяє деяким користувачам мережі виключити чинник персональної відповідальності за можливі наслідки своїх дій у віртуальному просторі.
- *Опосередкованість*. Інтернет комунікації, в своєї більшості, є непрямим діалогом між її учасниками, котрі часто не знайомі, безпосередньо не бачать один одного, та не можуть використовувати такі невербальні засоби комунікації як: - жести, міміка тощо (*виключенням є відеоконференцзв'язок, але це є не типовий спосіб здійснення кібертравлі*).

Зазначені особливості віртуальної комунікації приваблюють потенційних агресорів, які почувають себе в умовах мережі дуже безпечно та комфортно. Навіть, якщо у реальному житті вони нікому і не завдають шкоди, то в разі використання можливостей ІТ- технологій, внаслідок помилкового враження про відсутність контролю та безкарність, такі люди можуть почати проявляти свою агресивну сутність по відношенню до інших представників мереже-

вої спільноти. Можна стверджувати, що кібербулінг дозволяє мережевому нападнику уникнути відповідальності, так як, не застосовуючи пряме насильство над жертвою, він в більшості випадків, зможе ухилитись від особистої відповідальності. Більш того, для деяких кіберзлочинців вирішальним плюсом є саме те, що булінгом можна займатись не змінюючи привичного їм образу життя та практично з любого місця, де є доступ до мережі.

З досліджень на цю тему слід звернути увагу на роботи доктора психологічних наук *Al Cooper* [10]. У одній зі своїх робіт він виділив три найпривабливіші, на його думку, аспекти Інтернет-комунікації та назвав їх принципом «Потрійного А» (*від анг. «Triple A» – Anonymous, Accessible and Affordable*): 1 – анонімність; 2 – доступність; 3 – низька ціна.

Про *анонімність* вже було сказано вище. Саме цей аспект робить булінг дуже привабливим для його виконавця. Тут спрацьовує так званий «*ефект дистанціювання*», який передбачає, що мережевий агресор, який знаходиться на відстані від своєї жертви, робить більш жорстокі речі, ніж при звичайному прямому спілкуванні [11].

Доступність підключення до Інтернету, також значно полегшує процес кібербулінгу. На сьогоднішній день доступ до Інтернету є майже усюди (*високошвидкісні Ethernet та безпровідне з'єднання*) [1]. Причому, завдяки мобільним пристроям і високошвидкісним бездротовим мережам, цей доступ користувачі отримують практично безперервно [12, 13].

Низька ціна – вартість участі в Інтернет комунікації. При наявності у людини комп'ютера або будь-якого мобільного пристрою з доступом до мережі (*корпоративною або напряму з Інтернет*), практично забезпечує його технічну готовність до здійснення потрібних віртуальних комунікацій.

Як вже було зазначено вище, люди які вдаються до кібербулінгу, у реальному житті частіше за все не проявляють ніяких агресивних вчинків. При цьому кібербулінг, в першу чергу, приваблює тих людей, хто бажає миттєво змінити в віртуальному світі свій реальний стан, на іншу, більш сильну або привабливу позицію (*в будь-яких розуміннях*). Перш за все таких людей приваблюють переваги комп'ютерно-опосередкованої комунікації, які описані у «Гіперперсональній моделі комунікації» [14]. Завдяки визначеним особливостям Інтернет комунікації (*анонімність, знижені соціальні рамки, можливість попереднього планування дій, можливість ретельно обміркувати свою відповідь тощо*) онлайн комунікація стає ідеальним засобом для особистої презентації у навмисно перекрученому вигляді.

Комунікація, що здійснюється в кіберпросторі надає користувачам можливість ретельно вибирати інформацію про себе, яку вони хочуть надати в широкий доступ (*оприлюднити*). У більшості випадків це сприяє тому, що люди показують тільки свої «позитивні» сторони (*наприклад, спілкування в чатах*). В результаті цього у співрозмовників часто виникають симпатії один до одного, та вони вступають в довірчі відносини. Таким чином відбувається ідеалізація партнера по мережевої комунікації, і його інформація починає сприйматися набагато більш чуйно, аніж при прямій «фізичній» комунікації. Цей ефект з «успіхом» використовується в кібербулінгу, коли одна людина спочатку викликає максимальну довіру іншого, а потім різко змінює тактику спілкування, стаючи агресивним. В цьому сенсі онлайн комунікація дозволяє нападнику заздалегідь обмірковувати свої наступні дії (*тип контенту і форму його подання*) і, в певній мірі, контролювати часові параметри атаки (*інтенсивність видачі контенту, тривалість пауз та ін.*).

2.1.2 Компоненти кібербулінгу

Кібербулінг складається з декількох обов'язкових компонентів (*учасників процесу*), що впливають на те, як саме відбувається кожен конкретний прояв булінгу (*окремі властивості та чисельність кожної з груп*). Практично у кожному випадку учасники кібербулінгу поділяються на три категорії: – агресор, жертва і спостерігач (Рис. 1). Кожний з цих елементів може бути представлений, як в однині, так і в множині, тобто процес може відбуватися в групах. А сам процес може бути реалізований миттєво або бути пролонгованим у часі.

Агресор – людина (*або група*), яка навмисно ображає, несе загрозу чи агресію, щоб визвати страх чи страждання у інших.

Жертва – той (*група*), кого (*групу*) переслідує агресор. Жертви не можуть легко захищати себе і, по ряду причин, є більш слабкими ніж агресор.

Спостерігач – особа (чи група), яка є свідком інциденту, але не є його прямим учасником. В окремих випадках спостерігачі можуть оказувати підтримку жертві, реагуючи проти агресора. Але, вони, також, можуть посилювати «страждання» жертви, що були завдані агресором, опосередковано підтримуючи їх дії.

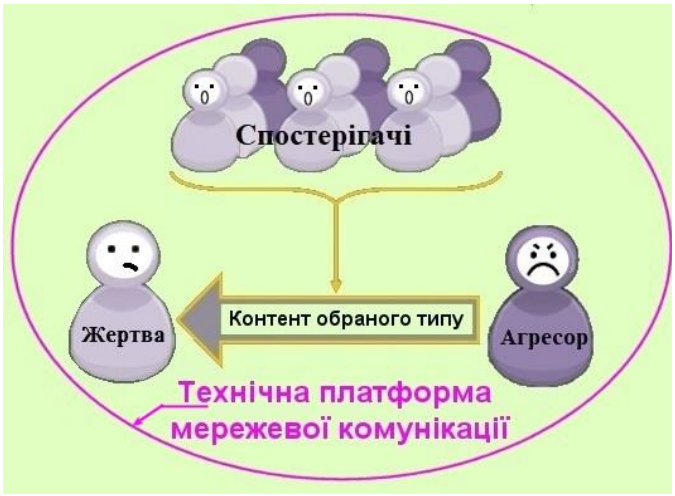

Рис. 1 – Складові процесу кібербулінгу

Платформа, на базі якій відбувається кібербулінг, також є дуже впливовим компонентом у цьому явищі. У загальному випадку платформа являє собою сукупність програмно-технічних засобів, а в деяких випадках і каналів зв'язку, за допомогою яких забезпечується функціональна взаємодія її абонентів. Так наприклад, на сьогоднішній день, соціальні мережі є основними комунікаційними платформами, які розгорнути на базі мережі Інтернет.

Соціальна мережа – це Web-платформа для побудови соціальних відносин між людьми зі схожими інтересами і діяльністю [15]. Соціальні мережі являють кожного зі своїх учасників через її особисту сторінку (*профіль, акаунт*), яка переважно містить особисту інформацію та інтереси користувача. Вони також надають користувачам засоби для взаємодії, наприклад, за допомогою миттєвих повідомлень. Сайти соціальних мереж різноманітні і пропонують різні види діяльності, такі як: обмін фото та відео, публікація коментарів та відстеження дій інших користувачів в мережі.

Ще одним обов'язковим елементом процесу кібербулінгу є *контент* та метод, за допомогою яких відбувається кібербулінг. Це може бути відео або фото зображення, комп'ютерна анімація (*включаючи комп'ютерну гру*), статичний текст, будь-яка інфографіка та ін.

Технічні можливості кожної платформи (*наприклад, підтримка можливості ведення чату, можливість передачі мультимедійного контенту, підтримка мобільності абонентів та ін*.) мають істотний вплив на організацію процесу цькування. Також, свої особливості *(наприклад, неспівпадіння видів контентного наповнення або часові параметри комунікації*) має і процес підтримки комунікацій для користувачів різних платформ (*кроссплатформна взаємодія*). Наявність різниці в часі підтримки з'єднання (*різниця в тарифікації послуг в межах кожної платформи*) та забезпечення мобільності абонентів (*доступ до бездротових мереж*) суттєвим образом, можуть змінювати конфігурацію процесу кібербулінгу та, в певній мірі, його наслідки. Таким чином, комбінація всіх зазначених обставин та факторів, обумовлює потенційне різноманіття можливих реалізацій кібербулінгу.

2.1.3 Види кібербулінгу

Наразі неможливо точно сказати які є види кібербулінгу. Через те, що це явище відносно нове, та постійно і швидко розвивається, різні дослідники по-різному класифікують прояви кібербулінгу. Ще однією причиною цього є те, що Інтернет-травля з кожним роком все більше поширюється, і разом з тим набуває нових форм і проявів. У межах даної роботи розглядаються тільки два різних трактування існуючих видів кібербулінгу: - точка зору, що поєднує погляди фахівців західних країн світу та сукупна точка зору вітчизняних фахівців за даною проблематикою.

У західній класифікації *Nancy E. Willard*, автор видання «*Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress*» (2007), виділила та організувала кібербулінг у сім різних категорій [16]:

1 – флеймінг (*Flaming*);
2 – домагання (*Harassment*);
3 – поширення чуток (*Denigration*);
4 – кіберсталкінг (*Cyberstalking*);
5 – самозванство (*Impersonation*);
6 – брехливість (*Outing* & *Trickery*);
7 – соціальна ізоляція (*Exclusion*).

Розглянемо кожен вид докладніше.

Флеймінг. Під цим видом Інтеренет-залякування розуміють короткі суперечки між учасниками онлайн комунікації. Це можуть бути різноманітні гнівні та образливі коментарі, повідомлення і т.д. Місцем для флеймінгу частіше за все виступають «публічні» майданчики Інтернету (*наприклад, форуми, чати і т.і.*). Часто, такий вид кібербулінгу переростає в затяжну «війну» між його учасниками. Хоч і здається, що флеймінг трапляється між рівними людьми, але інколи, він також може перетворитися на затяжний психологічний нерівноправний терор. Наприклад, це трапляється тоді, коли особа не знає скільки людей її підтримує, і чи буде її позиція підтримана найавторитетнішими учасниками даної комунікації.

Домагання (*харасмент*), передбачає регулярні виснажливі нападки на людину. Прикладом може бути постійне надсилання великої кількості образливих електронних листів, текстових повідомлень (*в т.ч. SMS-повідомлень з використанням можливостей платформи стільникового мобільного зв'язку*), електронних повідомлень із неприємними зображеннями і т. ін. Також до цієї категорії можна віднести численні телефонні дзвінки. Відмінність від флеймінгу полягає у тому, що в цьому випадку кількість повідомлень значно більше, і приходять вони, частіше, в односторонньому порядку.

Слід відмітити, що нещодавно з'явилась нова форма харасменту – гріфінг (*griefing, з англійської «grief» - горе, смуток*) [17]. Цей вид булінгу передбачає спрямоване притиснення одного з учасників комп'ютерної гри. Агресори у даному випадку, називаються гріфери. Це група гравців, метою яких є руйнування ігрового досвіду інших учасників гри. При цьому принциповим є той факт, що перемога у грі вже не є пріоритетом у даних гравців.

Поширення чуток. Ця категорія кібербулінгу передбачає навмисне розповсюдження неправдивої образливої інформації за допомогою електронних засобів комунікацій. Треба підкреслити, що цей вид кібербулінгу передбачає те, що агресор знає, що інформація є заздалегідь неправдивою. При цьому в якості такої інформації може виступати будь-який доступний контент. Для цього агресори створюють так звані «книги для критики» (*Slam Books*), головним сенсом котрої є розміщення образливих жартів про жертву, а також різноманітних наклепів. Потім, з таких книг обираються «мішені», на котрих інші будуть фокусувати свою агресію. Також прикладом поширення чуток є розсилка різноманітних образливих списків (*наприклад, «хто є хто»*).

Кіберсталкінг це скритне вистежування людини, і тих, хто знаходиться поряд із нею. Як правило це робиться анонімно, беручи за мету різноманітні злочинні дії. За допомогою різноманітних сервісів мережі Інтернет злочинець відстежує користувачів-жертв, дізнається про час, місце і всю іншу інформацію, що необхідна для подальшого скоєння злочину.

Самозванство, тобто втілення в іншу особу, це коли агресор присвоює собі повноваження або ознаки іншої людини, використовуючи при цьому акаунти жертви у соціальних мережах, пошті, блогах, різноманітних месенджерах і т. і. Для цього злочинець якимось чином *обов'язково* повинен заволодіти автентифікаційними даними жертви, а після нелегітимного проникнення у необхідний мережевий профіль жертви, злочинець здійснює спланована негативну комунікацію, тобто надсилає іншим людям образливу інформацію. Після того, як з адреси жертви (*без її відому*) відбулася відправка злочинних повідомлень, трапляється так звана «хвиля зворотних зв'язків».

При цьому розгублена жертва не розуміє у чому справа. Таким чином, агресор робить провокацію, залишаючись, при цьому, непомітним для всіх сторін здійсненої їм фіктивної комунікації.

Брехливість передбачає те, що злочинець якимось чином отримує доступ до чутливої інформації про особу, а потім несанкціоновано розповсюджує її у мережі. У цьому разі за мету агресор ставить знищення репутації жертви, та спробу зміни ставлення до неї інших людей.

Різновидом *брехливості* є секстінг (*Sexting*). До нього відноситься поширення особистих фото відвертого характеру, без згоди жертви, а також повідомлення інтимного змісту за допомогою різних засобів зв'язку. Нажаль, такі дані залишаються у мережі надовго що створює загрозу кар'єрного, психічного і фізичного насилля над жертвою.

Соціальна ізоляція є особливо тяжкою категорією булінгу (*особливо для підлітків*). Так як людина є соціальною істотою, то її виключення з певного соціуму, в переважній більшості випадків, може сприйматись дуже тяжко. У онлайн середовищі ізоляція теж несе дуже неприємні наслідки. Ізоляція можлива у будь-яких середовищах, де можливо сформувати різноманітні списки (*наприклад, «найкращі друзі» у соціальній мережі Instagram*), заблокувати користувача, чи сформувати список небажаних повідомлень. В цьому сенсі, відсутність швидкої відповіді на електронне повідомлення теж може бути віднесено до соціальної ізоляції.

В контексті вищезазначеного слід підкреслити, що у деяких фахівців з окресленої проблематики є дещо інша точка зору. Так, наприклад, думка психолога Галини Солдатової [18] стосовно існуючих різновидів кібербулінгу відрізняється від загальноприйнятих критеріїв. Зі своєї сторони вона виділяє три основні види Інтернет-травлі: 1 – флеймінг (*Flaming*); 2 – хейтінг (*Hate*); 3 – тролінг (*Cyber trolls*).

Хейтінг передбачає негативні коментарі і неконструктивну критику в адресу об'єкту травлі без обґрунтування або запиту. У час, коли великого поширення здобув такий рід діяльності як блогерство (блогер – людина яка веде свій он-лайн щоденник, у який записує тексти на різні тематики, публікує фото- і відео-контент), хейтінг став дуже критичною проблемою. Слід особливо підкреслити, що даний вид кібербулінгу передбачає саме неконструктивну критику. Це можуть бути коментарі про зовнішність людини, її діяння та багато іншого.

Тролінг (*кепкування*) передбачає провокування жертви до діалогу, використовуючи в переважної більшості насмішки чи образливі коментарі. Тролі (*нападники*) можуть бути відносно нешкідливими (*одноразові жарти у коментарях*), але можуть збиратися у цільові групи і водночас атакувати жертву, використовуючи для цього всі наявні ресурси та засоби. За статистичними даними [19], близько чотирьох з десяти користувачів мережі хоч раз принижували чи ображали когось в Інтернеті, а тих, хто був свідком нападу тролей у рази більше.

Кібербулінг все частіше призводить до трагічних випадків. Не розуміючи, що їх вчинки можуть призвести до дуже серйозних наслідків, злочинці стають все більш вигадливими і злими. У США навіть з'явився новий термін «буліцид». Віз означає загибель людини внаслідок булінгу.

2.2 Аналіз статистичних даних щодо кібербулінгу

Щоб наглядно підтвердити всю актуальність проблеми кібербулінгу, потрібно звернутися до відповідних статистичних даних. Варто зауважити, що, нажаль, більшість статистичних даних стосуються лише підлітків та дітей.

Задля підтвердження актуальності проблеми поширення кібербулінгу, звернемося до відповідних статистичних даних [20-21]:

– один з трьох підлітків у 30 різних країнах стверджує, що він був жертвою булінгу в Інтернеті, при цьому кожен п'ятий повідомив, що пропустив школу саме через кібербулінг;

– 37 % підлітків у віці від 12 до 17 років піддавалися знущанням в Інтернеті, а у 30 % опитаних, це було не одноразово;

– 23 % студентів повідомили, що вони зробили щось погане по відношенню до іншої людини в Інтернеті;

– 27 % студентів піддавалися зовнішнім образам в мережі;

– 60 % підлітків стали свідками знущань в Інтернеті, але більшість з них не втручалася в цей процес;

– тільки 1 з 10 постраждалих підлітків повідомили дорослим про ці інциденти.

На рис. 2-3 приведено результати опитування підлітків щодо кібербулінгу, які були отримані організацією *Unicef* [22]. Аналіз відповідних даних дозволяє зробити висновок: - в Україні 21,5 % школярів були жертвою Інтернет-травлі, а 4,1 % з них піддаються постійному кібербулінгу (*один чи декілька разів на тиждень*).

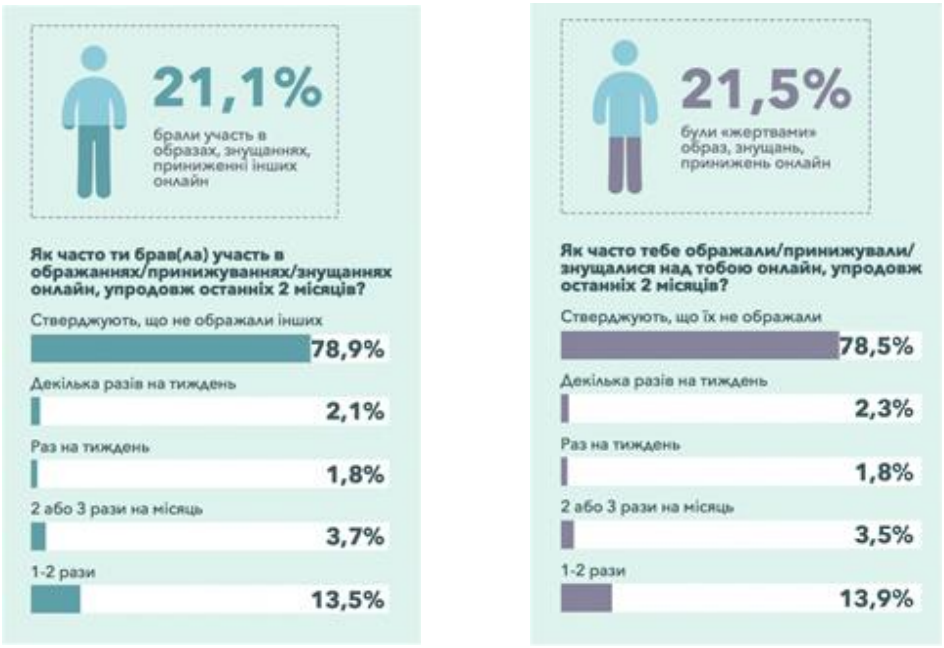

Рис. 2 – Дані щодо кібербулінгу серед підлітків України

Рис. 3 – Час, який підлітки витрачають на соціальні мережі

3 Особливості законодавчого врегулювання кібербулінгу

За результатами аналізу найбільш показових прикладів боротьби з кібербулінгом на законодавчому рівні (США [23], Канада [24], Швеція [25], Франція [26], Великобританія [27], Іспанія [28], деякі країни СНД [29-31], Україна [32-36], Південна Африка, Японія, Сінгапур та ін. [37]), можна стверджувати наступне:

1 – в тих випадках коли відсутні прямі норми, що стосуються булінгу і кібербулінгу, такі випадки можуть бути трактовані, як дискримінаційні домагання, якщо вони засновані на расі, кольору шкіри, релігії, віку, статі чи інвалідності тощо. В цьому разі, інколи, для злочинців можуть бути висунуті федеральні звинувачення у переслідуванні (*наприклад, в США*). При цьому, якщо булінг переростає у переслідування, то навчальні заклади, які отримують федеральні (*державні*) кошти, зобов'язані вирішити дану проблему;

2 – в разі федеративного устрою держави, існує розмежування відповідальності на регіональному та федеральному рівнях. Причому баланс відповідних законодавчих актів у кожній окремій країні має свою специфіку. Наприклад, у США кібербулінг, у першу чергу, підпадає під закони штатів. При цьому у більшості штатів у правоохоронних органах навіть є спеціальні підрозділи по боротьбі з кіберзлочинністю [23];

3 – у разі існування відповідної законодавчої бази, ці закони часто поділяються на ті, що стосуються дітей та підлітків, а також закони, які захищають дорослих жертв кібербулінгу чи жертв будь-якого віку [23];

4 – в залежності від конкретної країни, відповідальність за даний тип злочину (*булінгу і кібербулінгу*) може передбачати собою позбавлення волі та/чи штраф у відповідному розмірі;

5 – в більшості країн світу працівники навчальних закладів повинні повідомляти про будь-які відомі їм випадки булінгу, що сталися в їх установах;

6 – в більшості країн з явищем кібербулінгу борються не тільки коли злочин вже відбувся, але й активно розвивають профілактичні міри щодо його запобіганню;

7 – в разі існування відповідної законодавчої бази, її норми, в рівній мірі стосуються випадків кібербулінгу, як у навчальних закладах, так і на робочому місті (*виробництві*);

8 – законодавчі акти ряду країн передбачають норму, яка спонукає свідків проявів кібербулінгу повідомити про це, так як в іншому випадку вони можуть бути притягнуті до відповідальності [24];

9 – в тих країнах де не існує юридичного визначення явища кібербулінгу, використовують діючі закони, норми яких можуть бути застосовані до даних випадків [25, 32]. Таким чином використовуються окремі правові акти, котрі розглядають склад правопорушень, які містять певні ознаки даних явищ;

10 – норми законів деяких країн вимагають, щоб Інтернет провайдери передавали контактні дані осіб, що здійснюють дії із характерними ознаками Інтернет травлі;

11 – ефективною мірою протидії є деанонімізація користувачів мережевих сервісів. Наприклад, в Китаї є закон, згідно якому люди повинні реєструвати в мережі свої реальні імена, завдяки чому вони стають більш відповідальні за свої слова і дії у мережі;

12 – ефективною технічною мірою протидії кібербулінгу є допуск неповнолітніх в Інтернет тільки при наявності на їх гаджетах встановлених програмних фільтрів (*наприклад, в Японії де діє Закон «Про підтримку здорового Інтернет-середовища для молоді»*).

Таким чином, закони, які спрямовані на протидію кібербулінгу, є відносно новими і тому не дуже поширені у світі. Через це в більшості країн, при визначенні заходів покарання для особи, яка причасна до кібербулінгу, використовують норми інших законів. При цьому певною проблемою є те, що та невелика кількість законів, які все ж таки приймаються, націлені на протидію кібербулінгу переважно серед неповнолітніх. Це породжує певний правовий дисбаланс, так як це явище охоплює всі вікові, соціальні та етнічні групи.

4. Технології і засоби протидії кібербулінгу

Станом на сьогоднішній день, практично існують три основні шляхи протидії проявам кібербулінгу: 1 – соціальний; 2 – законодавчій; 3 – технічний. У попередньому пункті були розглянуті законодавчі аспекти протидії кібербулінгу, в межах цієї частини основна увага буде приділена технічній стороні питання що розглядається.

Слід підкреслити, що, як і у випадку законодавчих ініціатив, цьому напряму, також, приділялося недостатньо уваги. Однак на сьогодні, із-за значного поширення цього явища, почалася інтенсифікація робіт і за технічним напрямком. Вдалим прикладом цього може бути нідерландська розробка *Friendly ATTAC* [38], яка спеціально націлена на поведінку свідків кібербулінгу. Базисом цього рішення є ствердження, згідно якого соціально вірна реакція свідків даного різновиду злочину, може зменшити масштаб цькування і завдану ним шкоду.

На даний час відомо багато різних технологій захисту даних та забезпечення конфіденційності роботи користувачів в мережі [13, 39-40], але не всі вони підходять для захисту від кібербулінгу. Як вже згадувалося раніше, наразі немає вузькоспеціалізованих програмно-апаратних рішень для ефективного захисту від цієї загрози. Тому розглянемо деякі види технологій мережевого захисту, які у той чи іншій мірі можуть бути корисними у боротьбі з цькуванням у мережі.

Для протистояння булінгу в Інтернет використовують технології захисту на основі певних обмежень. Їх головна мета полягає у тому, щоб локалізувати різноманітний небажаний контент (*з точки зору існування ознак кібербулінгу*). В цьому сенсі слід виділити наступні техно-

логії [41]: – аналіз контенту та поведінки; – фільтрація; – моніторинг; – блокування небажаних користувачів (*контактів*); – звітність; – перевірка віку/особистості (*в якоїсь мірі повноважень*); – освітні технології. Аналіз специфіки роботи цих технологій дозволяє виділити один спільний недолік, а саме: - їх використання сприяє порушенню конфіденційності учасників процесу комунікацій. В цьому контексті слід зауважити, що обмежувальні технології можуть порушувати право людини на свободу інформації та вираження особистої думки.

Перед тим як розглянути деякі із існуючих засобів протидії проявам кібербулінгу, систематизуємо бажані характеристики [42], які повинні забезпечувати відповідні технології захисту (Табл. 1).

Таблиця 1 – Бажані характеристики технологій протидії

№	Характеристика	Пояснення
1	**Універсальність**	Технологія повинна враховувати існуючи види мережевої травлі, середовища поширення і методи, за допомогою яких це відбувається.
2	**Безперервність**	Технологія потрібна забезпечити цілодобовий захист у реальному часі.
3	**Добровільність** * * - *в сенсі її використання користувачем.*	Захист повинен грунтуватися на добровільному бажанні користувачів використовувати ці технології (*засоби*). Якщо жертви *(можливо і свідки*) мотивовані використовувати захист, то агресор ніколи не буде брати участь в цьому добровільно, тому що булінг це виключно навмисний акт.
4	**Конфіденційність**	Технологія не повинна порушувати конфіденційність людини (*або мати чітко декларовані обмеження*).
5	**Транспарентність** ** ** - *Свобода волевиявлення.*	Кожна людина має право на свободу самовираження, тому технологія повинна забезпечувати (*не порушувати*) баланс інтересів між правами кожної окремої особистості (*користувача комунікаційної платформи*) та прийнятими нормами суспільної моралі.

Варто зауважити, що такі характеристики, як «Конфіденційність» та «Транспарентність», в кожному окремому випадку, є достатньо дискусійними і, як наслідок, складно формалізуються (*з точки зору синтезу відповідних алгоритмів роботи системи захисту*). В цьому випадку особисте життя людини та її право на свободу вираження повинні бути ретельно збалансовані з потенційними перевагами технології для захисту від кібербулінгу.

4.1 Огляд технологій протистояння кібербулінгу

Коротко розглянемо основні з існуючих технологій Інтернет-безпеки та визначимо особливості їх застосування для боротьбі з кібербулінгом [42].

Аналіз контенту та поведінки. Аналіз контенту та поведінки практично зводиться до процедур автоматичного вилучення індикативної інформації з будь-яких типів даних. Теоретично, ця технологія може бути вдало використана для виявлення кібербулінгу. Проте, деякі результати схожих задач показують, що автоматично дуже складно розпізнати різні види травлі в різних видах контенту (*складність формалізації прийняття рішення та висока обчислювальна складність морфологічного аналізу контенту*). Так наприклад, *Pendar N.* статистично дослідив здатність автоматично розпізнати сексуальні домагання у повідомленнях, де показники доходили до 95 % випадків [43]. Проте, по-перше, набори даних що використовувались у експерименті були невеликими (*701 розмова*). По-друге, у розмовах, які використовувались для дослідження було зрозуміло, що людина хоче причинити шкоду (*зазвичай, таке трапляється не часто*). Тому, перед тим як цей метод можливо буде використовувати в якості практичного захисту від кібербулінгу, його треба ще значно удосконалити.

Технологія аналізу контенту та поведінки працює у реальному часі, і може бути застосована як добровільно, так і ні. Оскільки для аналізу мережевого контенту потрібно зберігати та інтерпретувати дані про поведінку всіх учасників комунікацій (*що може бути розцінено як обробка особистих даних*), то конфіденційність цих користувачів, потенційно, може постраждати. Хоча виявлення неналежних даних і не обмежує свободу вираження, однак дії, які приймаються після цього, можуть. Наразі, у численних програмних рішеннях, так званого «батьківського контролю» використовуються деякі види аналізу Інтернет-ризиків (*наприклад: - контентні, комунікаційні, споживчі та електронні ризики*) [44-45].

Фільтрація. Програмне забезпечення (ПЗ) для Web-фільтрації блокує доступ к Web-ресурсам з небажаним контентом. Методи фільтрації включають в себе «дозволені списки» (*списики Web-сайтів, які дозволено відвідувати*), «заборонені списки» (*списики ресурсів, доступ до яких заблоковано*) та аналіз контенту (*відповідний алгоритм, що приймає рішення, наприклад, на основі появи певних ключових слів і т.і.*). У всіх ПЗ даного типу є два спільних недоліки: – це недостатнє блокування (*неможливість заблокувати деякі ресурси з небажаним контентом*), та надмірне блокування (*помилкове блокування*).

В цілому фільтрація – це більше профілактична міра. І хоча вона не була призначена спеціально для комунікації, фільтрація вхідного та/або вихідного трафіку може відчутно обмежити чи, навпаки, запобігти шкідливому контакту між учасниками кожної окремої комунікації. Проте, як вже було зазначено вище, розпізнавання кібербулінгу на основі комунікації чи контенту, з технічної точки зору, досить складно формалізується, і тому потребує залучення досить серйозних ресурсів (*фінансових, технічних, людських і т. і.*). Ще одним недоліком ПЗ даного типу є те, що фільтрацію можливо обійти. Наприклад, можна замінити початкові терміни, що є заблокованими, на інші, які так само будуть ображати (*наприклад, англійське слово «loser» стає «l o s e r», «LOS3R», «looser» і т.п.*).

Фільтруюча технологія працює у реальному часі, та в переважній більшості випадків, не передбачає зберігання персональних даних користувача, тому не загрожує його конфіденційності. Однак вона не є добровільною, так як користувачі, часто не мають можливість здійснення свого вибору, стосовно наступної фільтрації контенту. Також, блокування комунікації (*фільтрація*) чи запобігання доступу к Web-сайтам, потенційно, може обмежувати параметри обміну інформації та, як слідство, вираження думки.

Моніторинг. Дана технологія є більш профілактичною і працює на основі припущення, що користувачі комунікації будуть контролювати свою поведінку, якщо вони знають, що за їх он-лайн активністю хтось або щось слідкує. ПЗ що реалізує дану технологію, теоретично, підходить для всіх типів, середовищ і методів кібербулінгу. Проте на практиці, інциденти, які пов’язані з мережевою травлею, потрібно буде шукати буквально у ручному режимі. Враховуючи, що кібербулінг у багатьох випадках тяжко розпізнати, то з великою часткою впевненості можна стверджувати, що це є дуже ресурсномістка та втомлива робота. Як свідчить відомий досвід ПЗ для моніторингу не є добровільним, тому користувачі зазвичай не знають і не помічають що їх контролюють. Активність реєструються в режимі реального часу, проте, якісь зворотні дії можуть бути зроблені тільки після того, як відповідні записи пройшли аудит експертною стороною (*наприклад, батьками, в разі використання ПЗ типу «батьківській контроль»*). Технологія моніторингу порушує конфіденційність, тому що вся онлайн активність, яка може розглядатись, як особисті данні, фіксується та зберігається для її подальшого аналізу. Свобода слова не зачіпається.

Більша частина програмних рішень для моніторингу трафіку працює в режимі реального часу та не вносить будь-яких затримок у процес комунікацій (*працює в фоновому режимі*).

Блокування небажаних користувачів (контактів). Більшість сучасних додатків обміну миттєвими повідомленнями та соціальних мереж надають користувачам можливість заблокувати інших користувачів, щоб виключити небажаний контакт. Також, соціальні мережі надають можливість заборонити невідомим користувачам зв’язуватись з власником акаунту і отримувати доступ до його профілю. В цьому разі, блокування трапляється у відповідь на минулі інциденти та обмежує шкідливу комунікацію між людьми. Однак, на жаль, ця техно-

логія можлива поки тільки у соціальних мережах і месенджерах. Блокування – це добровольчий акт, який допомагає користувачам контролювати *(в певній мірі суб'єктивно)* своє віртуальне спілкування. Вони можуть блокувати агресорів у будь-який момент, тому ця технологія працює у реальному часі. В даному випадку, блокування ніяк не пов'язане з конфіденційністю користувача, і таким чином практично не обмежує свободу його самовираження.

Звітність. Багато існуючих соціальних мереж надають можливість повідомляти про неприємний та незаконний контент (*наприклад, застосувавши функцію «повідомити про порушення»*). Ці донесення, зазвичай, відправляються модераторам платформи, які особисто його переглянуть, і вирішать, варто реагувати на скаргу, чи ні. В даному випадку, принциповим питанням стає дотримання вимог професійної етики, з боку модераторів (*цензорів*), тому що вони отримують доступ до "чутливого" персоніфікованого контенту користувачів. Деякі соціальні мережі, чати, онлайн ігри та форуми також надають можливість повідомити про дії користувача, який, на думку жертви, займається кібербулінгом. В цьому разі модератори також вирішують, як слід поступити з цим користувачем. Нажаль, даний вид захисту можливий тільки якщо є можливість залучення системного цензору, тому він не є універсальним.

Так як всі користувачі комунікаційної платформи можуть повідомляти про небажаний контент, ця технологія є добровільною. Але, вона не працює у реальному часі, тому що модератори перевіряють звіти особисто, а на це потрібен певний час. Конфіденційність не страждає, тому що особисті дані не зберігаються у звітах (*принаймні це не задекларовано*).

Перевірка віку/особистості. Перевірки віку та/чи особистості націлені на обмеження небажаних контактів неповнолітніх зі сторонніми дорослими, а також запобіганню доступу неповнолітніх до небажаного контенту. Ця технологія є профілактичною. Перевірка віку та/чи особистості може використовувати публічні та закриті бази даних (БД), які містять інформацію, як про неповнолітніх (*шкільні записи*), так і про дорослих (*наприклад, людей, які здійснили зґвалтування*). Особам які є у цих БД, або користувачам певного віку дозволяється, або навпаки не дозволяється підтримувати зв'язок з деякими іншими групами користувачів.

Дана технологія не є універсальною, тому що вона не націлена на різні форми кібербулінгу. Перевірка віку/особистості може бути як добровільною (*наприклад, при проходженні реєстрації*), так і не добровільною (*наприклад, якщо шкільний сайт дозволяє доступ тільки учням цієї школи*). Технологія працює у реальному часі. Оскільки перевірка віку/особистості потребує збору і зберігання особистих даних, то конфіденційність може бути під загрозою.

Освітні технології. Освіта є ще однім, опосередкованим, засобом підвищення мережевої безпеки для неповнолітніх. Освітні технології для боротьби з кібербулінгом – це, здебільшого, різноманітні інтерактивні комп'ютерні ігри та програми, які навчають дітей безпеці в мережі, та їх правильній поведінці у випадках кібербулінгу. Наприклад, «*FearNot!*» – це інтелектуальне віртуальне середовище (*Intelligent Virtual Environment - IVE*) в 3D, де вигадані персонажі розігрують сценарії булінгу. Даний додаток було розроблено для дітей 8-12 років, щоб вони могли спостерігати за подіями з позиції третьої особи. *IVE* пропонує дітям безпечне середовище, яка підтримує соціальне та емоційне навчання. Контрольні дослідження, які були проведені у Німеччині і Великобританії [46], встановили короткочасний ефект запобігання булінгу для жертв у Великобританії.

Оскільки основною метою освітніх технологій є стимулювання правильної поведінки у підлітків, в цілому вони призначені для усіх типів і методів кібербулінгу. Освітні програми зазвичай є обов'язковими, тому це не є добровільною технологією. Здебільшого вони призначені для формування правильної поведінки, тому вони не захищають безпосередньо від проявів кібербулінгу. Також, ці технології не порушують конфіденційність дитини.

Головна проблема, яка пов'язана з використанням освітніх технологій, полягає у їх обмеженій ефективності. У 2010 році *Faye Mishna* та інші [47] провели дослідження, у ході якого зробили огляд трьох освітніх програм. У кінці дослідження вони прийшли до висновку, що участь у цих програмах дає покращення знань про безпеку в Інтернеті, проте зміна поведінки в мережі учасників програми була не суттєва. Тобто, більші знання про безпечне використання Інтернету не обов'язково корелює з меншим онлайн ризиком.

Узагальнені результати основних можливостей існуючих технологій захисту від кібербулінгу наведені у Табл.1-2. Слід підкреслити, що всі технології, які розглядалися, відповідають відразу декільком з приведених в Табл. 2 характеристикам. При цьому, більшість з розглянутих технологій (*перевірка віку/особистості, фільтрація, моніторинг, звітування та блокування небажаних контактів*) не створювались спеціально для захисту від кібербулінгу, та добре захищають від інших загроз [1]. В першу чергу вони призначені для блокування доступу до небажаного контенту, тому їх успіх, в плані захисту від кібербулінгу (*котрий в більшій мірі пов'язано зі спілкуванням*) є досить обмежений.

Таблиця 2 – Результати аналізу різних технологій

Технологія	**Оцінюваний параметр**				
	Універсальність	Безперервність	Добровільність	Конфіденційність	Транспарентність
Аналіз контенту / поведінки	+/-	+	–	+/-	+
Фільтрація	+/-	+	–	+	–
Моніторинг	+/-	–	–	–	+
Блокування контактів	–	+	+	+	+
Звітність	–	–	+	+	–
Перевірка віку та/або особистості	–	+	+/-	–	+
Освітні технології	+	–	–	+	+

Згідно аналізу характеристик, що були визначені у Табл. 1, та враховуючи специфіку питань, які розглядаються, найбільш відповідною технологією слід вважати блокування небажаних контактів. В цілому можна стверджувати, що у більшості існуючих технологій мережевої безпеки, які в певній мірі адаптовані до умов боротьби з кібербулінгом, є одна спільна особливість: - вони всі намагаються керувати поведінкою користувачів, так чи інакше обмежуючи її! Таким чином, станом на сьогоднішній день, обмеження потенційних агресорів та/або жертв є ефективним напрямом протидії, але навчити їх справлятись саме з інцидентами кібербулінгу, було би значно більш кращим результатом. Проте, поки це лише у перспективі. На практиці ж (*як це вже було зазначено вище*), освітні технології, що застосовують такий метод, слід вважати малоефективними.

4.1.1 Комплексування технологій

Показовим прикладом поліпшення рівня захисту від кібербулінгу, є шлях інтеграції декількох різних технологій в межах одного рішення. Вдалим прикладом відповідного ПЗ можна вважати функцію «батьківський контроль», котра може бути реалізована, як на рівні окремого модулю в складі комплексного рішення ІБ (*наприклад, в рішеннях класу Internet Security*), так і у вигляді самостійного спеціалізованого ПЗ [44-45, 48].

Батьківський контроль – це комплексний продукт, який не залежно від типу кінцевого пристрою, одночасно використовує технології моніторингу, фільтрації (*в т.ч. із застосуванням SaaS - Software as a Service*) і аналізу контенту та/або поведінки кінцевого користувача. Традиційно, функції батьківського контролю реалізуються за рахунок застосування 2-х видів контролю: - пасивного і активного [48]. Пасивні методи реалізують наступні функції:

- Обмеження на запуск деяких програм;
- Обмеження на час використання пристрою;
- Обмеження на час використання якоїсь програми;
- Обмеження на відвідування певних Web-ресурсів (*за різними критеріями*).

До активних методів відносяться:

- Відстеження місцезнаходження;
- Перегляд контактів, повідомлень, завантажувань, історії дзвінків;
- Відстеження переглянутого відео/аудіо контенту.

На думку фахівців та Інтернет користувачів, станом на 2019 рік, перелік п'яти найкращих модулів «батьківській контроль» виглядає наступним чином [49]: – *Avira* (Німеччина); – *Blue Coat* (США); – *DrWeb* (Росія); – *BitDefender* (Румунія); – *ContentKeeper* (Австралія).

4.2 Кібербулінг і соціальні мережі

На рис. 4 представлена статистична інформація, яка надана *Ditch the Label*, однією з провідних організацій проти знущань. Ці відомості відображають дані опитування студентів, стосовно платформ, на яких вони зазнали кібербулінг.

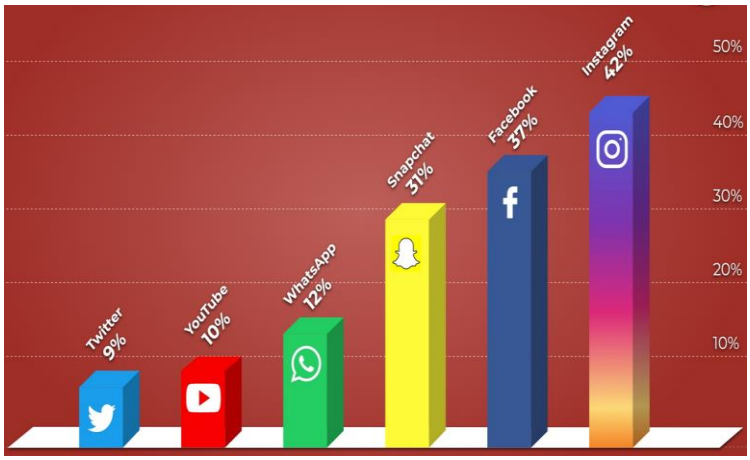

Рис. 4 – Дані щодо кібербулінгу соцмережах

Згідно цих даних, найбільш за все кібербулінгу піддавались користувачі соціальних мереж *Instagram, Facebook* та *Snapchat*. Ці комунікаційні платформи щодня налічують мільйони користувачів і тому проявляють очевидну зацікавленість в ефективній протидії кібербулінгу.

Facebook. На сьогодні є найкрупнішою соціальною мережею у світі. Число користувачів, які регулярно (*не менше ніж 1 раз на місяць*) використовують цей ресурс, складає порядку 2,5 мільярди чоловік. Дана платформ активно бореться з різноманітними проявами кібербулінгу. Фахівці цієї мережі поєднали одразу три технології: - блокування контактів (*можливість заблокувати небажаного користувача*); - звітування (*користувач може повідомити про небажаний контент*); - та освітні технології (*«Центр захисту від травлі»*).

У 2013 році *Facebook* запустив свій спеціальний проект «Центр захисту від травлі» [50], котрий позиціонується, як ресурс для підлітків, батьків і викладачів, що потребують підтримки та допомоги з питань, які пов'язані зі знущаннями та іншими конфліктами в мережі. У 2017 році було реалізовано декілька нових додаткових функцій, котрі можуть допомогти попередити булінг та переслідування [51]. Також соціальна мережа у подальшому планує надати своїм користувачам можливість повідомляти про булінг чи переслідування від імені іншого користувача. А наразі тестується ще одна функція, за допомогою якої користувач зможе блокувати появу певних слів в своїх коментарях [52].

Instagram. *Instagram* (*власник Facebook*) позиціонує себе, як соціальна мережа для обміну медіа-контентом (*Media sharing networks*). Нажаль, але ця платформа наразі є найпопулярнішою для кібербулінгу. У *Instagram*, так само як і у *Facebook*, присутні технології блокування

контактів та звітування. Тобто, користувачі даної мережі можуть подати скаргу на небажаний коментар та обліковий запис, чи заблокувати його. Також, є можливість зробити свій профіль «закритим» (*тільки для «своїх» підписантів*).

З 2019 року компанія почала вводити нову функцію [53], яка повідомляє користувачів, коли їх коментар до фото чи відео контенту «вважається як образливий». Керівництво мережі повідомило, що вони впроваджують елементи штучного інтелекту (ШІ), котрий може розпізнавати різні види булінгу в рамках їх платформи. Так, перед тим, як небажаний коментар буде опубліковано алгоритм ШІ повідомить відправника про потенційну небезпеку його коментарів. Представники *Instagram* вважають, що такий підхід змусить користувачів ресурсу замислитись стосовно змісту особистих коментарів. Також, проходить апробацію функція «тіньового бану», яка дозволяє користувачам мережі робити коментарі кривдника прихованими для всіх інших користувачів платформи, крім нього самого.

Twitter. *Twitter* позиціонується, як соціальна мережа для авторських записів. Наразі, це є найпопулярнішим сервісом мікро-блогів у світі. І хоча *Twitter* знаходиться не на 1-му місті по розповсюдженості кібербулінгу (*лише 9% студентів відповіли, що зустрічались з булінгом на цій платформі*), ця компанія теж активно бореться за безпеку своїх користувачів [54]. Наразі можна виділити 7 способів, за допомогою яких фахівці компанії протидіють кібербулінгу на їх платформі:

1. Розширена фільтрація повідомлень. Користувачі можуть використовувати цей інструмент для багатофакторної фільтрації облікових записів, від яких вони можуть приймати повідомлення. Ця функція призначена для недопущення зловживань з неперевірених облікових записів чи певних користувачів, які мають статус «небажаних»;
2. Розширення способів вимкнути контент. Розширені можливості функції вимкнення повідомлень: - користувачі мають можливість приховати відображення ключових слів чи цілих фраз, та управляти часом блокування відображення небажаних повідомлень. Таким чином, користувач може налаштувати контент, якій він бажає бачити у повідомленнях;
3. Прозорість процедури звітування. Фахівці мережі забезпечили більшу прозорість опрацювання скарг про виявлені зловживання, в наслідок чого користувачі отримують службові повідомлення, стосовно дій, які приймає *Twitter* на їх скаргу щодо булінгу;
4. «Тайм-аут» *(тимчасова перерва активності)*. Якщо твіти (*текстові записи*) користувачів помічені, як образливі, або ті, що іншим чином порушують системні Правила, то активність профілю тимчасово скривається. Таким чином інші користувачі не матимуть змогу переглядати записи цього профілю;
5. Безпечні результати пошуку. Алгоритми ШІ фільтрують результати пошуку, щоб користувачі не отримували контент з облікових записів, які були «вимкнено» (*за скаргою*). Однак, ці дані все ще будуть зберігатися, тому, якщо користувач справді шукає саме їх, то він повинен знайти саме цей контент. Але в цьому разі він/контент не буде відображатись у якості основного результату пошуку;
6. Руйнування образливих записів. Алгоритми ШІ приховують записи, які визначені образливими, чи порушують правила мережевої спільноти. Користувач може переглянути дані твіти, але тільки якщо «зайде» безпосередньо у профіль автора запису;
7. Блокування створення нових образливих профілів. Алгоритми ШІ запобігають створенню нових облікових записів, якщо інші профілі користувача вже були позначені системою, як «образливі». Це унеможливлює створення і наступне використання фальшивих профілів для розсилки спаму, переслідування чи булінгу інших користувачів. Поведінковий алгоритм в межах платформи сканує декілька облікових записів-клонів з однаковими реквізитами, та визначає присутність можливих шахраїв та кривдників.

Узагальнюючи все вище зазначене, можна зробити висновок, що практично усі розглянуті технології протидії кібербулінгу відповідають хоча б одному з визначених критеріїв, однак жодна з них, поки, не відповідає більшості бажаних характеристик (*не кажучи вже про всі*). Скоріш за все це обумовлено тим, що станом на сьогоднішній день майже не існує техноло-

гій, які б були розроблені спеціально задля протидії саме кібербулінгу (*окрім освітніх технологій, хоча і вони є спірними*). Тому, їх ефективність у боротьбі з Інтернет-травлею дуже обмежена. В цьому сенсі, дещо ліпші показники мають програмні рішення класу «батьківський контроль». Вони інтегрують у собі декілька технологій захисту та мають більш таргетований функціонал, завдяки чому забезпечують і більш адекватний рівень парирування спроб проведення кібербулінгу.

5 Висновки

Хоча розвиток ІТ- технологій і несе сучасному суспільству багато корисних новацій, він теж, нажаль, має свої, приховані від необізнаних користувачів, негативні наслідки. У нашому випадку, однією з таких негативних сторін, є проблема булінгу, котра в наслідок масштабної інформатизації суспільства, «перейшла» у віртуальне середовище, та відкрила нову, «темну», сторінку в технологічної історії людства – сторінку кібербулінгу. Мета даної роботи полягала в дослідженні явища кібербулінгу, його основних видів, способів реалізації, характеристик та можливостей протистояння його проявам [55]. За результатами аналізу питань за даною проблематикою, можна стверджувати наступне:

1. Хоча явище булінгу досліджується вже декілька десятиліть, однак в його кіберваріації воно ще залишається дуже не вивченим. Так, поки все ще немає чіткого поділу на різні види кібербулінгу, за рахунок чого, кожен дослідник приводить своє бачення цього питання;

2. У плані вироблення консолідованої позиції в протистоянні кібербулінгу, принциповим є той факт, що не у кожній країні світу ведеться офіційна статистика, стосовно масштабів цього явища та його жертв (*наслідків*). А якщо вона і є, то частіше за все, акцент робиться на кібербулінгу у підлітковому середовищі. Однак, як це було підкреслено у роботі, в сучасному світі кібербулінг може стосуватися кожного, і це не залежить від віку, статі, соціального статусу та багатьох інших чинників;

3. За результатами огляду законодавчої бази різних країн, зроблено висновок, про існування гострої нестачі відповідних законів. Наразі, навіть провідні країни світу не мають розвиненої законодавчої бази стосовно протидії Інтернет-травлі;

4. Визначено, що в Україні є закон який регулює булінг (*і кібербулінг зокрема*), але він націлений тільки на учасників навчального процесу;

5. У більшості існуючих технологій мережевого захисту, які так чи інакше адаптовані до умов протидії кібербулінгу, є одна спільна особливість: - вони всі намагаються обмежувати поведінку користувачів. Таким чином, станом на сьогоднішній день, обмеження потенційних агресорів та/або жертв є найбільш ефективним напрямом протидії кібербулінгу;

6. В роботі систематизовано критерії, яким повинна відповідати сучасна технологія протидії кібербулінгу, та представлені приклади вдалої реалізації захисту користувачів у деяких найбільш популярних соціальних мережах. Підкреслено, що наразі є велика нестача спеціальних технологій для ефективної протидії проявам кібербулінгу;

7. Станом на сьогоднішній день, явище кібербулінгу є дуже недооціненим і тому являє собою серйозну проблему. З великою часткою впевненості можна стверджувати, що в подальшому кібербулінг буде тільки поширюватись, адже з кожним роком все більше людей стають активними користувачами все нових мережевих сервісів та онлайн послуг;

8. Для ефективної протидій проявам кібербулінгу потрібно застосовувати виключно комплексний підхід, тобто впроваджувати відповідні заходи в межах всіх зазначених у роботі шляхів протидії: - соціального, законодавчого та технологічного. В межах реалізації кожного з цих заходів, потрібно періодично проводити різноманітні освітні заходи, які будуть інформувати суспільство про особливості проявів цього явища;

9. Ефективним засобом захисту дітей і підлітків від негативного впливу мережевих загроз і проявів кібербулінгу, є захисне ПЗ класу «батьківський контроль». Установка таких рішень на пристрої, якими безпосередньо користуються діти, за умови постійної уваги до змісту log-файлів і коригування налаштувань даних програм, робить цей засіб досить ефективним в протистоянні кібербулінгу.

Однак, незважаючи на всі можливості існуючих технологій батьківського контролю, одних лише програмних засобів явно недостатньо, тому що навіть найпередовіші технічні рішення не замінять довірливої розмови з «близькою» людиною. Як наслідок, не варто нехтувати регулярними бесідами з підлітками і дітьми про правила поведінки в Інтернеті та основні різновиди онлайн загроз. Вже сам факт існування такої бесіди, підтверджує те, що і батьки і діти об'єктивно оцінюють загрози сучасного віртуального світу та готові протистояти потенційним викликам сучасності;

10. Потужним інструментом для подальшого вдосконалення процедури рецензування «спірних» записів користувачів в соціальних мережах, може послужити практика використання фахівцями комунікаційних майданчиків додаткових технічних параметрів, видобутих з пристроїв користувачів (*наприклад, параметри геолокації, поведінковий профіль користувачів, аналіз структури сузір'я контактів, репутаційний рейтинг та ін.*);

11. Основою технологічного фундаменту майбутніх захисних рішень, що протидіють проявам кібербулінгу можуть виступати останні напрацювання в сферах штучного інтелекту, синтезу поведінкових алгоритмів та удосконалення технологій хмарних обчислень.

Посилання

[1] Маллери Д. Безопасная сеть вашей компании. Защита и администрирование / Пер. с англ. Е. Линдеман. – М.: НТ Пресс, 2007. – 640 с.

[2] What is cyberbullying? // nuedusec. URL: https://nuedusec.com/blog/cyberbullying/, 11.02.2020

[3] Цькування. // wikipedia. URL: https://uk.wikipedia.org/wiki/%D0%A6%D1%8C%D0%BA%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F, 11.02.2020

[4] Hyojin Koo. A time line of the evolution of school bullying in differing social contexts. // Asia Pacific Education Review Copyright 2007 by Education Research Institute 2007, Vol. 8, No. 1, 107-116 URL: https://files.eric.ed.gov/fulltext/EJ768971.pdf, 15.02.2020

[5] History of bullying. // blogspot. URL: http://bullying190.blogspot.com/2012/10/history-of-bullying.html, 15.02.2020

[6] What is bullying? // humanrights. URL: https://humanrights.gov.au/our-work/commission-general/what-bullying-violence-harassment-and-bullying-fact-sheet, 15.02.2020

[7] Columbine Shooting. // history. URL: https://www.history.com/topics/1990s/columbine-high-school-shootings, 21.02.2020

[8] Cyberbullying: An Emerging Threat to the “Always On” Generation // billbelsey. URL: http://www.billbelsey.com/?cat=13, 21.02.2020

[9] А.И. Маренцова. Запугивание и издевательство в сети. Феномен: CYBERBULLYING. Москва, 2015, сс. 16-20.

[10] A. Cooper. Sexuality and the Internet Surfing into the New Millennium. Cyber Psychology and Behavior, Vol. 1, No. 2, 1998, pp. 181-187.

[11] Donegan R. Bullying and Cyberbullying: history, statistics, law, prevention and analysis. – The Elon Journal of Undergraduate Research in Communications, 2012.

[12] Григорьев В.А., Лагутенко О.И., Распаев Ю.А. Сети и системы радиодоступа. – М.: Эко-Трендз, 2005. – 384 с.

[13] Шахнович И.В. Современные технологии беспроводной связи. Издание второе, исправленное и дополненное. - М.: Техносфера, 2006. – 288с.

[14] Hyperpersonal model. // wikipedia. URL: https://en.wikipedia.org/wiki/Hyperpersonal_model, 02.03.2020

[15] Maral Dadvar. EXPERTS AND MACHINES UNITED AGAINST CYBERBULLYING, 2014, pp. 23-25

[16] Mary Howlett-Brandon. CYBERBULLYING: AN EXAMINATION OF GENDER, RACE, ETHNICITY, AND ENVIRONMENTAL FACTORS FROM THE ETHNICITY, AND ENVIRONMENTAL FACTORS FROM THE NATIONAL CRIME VICTIMIZATION SURVEY: STUDENT CRIME NATIONAL CRIME VICTIMIZATION SURVEY: STUDENT CRIME SUPPLEMENT, 2009, p. 8. URL: https://scholarscompass.vcu.edu/cgi/viewcontent.cgi?article=4485&context=etd, 02.03.2020

[17] Грифер. // wikipedia. URL: https://ru.wikipedia.org/wiki/%D0%93%D1%80%D0%B8%D1%84%D0%B5%D1%80, 09.03.2020

[18] Солдатова Г. У., Ярмина А. Н. Кибербуллинг: особенности, ролевая структура, детско-родительские отношения и стратегии совладания, 2019, № 3(35). С. 17–31.

[19] Что значит интернет-тролль, как его отличить? // fb. URL: https://fb.ru/article/245287/chto-znachit-internet-troll-kak-ego-otlichit-kak-zarabatyivayut-trolli-v-internete-kak-vesti-sebya-s-trollyami-v-internete-kak-borotsya-s-trollyami-v-internete, 11.03.2020

[20] 51 Critical Cyberbullying Statistics In 2020. // broadband. URL: https://www.broadbandsearch.net/blog/cyber-bullying-statistics, 20.03.2020

[21] 11 FACTS ABOUT CYBERBULLYING // dosomething. URL: https://www.dosomething.org/us/facts/11-facts-about-cyber-bullying, 16.03.2020

[22] Булінг та кібербулінг у підлітковому середовиші // unicef. URL: https://www.unicef.org/ukraine/bullying-cyberbylling-teens-Ukraine, 20.03.2020

[23] Cyberbullying Laws. // criminal.findlaw. URL: https://criminal.findlaw.com/criminal-charges/cyber-bullying.html, 30.03.2020

[24] Canada: The New Age Of Cyberbullying. // monaq. URL: https://www.mondaq.com/canada/social-media/727084/the-new-age-of-cyberbullying, 30.03.2020

[25] Proskauer. Bullying, Harassment and Stress in the Workplace — A European Perspective, 2013. URL: https://www.internationallaborlaw.com/files/2013/01/Bullying-Harassment-and-Stress-in-the-workplace-A-European-Perspective.pdf, 04.04.2020

[26] French Law Prohibiting Bullying in the Workplace. // thehrdirector. URL: https://www.thehrdirector.com/business-news/diversity_and_equality/french-law-prohibiting-bullying-in-the-workplace/, 04.04.2020
[27] The Law on Cyberbullying. // localsolicitors. URL: https://www.localsolicitors.com/criminal-guides/the-law-on-cyberbullying, 04.04.2020
[28] Ciberacoso, código penal y leyes al acoso. // ciberintocables. URL: https://ciberintocables.com/ciberacoso-codigo-penal/, 05.04.2020
[29] Уголовный Кодекс Республики Беларусь – Статья 189. Оскорбление // koddeksy-by. URL: https://kodeksy-by.com/ugolovnyj_kodeks_rb/189.htm, 07.04.2020
[30] Ответственность за оскорбление в Интернете. // berestovitsa.grodno-region. URL: http://berestovitsa.grodno-region.by/uploads/files/Otvetstvennost-za-oskorblenie-v-Intnrnete.pdf, 10.04.2020
[31] Валентина Алексеевна Мальцева. Защита детей от кибербуллинга. Вопросы уголовно-правового регулирования. 2019, pp. 95-99. URL: https://cyberleninka.ru/article/n/zaschita-detey-ot-kiberbullinga-voprosy-ugolovno-pravovogo-regulirovaniya, 10.04.2020
[32] Конституція України: Редакція від 01.01.2020
[33] Кодекс України про адміністративні правопорушення: Редакція від 14.05.2020
[34] В 2019 суд рассмотрел 310 дел о буллинге. // osvita. URL: https://ru.osvita.ua/school/69377/, 17.04.2020
[35] Проект Закону про внесення змін до деяких законодавчих актів України щодо протидії мобінгу. // w1.c1.rada. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65602, 17.04.2020
[36] Проект Закону про внесення змін до деяких законодавчих актів України щодо забезпечення захисту педагогічних, науково-педагогічних та наукових працівників. // w1.c1.rada. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=67110, 18.04.2020
[37] A Guide to Worldwide Bullying Laws. // hcalawyers. URL: https://www.hcalawyers.com.au/blog/bullying-laws-around-the-world/, 18.04.2020
[38] Friendly Attac. // friendlyattac. URL: https://www.friendlyattac.be/, 23.04.2020
[39] Телекоммуникационные системы и сети: Учебн. пос. В 3-х т. Т. 3. Мультисервисные сети / В.В. Величко, Е.А. Субботин, В.П. Шувалов, А.Ф. Ярославец / Под ред. В.П. Шувалова. – М.: Горячая линия-Телеком, 2005. – 592 с.
[40] Ріпний О.С., Дьяченко О.О., Гостєв О.Л. Аналіз особливостей організації IDS/IPS систем в сучасних інформаційно-телекомунікаційних системах. // Проблеми інформатизації. VII міжнародна НТК. 13-15 листопада 2019. Том 1: секції 1-3. – Ч.: ЧДТУ. – 2019. – С.119.
[41] Internet Safety Technical Task Force, 2008. URL: http://cyber.law.harvard.edu/pubrelease/isttf/, 23.04.2020
[42] Janneke M. van der Zwaan, Virginia Dignum, Catholijn M. Jonkerand Simone van der Hof. On Technology Against Cyberbullying. Chapter 12, 2014, pp. 217-218, 218-225. URL: http://mmi.tudelft.nl/sites/default/files/zwaan_Technology%20against%20b.chapter%202014.pdf
[43] Pendar N. Toward spotting the pedophile telling victim from predator in text chats. In:ICSC'07: Proceedings of the international conference on semantic computing. IEEEComputer Society, 2007, pp 235–241.
[44] Родительский контроль на новом уровне // URL: https://www.securitylab.ru/analytics/423870.php.html
[45] Светлана Шляхтина. Родительский контроль - дело тонкое. // URL: https://compress.ru/article.aspx?id=23035
[46] Watson S. FearNot! An Anti-Bullying Intervention: Evaluation of an Interactive Virtual Learning Environment. 2007. URL: https://www.researchgate.net/publication/30384409_FearNot_An_Anti-Bullying_Intervention_Evaluation_of_an_Interactive_Virtual_Learning_Environment, 27.04.2020
[47] Faye Mishna, Charlene Cook, Tahany Gadalla, Joanne Daciuk, Steven Solomon, Ajita Deodhar. Cyber bullying behaviors among middle and high school students. Vol. 80, No. 3, 2010, pp. 362-374.
[48] Parental controls. // wikipedia. URL: https://en.wikipedia.org/wiki/Parental_controls, 08.05.2020
[49] Рейтинг - лучшие родительские контроли 2019. // anti-malware. URL: https://www.anti-malware.ru/parental_control_test_history, 08.05.2020
[50] Как бороться с травлей. // facebook. URL: https://www.facebook.com/safety/bullying/, 13.05.2020
[51] Facebook introduces new tools to fight online harassment. // engadget. URL: https://www.engadget.com/2017-12-19-facebook-new-tools-fight-online-harassment.html, 13.05.2020
[52] Facebook bullying: How it happens and what to do about it. // comparitech. URL:https://www.comparitech.com/internet-providers/facebook-bullying/, 13.05.2020
[53] Использование ИИ для борьбы с травлей пользователей в Интсаграм. // androidsider. URL:https://androidinsider.ru/novosti/instagram-budet-ispolzovat-ii-dlya-borby-s-travlej-polzovatelej.html, 15.05.2020
[54] How Twitter Is Fighting Harassment & Cyberbullying. // blog.hubspot. URL:https://blog.hubspot.com/marketing/twitter-harassment-cyberbullying, 20.05.2020
[55] Гайкова В. В. Дослідження явища кібербулінгу і аналіз шляхів протидії його проявам : Пояснювальна записка до дипломної роботи бакалавра: напрям підготовки 125 – Кібербезпека / В. В. Гайкова; Харківський національний університет імені В. Н. Каразіна. – Харків: [Б. В.], 2020. – 64 с.

Рецензент: Владимир Хома, д.т.н., проф., Опольский Политехнический Университет, Ополе, Польша.
E-mail: xoma@wp.pl

Поступила: Март 2020.

Авторы:
Валерия Гайкова, студентка факультета компьютерных наук, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: valeriagaikova98@gmail.com
Сергей Малахов, к.т.н., с.н.с., доцент кафедры, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: mailgate@meta.ua

Исследование явления кибербуллинга и путей противодействия его проявлениям.

Аннотация. В работе исследованы основные характеристики Интернет травли (кибертравли или кибербуллинга). Рассмотрены основные особенности проявлений этого явления. Выполнен анализ существующих видов кибербуллинга и их отдельных характеристик. Рассмотрены примеры законодательных актов различных стран по противодействию кибербуллингу. По результатам обзора имеющейся нормативно-правовой базы разных стран, сделан вывод о существенном дефиците соответствующих норм законов. Подчеркнуто, что в современном мире жертвой Интернет травли может стать любой человек. При этом, риск стать жертвой кибербуллинга практически не зависит от каких-либо факторов (например, финансового положения жертвы, его возраста, пола, социального положения и др.). Отмечено, что коммуникации, которые осуществляются в киберпространстве, предоставляют пользователям возможность заранее и тщательно выбирать информацию о себе, которую они хотят обнародовать. В большинстве случаев это способствует тому, что люди демонстрируют только свои «положительные» стороны (например, при общении в чатах). В результате этого у сетевых собеседников часто возникают ложные взаимные симпатии, в результате чего они опрометчиво вступают в доверительные отношения. Таким образом, происходит идеализация партнера по сетевой коммуникации, и любая его информация начинает восприниматься гораздо чувствительнее, чем при прямом «физическом» общении. Этот эффект с «успехом» используется при проведении акций кибербуллинга, когда один человек сначала вызывает максимальное доверие другого, а потом резко меняет тактику общения, становясь немотивированно вероломным и агрессивным. Подчеркнуто, что явление кибербуллинга является значительно недооцененным и поэтому представляет собой серьезную проблему. Выполнен краткий обзор существующих технологий и средств противодействия этому явлению. Проведено сравнение их эффективности. Систематизированы критерии, которым должна соответствовать современная и эффективная технология противодействия кибербуллингу. Представлены примеры удачной реализации защиты пользователей в некоторых наиболее популярных социальных сетях. Акцентировано внимание на том, что для противодействия кибербуллингу, в настоящее время, в подавляющем большинстве случаев, используют технологии защиты на основе ограничений. Главная цель соответствующих средств защиты заключается в том, чтобы максимально локализовать нежелательный контент (с точки зрения существования признаков кибербуллинга). Сделан вывод, что и в дальнейшем кибербуллинг будет только распространяться. Это обусловлено постоянным увеличением численности пользователей новых сетевых сервисов и онлайн площадок для общения. Высказано мнение, что для активного противодействия и эффективной защиты от кибербуллинга требуется внедрение комплексных организационно-технических мероприятий. В завершении предложена общая оценка дальнейшего развития кибербуллинга и путей совершенствования соответствующих инструментов противодействия.

Ключевые слова: буллинг; кибербуллингу; социальная сеть, информационная безопасность; контент; защита; технология, сетевая безопасность.

Reviewer: Volodymyr Khoma, Dr. of Sciences (Eng.), Full Prof., The Opole University of Technology, Opole, Poland.
E-mail: xoma@wp.pl

Received: March 2020.

Authors:
Valeriia Haikova, CSD Student, V.N. Karazin Kharkiv National University, Ukraine.
E-mail: valeriagaikova98@gmail.com
Serhii Malakhov, Ph.D., Senior Researcher, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: mailgate@meta.ua

Research of the cyberbullying phenomenon and analysis of ways to counter its manifestations.

Annotation. The main characteristics of Internet harassment (*cyberbullying*) are investigated in the research. The main features of this phenomenon are considered. The analysis of existing types of cyberbullying and their individual characteristics is made. The examples of legislative acts of different countries is concluded that there is deficiency of relevant rules of low. It is emphasized that anyone can become a victim of in the modern world. At the same time a risk of becoming a victim of cyberbullying does not depend on any factors (*for example financial position of victim, his or her age, sex, social position etc.).* It is noted that communications that are made in cyberspace provide an opportunity for users to choose information they want to make public carefully and in advance. In most cases it contributes to help people show theirs strengths (*for example, when communicating in chats*). In results there is often false sympathy between network interlocutors and they trust each other. So the idealization of the partner happens and any his or her information is perceived more sensitive than during direct communication. This effect is successfully used during cyberbullying, when first one person inspires the trust of another and then changes communication tactics, becoming faithless and aggressive. It is emphasized that the cyberbullying phenomenon is very underestimated and that`s why it is a serious problem. The brief overview of existing technologies and means of counteracting this phenomenon is made. The comparison of their effectiveness is made. The standards that modern and effective technology of cyberbullying resistance must meet are systematized. There are examples of successful realization of user protection in most popular social network. It is emphasized that for cyberbullying resistance nowadays in most cases the protection technologies of it is to localize undesirable content in terms of the existence of cyberbullying. Based on the results of this research it is confirmed that the cyberbullying will spread further. This is due to the constant increase in the number of users of new network services and online platforms for communication. For effective defense against cyberbullying it is required the introduction of organizational and technical measures. At the end it is proposed the general assessment of further development of cyberbullying and the ways to improve appropriate countermeasures.

Keywords: Bullying; Cyberbullying; Social Network; Informational Security; Content; Protection; Technology; Network Security.