УДК 004.5: 316.472.4 DOI: 10.26565/2519-2310-2021-1-04

АНАЛІЗ ФАКТОРІВ І УМОВ РЕАЛІЗАЦІЇ КІБЕРБУЛІНГУ З УРАХУВАННЯМ МОЖЛИВОСТЕЙ СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

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

Надійшла: Січень 2021.

Анотація: *Представлений перелік основних узагальнень і чинників, які характерні для різних варіантів та умов здійснення акцій мережевий цькування (кібербулінгу). Запропонована аргументація певних аналогій і співпадінь між процесом мережевого цькування та умовами, і цілями проведення сучасних інформаційних операцій. Звернено увагу те, що умови кібертравлі багато в чому збігаються з парадигмою експерименту С. Мілгрема. Запропоновано аргументація суті деяких аналогій між проявами кібербулінгу та основною фабулою експерименту про покору. Підкреслено, що рівень ієрархічної важливості об'єктів кібертравлі, обумовлює ступінь необхідної інтеграції функцій адміністрування контентом і основних складових ресурсного забезпечення сучасних інформаційних систем. Зазначено, що інтеграція в одному центрі прийняття рішень основних складових ресурсного забезпечення та функцій адміністрування контенту, є серйозною проблемою навіть для рівня окремих держав, не кажучи вже про персональний рівень впливу. Звернуто увагу на той факт, що кібербулінг може реалізовуватися, як шляхом використання можливостей окремих інформаційних технологій, так і втілювати концепцію інтегрованої атаки. Підкреслено, що явище кібербулінгу є значно недооціненим і тому являє собою серйозну проблему сучасності.*

Ключові слова*: булінг; кібербулінг; інформаційна повістка; контент; інформаційні технології; технічна платформа; мережева поведінка; мережевий статус; експеримент Мілгрема.*

1 Вступ

Стрімкий розвиток інформаційних технологій (ІТ) привносить в сучасне суспільство багато позитивних та корисних тенденцій, однак, нажаль, він має і свої «темні» сторони, що приховані від непосвячених в реалії існування сучасного цифрового світу. Однією з таких сторін, є явище булінгу, яке в наслідок стрімкого науково-технічного розвитку останніх десятиліть, поступово «перейшло» в кіберпростір, та відкрило нову, неприваблиу сторінку технологічної історії людства – сторінку кібербулінгу [1-3]. Процес протистояння булінгу в кіберпросторі [4-5], обумовлює необхідність постійної розробки нових та вдосконалення вже існуючих технологій і засобів протидії, які спрямовані, в тому числі, на завчасне коригування мережевої поведінки користувачів різних інформаційних систем, та онлайн сервісів [6].

2. Основна частина

Результати всебічного аналізу інцидентів, що пов'язані з різними формами проявів булінгу в кіберпросторі, дозволяє зробити кілька принципових узагальнень:

1 – цькування (або травля) в кіберпросторі має два рівня впливу на обрані об'єкти психологічної атаки : - груповий *(глобальний)* та індивідуальний *(персональний)*;

2 – об'єкти кібертравлі значною мірою збігаються з основними об'єктами впливу/атаки в ході ведення сучасних інформаційних операцій [7];

3 – практично всі випадки кібербулінгу, мають структуру і основні складові, які притаманні для сучасних[1] умов ведення інформаційних операцій [7, 8];

4 – рівень значущості заявленої жертви мережевого булінгу, визначає необхідний обсяг фінансової складової ресурсного забезпечення заходів кібертравлі;

5 – доступність і неперервність використовуваних комунікаційних сервісів і онлайн послуг, що надаються різними інформаційними системами, є визначальним (*критично важливим*) фактором для досягнення кінцевих цілей будь-яких акцій булінгу в кіберпросторі;

6 – характер поведінки і ролі [9] основних учасників процесу кібертравлі, багато в чому ідентичні умовам і цілям проведення експерименту Стенлі Мілгрема (*відомий, як «Експеримент про покору»*) [10-12]. У разі акцій кібертравлі, в незалежності від рівня впливу на обрану жертву та рівня її ієрархічної значущості, ми є свідками процесу масової реінкарнації цього експерименту в умовах існування сучасного інформаційного суспільства [13-14], з відповідною «еволюцією»[2] уявлень учасників цього процесу, про норми соціальної і мережевої поведінки людини[3] в кіберпросторі.

Примітки:

[1] – *мається на увазі, використання можливостей існуючих інформаційних систем (технічних комунікаційних платформ) та IT-технологій;*

[2] – *може і не являтися такою, а бути, лише, похідною поточних комерціалізованих тенденцій, сформульованих домінуючими постачальниками телекомунікаційних послуг і сервісів (наприклад, гігантами IT-індустрії: Twitter, Facebook, YouTube та ін.);*

[3] – *однієї зі сторін процесу може являтися комп'ютеризована система (бот), що реалізує, як наперед задані поведінкові алгоритми, так і підтримувати функції самонавчання (штучного інтелекту). У останньому випадку складно говорити про «соціалізацію» поведінкових алгоритмів боту, зважаючи на значну складність формалізації його поведінкових реакцій.*

Розглянемо запропоновані узагальнення та зробимо деякі пояснення по кожному з них.

1. В рамках зазначених рівнів впливу, в якості заявленої цілі атаки (*тобто жертви кібертравлі*) можуть виступати:

- конкретні фізичні персони (*окремі користувачі будь-яких інформаційних систем і онлайн сервісів, представники бізнес структур, політичних партій і громадських об'єднань, представники ланок державної влади, культових організацій та ін.*);

- мережеві об'єднання груп користувачів в межах існуючих інформаційно-комунікаційних платформ *(учасники соціальних мережевих співтовариств (чати, форуми та ін.) з різними критеріями групоутворення (політичні, культурні, професійні та ін.))*;

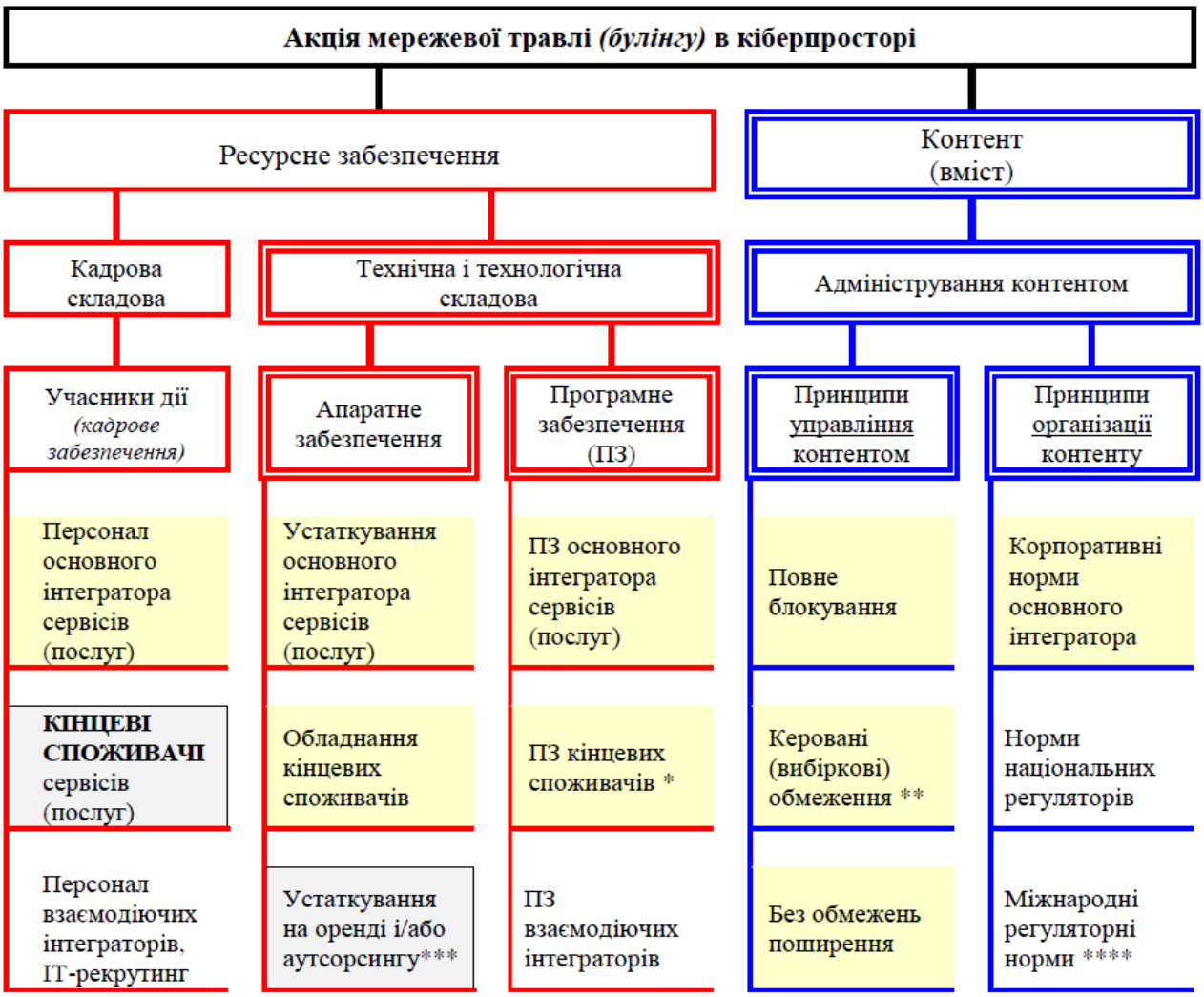
- корпоративний сегмент (*представництва окремих бізнес структур, галузевих об'єднань, медійних холдингів, політичних партій, представництва культових організацій, окремі ланки державного управління та ін.*);

- цивілізаційно-ціннісні основи суспільства (*історико-культурні та релігійні традиції, міжрасові і соціальні норми відносин тощо*).

В наведеному переліку «потенційних жертв» особливого коментарю потребує питання, що стосується співвіднесення ієрархічної значущості об'єктів атаки при реалізації акцій булінгу, стосовно існуючих цивілізаційно-ціннісних основ суспільства. З огляду на очевидний суспільний резонанс від спроб проведення заходів подібного характеру, рівень представництва основних учасників відповідних атак, вимагає високого ступеня їх повноважень (*протегування*). Характерним прикладом акцій подібного рівня значущості, може слугувати епізод, що пов'язаний з трагічними подіями 2015 року в редакції щотижневика *Charlie Hebdo* [15].

2. Рівень важливості (*ієрархічної значущості*) об'єктів, обраних для кібертравлі, зумовлює ступінь необхідної інтеграції (*об'єднання*) ***функцій управління*** контентом та основних складових ресурсного забезпечення (рис. 1) використовуваних інформаційних систем. При цьому, реалізація акцій мережевої травлі проти об'єктів з високим рівнем ієрархічної значущості, на відміну від атак цілей з низькою ієрархічної важливістю, потребує безумовного об'єднання в одному центрі прийняття рішень функцій адміністрування контентом та технічного забезпечення (*подвійний контур на рис. 1*). Характерним прикладом подій відповідного ієрархічного рівня може слугувати епізод політичної кризи в Венесуелі у 2019 році [16].

Можна стверджувати, що відсутність у представників атакуючої сторони (*перш за все рольових груп «агресор» та «помічник агресора»* [9]) функцій управління та контролю використовуваних інформаційно-комунікаційних платформ (рис. 2), обумовлює локальний характер для будь-яких заходів кібертравлі проти жертв з низькими рівнями їх ієрархічної значущості (*наприклад, випадки підліткової цькування на ґрунті боротьби за домінування в своїх мікрогрупах*).



* - *додатки користувачів, програмна «прошивка» мобільних гаджетів, комунікаційних терміналів і мультимедійних пристроїв;*

** - *за часом, геолокацією, мовою і/або каналами видачі контенту, пошуковими запитами, типом і/або швидкістю трафіку та ін.;*

*** - *тимчасові посередники телекомунікаційних послуг, IT-аутсорсинг, хостинг, оренда додаткових апаратних і/або канальних ресурсів інформаційно-комунікаційних систем (наприклад, розширення серверних можливостей, використання «віртуального» волокна, збільшення потужності TV- і радіо передавачів систем мовлення, збільшення кількості транспондерів супутників зв'язку та ін.);*

**** - *наприклад, відповідні визначення ООН, ЮНЕСКО та ін.*

Рис. 1 – Тотожність структури складових кібербулінгу та сучасних інформаційних операцій

3. Для аргументації узагальнення, стосовно тотожності структури кібербулінгу (*особливо для випадків глобального рівня впливу*) та основних складових інформаційних операцій, слід проаналізувати відомості, які систематизовані на рис. 1.

Аналіз наведеної схеми дозволяє стверджувати, що основні складові процесу булінгу в кіберсфері, співпадають з відповідними елементами, які притаманні для сучасних умов ведення інформаційних операцій [7]. Існування можливих відмінностей, в частині ієрархічної значущості обраної жертви, складу кадрового забезпечення та ролей учасників цькування, абсолютно не принципово, так як в будь-якому випадку присутні безпосередні виконавці акції мережевої травлі, та є маркована ціль для атаки.

В разі високої ієрархічної значущості жертви, основні учасники заходів мережевої травлі присутні в усіх 3-х складових кадрового забезпечення (*див. рис. 1*). Так, представники основного інтегратора (*або інтеграторів*) комунікаційних послуг, на базі котрого (-*рих*), безпосередньо, здійснюється інформаційний вплив, представлені на рівні її технічних спеціалістів і фахівців, котрі здійснюють концептуальну модерацію контенту та визначають етапність його подачі (*тобто, фактично, визначають інформаційну повістку всієї акції*).

Другій рівень – «***КІНЦЕВІ СПОЖИВАЧІ***», за рахунок щільної взаємної інтеграції використовуваних телекомунікаційних сервісів і послуг, формує наймасовішу кадрову складову подій. Даний рівень поєднує заявлену жертву атаки, та саму представницьку рольову групу – «спостерігачів», яка, власне, і є прихованою (*неявною*) головною метою здійснюваного інформаційного впливу.

Третій рівень – «***Персонал взаємодіючих інтеграторів …***», складають тимчасові IT–аутсорсери [17] та фахівці на IT–рекрутингу, які залучаються для підтримки необхідних форм (*чат-боти, стрім-канали, тематичні форуми тощо*), масштабів і термінів проведення акції. Представники цієї групи здійснюють проміжну обробку і розповсюдження потрібного контенту, та можуть приймати безпосередню участь в здійсненні певних заходів цькування.

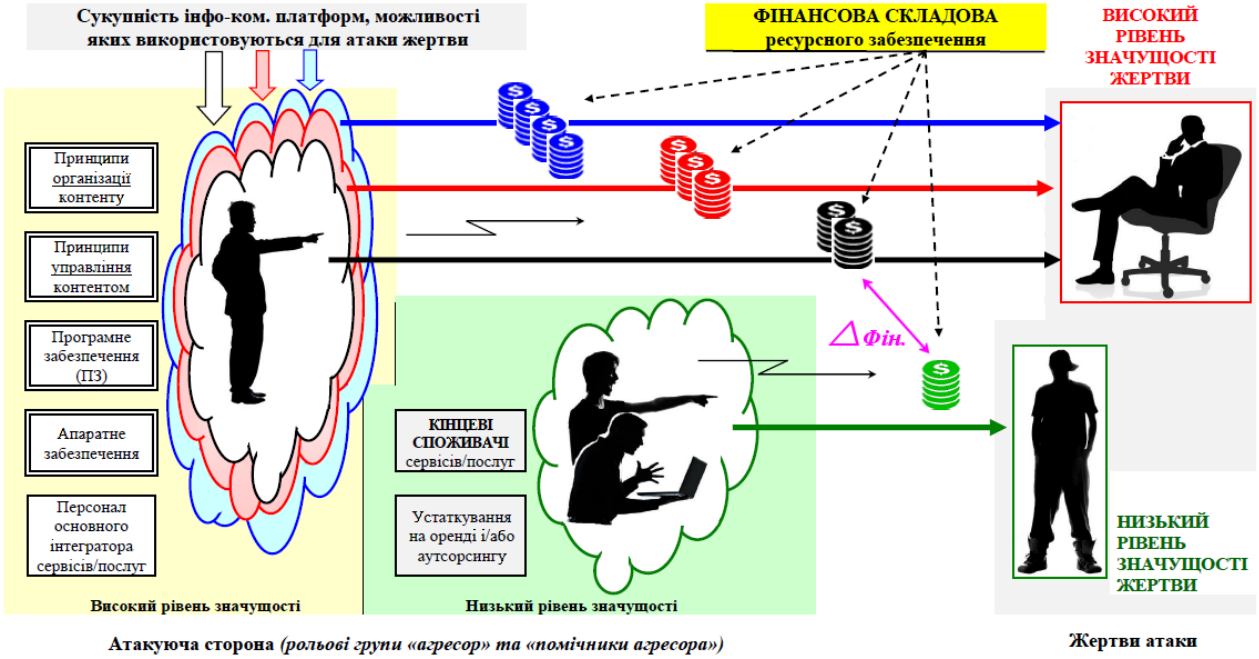


Рис. 2 – Відмінності повноважень адміністрування контенту та складових ресурсного забезпечення агресора для різних рівнів значущості жертви

При низьких рівнях ієрархічної значущості жертв атаки *(наприклад, у випадках підліткового цькування),* основні учасники травлі, об'єктивно обмежені представництвом рівня «***КІНЦЕВІ СПОЖИВАЧІ***». Іншими словами, всі учасники будь-яких можливих подій подібного масштабу та рівня значущості, повністю позбавлені компетенцій зі зміни параметрів технічної складової ресурсного забезпечення та функцій адміністрування "***принципів управління контентом***" (рис. 1-2). Власне ця обставина і обумовлює допустимі межі умовних "правил гри". Незначні відхилення від цих обмежень можливі в разі проведення акцій булінгу на рівні корпоративного сегменту, що може бути обумовлено наявністю відповідних елементів ресурсного забезпечення у окремих учасників процесу (*наприклад, наявність власного медійного ресурсу*) та/або їх можливістю здійснювати хоча б часткове адміністрування контенту *(наприклад, визначати власні "принципів управління контентом")*. Також, при здійсненні булінгу на корпоративному рівні впливу та/або проти об'єктів з високим рівнем ієрархічної значущості, категорія «***Персонал взаємодіючих інтеграторів…***» (рис. 1) може поєд-

нувати в собі представників ролевих груп «***помічники агресорів***» і «***хамелеони***», які будуть діяти згідно загальної концепції заходів мережевого цькування (*буде розглянуто нижче*).

4. Вочевидь, що необхідність збільшення кількості задіяних технічних ресурсів *(наприклад, використання можливостей відразу декількох інформаційно-комунікаційних платформ (див. рис.2))*, зумовлює зростання потрібного обсягу "**ФІНАНСОВОЇ СКЛАДОВОЇ**" **ресурсного забезпечення** заходів мережевий цькування, які проводяться або плануються. Тобто фінансове забезпечення заходів кібертравлі проти жертв з низьким рівнем значущості, може носити вельми умовний характер. В даному випадку, обмеження можливостей по контролю апаратного і програмного забезпечення тільки на рівні "**Кінцевих споживачів**", обумовлює "скромні" рівні бюджету подібних акцій (*в даному випадку, взагалі, можна говорити про ситуативний булінгсорсинг*). У той же час, атака жертви з низьким рівнем ієрархічної значущості, може здійснюватись шляхом "злому" та подальшого використання сторонніх апаратних ресурсів (*наприклад, шляхом формування бот-мережі, що поширює наклепницький контент*). В даному випадку всі витрати, що стосуються оплати мережевого трафіку і електроживлення скомпрометованих пристроїв, несуть власники цих (*зламаних*) пристроїв.

Таким чином, склад, структура і масштаб (*або кількість*) залучених ресурсів (рис. 1), визначають різницю в потрібних обсягах "**ФІНАНСОВОЇ СКЛАДОВОЇ**" для різних акцій мережевого булінгу (рис. 2). Крім того, маючи на увазі значну кореляцію структури і основних складових інформаційних операцій та кібербулінгу, можна стверджувати, що розмір "**ФІНАНСОВОЇ СКЛАДОВОЇ**" **ресурсного забезпечення**, безпосередньо визначає рівень потенційної складності структури заходів кібертравлі. Іншими словами, враховуючи багаторівневий (*або пошаровий*) характер сучасних інформаційних операцій, наявний розмір фінансового забезпечення заходів мережевого цькування, обумовлює кількість відповідних верств на кожному з етапів інформаційного впливу. Усунення або інформаційне купірування одного або ж відразу декількох шарів «атакуючого» контенту (*безвідносно причини події*) не змінює загального вектору проведеної атаки (кібертравлі) та гарантує збереження необхідної інформаційної повістки. Вочевидь, що послідовність, інтенсивність та тривалість інформаційного тиску на жертву, безпосередньо пов'язані з "**ФІНАНСОВОЮ СКЛАДОВОЮ**" **ресурсного забезпечення**, що є в розпорядженні потенційного агресора [18].

Так, наприклад, при необхідності легітимації джерела даних з заздалегідь неправдивою інформацією (*для умов булінгу - джерела даних з наклепницьким контентом*), в одному шарі, необхідно послідовно реалізувати кілька процедур:

а) синтезувати (*а згодом оновлювати*) «атакуючий» контент;

б) створити відповідний інформаційний ресурс - «прокладку» (*наприклад сайт або ж тематичну гілку на форумі або паблік в соціальній мережі*);

в) забезпечити механізм постійної апеляції/відсилання до контенту на даному ресурсі (*для умов кібербулінгу це функція рольової групи «**помічники агресора**»[9]*).

Для нарощування ефекту необхідна організація другого шару, що дозволить з необхідною періодичністю забезпечувати взаємний репост та/або посилання/згадки «атакуючого» контенту. Вочевидь, що зі збільшенням кількості подібних шарів збільшується кількість взаємних посилань, підтримується необхідна тематична повістка (*в нашому прикладі, дані з наклепницьким змістом*), та експресія цькування. При цьому локалізація і підтримка необхідної інформаційної повістки, в рамках конкретної інформаційно-комунікаційної платформи (рис. 2), забезпечується шляхом розміщення інформаційного ресурсу - «прокладки» на потрібної технічної платформі. Важливо підкреслити, що локація (*присутність*) цілі атаки та локація інформаційних ресурсів - «прокладок», можуть не збігатися! Іншими словами, атака обраної жертви може проводитися:

- при її повній відсутності на обраної технічній платформі;

- при її часткової присутності на цій платформі (*наприклад, епізод з обмеженням «присутності» колишнього президента Сполучених Штатів Америки Д. Трампа на основних національних інформаційних ресурсах в ході виборчої кампанії 2020 року*);

- в умовах паритетного представництва агресора і жертви, принаймні, на початковій фазі атаки. Очевидно, що такі (*дуельні*) умови невигідні для агресора, тому що знижують ефект від вжитих ним дій.

Комплексна атака жертви, з використанням можливостей відразу декількох інформаційно-комунікаційних платформ (рис. 2), потенційно, дозволяє реалізувати багатоетапну та багатошарову структуру інформаційного впливу. Проте, така схема булінгу потребуватиме використання загального координуючого центру і залучення більшої кількості відповідних фахівців (рис. 1), що зумовить зростання фінансового забезпечення потрібних заходів.

5. Фактор доступності (*неперервності*) використовуваних онлайн сервісів і послуг визначає не тільки спосіб, масштаб і тривалість реалізації процесу кібертравлі, а й обумовлює саму можливість його здійснення. Характерним прикладом успішно реалізованих заходів кібертравлі, що експлуатують фактор доступності комунікаційних сервісів, є події по одночасної «ізоляції» (*виключенню та ігноруванню*) колишнього президента Сполучених Штатів Америки Д. Трампа, на основних національних інформаційних і глобальних комунікаційних ресурсах (*TV компанії, соціальні мережі та ін.*). Такий варіант реалізації атаки забезпечує підтримку головної умови успішності проведеної акції – нерівність сил агресора[4] і жертви.

Примітка:

[4] – *уточнення рольової категорії «агресор», в разі монополізації основних складових процесу кібербулінгу, буде надано нижче, при розгляді питань, стосовно аналогій з умовами проведення експерименту С. Мілґрема.*

Показовим прикладом критичності фактора доступності, є можливість потенційного об'єднання, в рамках однієї компанії, холдингу або держави, основних складових «***Ресурсного забезпечення***» та функцій «***Адміністрування контенту***» (*виділено жовтим тоном на рис. 1*). Подібний варіант інтеграції складових досить імовірний, наприклад, в разі повного розгортання низькоорбітальної глобальної супутникової системи *Starlink* (*від компанії SpaceX*). Поєднання в одному центрі прийняття рішень основних складових ресурсного забезпечення (*перш за все її програмної і апаратної компонент*) та функцій адміністрування контенту стає серйозною проблемою навіть для рівня окремих держав, не кажучи вже про персональний рівень впливу. Атакуюча сторона, що має такі ресурси, отримує в «свої руки» всі ключові функції процесу: - планування; - супровід; - контроль результату. Більш того, домінування корпоративних норм основного інтегратора послуг в питаннях адміністрування контенту, фактично зумовлює кінцевий результат. В цих умовах, можлива протидія обмежується заходами в двох основних напрямках: - правовому та технічному. Зусилля по першому напрямку повинні бути сконцентровані на спробах спонукання (*згодом і примусу (податкового, тарифного тощо))* закордонних ІТ-компаній [5] відкривати свої представництва на територіях під юрисдикцією суб'єкта [6], котрий демонструє подібний «мотивуючий тиск». Зусилля в рамках 2-го напряму, скоріш за все, будуть обмежуватись, заходами фрагментарної фільтрації контенту, ліцензування та контролю постачання абонентського обладнання (*в т.ч. попереднього встановлення і контролю джерел поширення відповідного ПЗ*), і то, тільки за умови дієздатності відповідних відомств, та служб.

Примітка:

[5] – *сервіси, служби та послуги яких, використовуються, або можуть бути використані, в тому числі, для цілей проведення акцій мережевого булінгу;*

[6] – *вирішення проблеми транспарентності кордонів у кіберпросторі, шляхом його сегментації нормативно-правовими засобами, в межах окремих територіальних юрисдикцій.*

6. Відповідно до умов експерименту Мілґрема (*експеримент про покору*), до його проведення залучались: – «експериментатор» (*персона з повноваженнями коригувати хід експерименту*); – «вчитель» (*випробуваний, який лише частково уявляв сенс експерименту*); – «учень» (*актор, що грав свою роль та мав уявлення про сенс експерименту*). Які ж аналогії можна виділити, порівнюючи учасників експерименту про покору та ролі основних фігурантів акцій цькування в кіберпросторі (див. рис. 3)?

Доречно зауважити, що рольова структура учасників звичайного булінгу набагато простіше, ніж рольова структура учасників кібербулінгу. Так, в ситуації «традиційного» булінгу присутні три основні ролі: – жертва, переслідувач і свідок. При цьому рольова структура кібербулінгу передбачає присутність наступних акторів [9]: 1 – «агресори»; 2 – «помічники агресорів», які забезпечують підтримку процесу цькування; 3 – «жертви», це учасники процесу, що піддаються публічному цькуванню; 4 – «захисники і хамелеони», представники цих груп не стабільні і можуть мігрувати між групами «спостерігачів» і «агресорів» (*або «помічників агресорів»*); 5 – «спостерігачі» це найчисленніша і ситуативно не ангажована група учасників (*принаймні, на початковому етапі подій*).

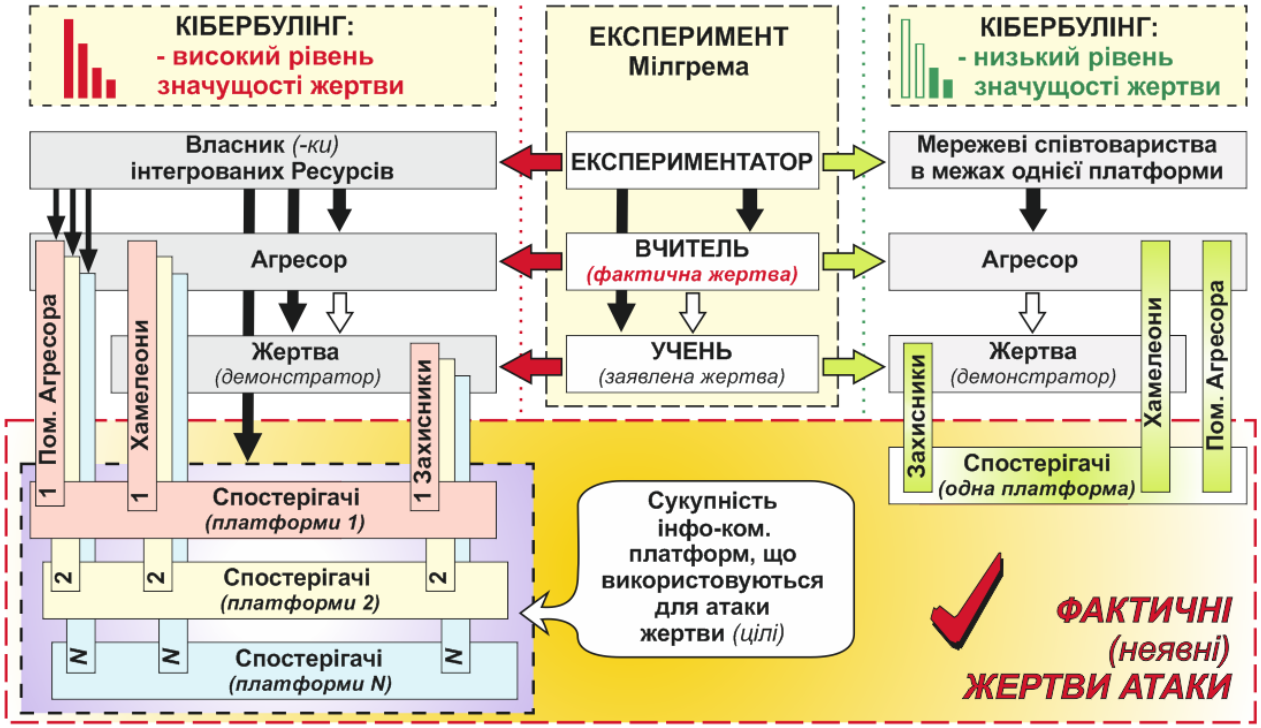


Рис. 3 – Передбачувана структура аналогій

Враховуючи фактор анонімності присутності представників 5-ї групи (*в ході здійснення заходів мережевої цькування*), можна зазначити, що на відміну від ситуації «традиційного» булінгу, в даному разі відсутній прямий контакт між «агресором» і «спостерігачами». При цьому, віддалена присутність учасників цієї групи та можливість швидкої зміни їх чисельності, визначають основну рольову функцію даної групи, заради якої, власне, організовується і підтримується все дійство. Таким чином, з огляду на швидкість, масштабованість та повторюваність процесу цькування, ця група учасників, де-факто, є кінцевою ціллю проведення всієї акції, за результатами якої повинні бути скориговані їх соціальний (мережевий) статус або соціальна (мережева) поведінка, або ж і те й інше одночасно. Тобто, в даному випадку, можна говорити про приховану насильницьку корекцію самоідентифікації учасників даної групи, шляхом послідовної і навмисної зміни їх уявлень, про норми соціальної (*мережевої*) поведінки в кіберпросторі.

Можна припустити, що саме таке трактування прихованих цілепокладань процесу кібербулінгу, є тією сполучною, котра забезпечує його концептуальну аналогію з основною парадигмою експерименту С. Мілгрема. У заявленому контексті неявній ролі «спостерігачів», роль «жертви» трансформується в інструмент для досягнення іншої, прихованої глобальної мети – забезпечення абсолютного домінування в найбільш представницької мережевій рольової групі. При такій постановці питання, роль «жертви», як це не дивно виглядає, це всього лише «ширма», основним призначенням якої, є нав'язування мережевого дискурсу із заздалегідь визначеним наративом і прихованим кінцевим цілепокладанням. Іншими словами,

в даному випадку, можна говорити про одну з можливих реалізацій стратегії непрямих дій, що адаптована до умов існування інформаційного суспільства і можливостям ведення інформаційних операцій в кіберпросторі.

А тепер, власне, про аналогії з «експериментом про покору». Вочевидь, що найпростіше виділити учасників групи «***вчитель***» (*головний випробовуваний цього експерименту*). Відносно процесу булінгу в кіберсфері, такі функції виконує «***агресор***». При цьому визначальною якістю представників цієї групи (*мережевого співтовариства*) повинна бути готовність «йти до кінця», в рамках реалізації всього комплексу заходів цькування, об'єднаних загальною стратегією дій. Крім того, група «***вчитель***» може поглинати і рольову категорію «***помічники агресорів***», яка в більшості випадків знайома з порядком та умовами проведення заходів травлі (рис. 3). Однак, у випадках проведення заходів з «глобальним рівнем впливу», представники цієї рольової групи, швидше за все, не будуть ознайомлені з кінцевою метою проведеної акції (*залучаються для завдань підготовки контенту або підтримки процесу цькування*). Іншими словами завдання акторів групи «***вчитель***» можуть бути фрагментовані, а їх використання обмежуватися рамками передбачених етапів/стадій мережевої атаки.

Також слід мати на увазі, що на відміну від умов експерименту С. Мілгрема, де «***учень***» мав певні уявлення про задум та хід експерименту, в випадку здійсненні заходів кібербулінгу маркована ***жертва*** атаки не має відповідних преференцій. В умовах мережевої травлі таку обізнаність можуть мати тільки представники рольової групи *«**хамелеони**»*, які виступають своєрідними каталізаторами або провокаторами потрібних дій ***жертви***. Перебуваючи, на різних стадіях атаки, в різних рольових іпостасях *(«спостерігач», «захисник жертви» або «помічник агресора»*), учасники рольової групи *«**хамелеони**»* є еквівалентом поведінкових якостей «***учня***» з експерименту Мілгрема. Вочевидь, що представники цієї групи повинні бути досить інформовані з приводу реалізованих заходів цькування (*принаймні, про заплановані стадії заходів травлі та маркери власної рольової міграції*). Зрозуміло, що краудсорсінг в даному випадку виключений, тому залучення фахівців відповідних кваліфікації, професійних якостей та мотивацій, можливо тільки на основі підряду або IT-аутсорсінгу (рис. 1-2).

Виникає логічне запитання: - хто ж визначає «***жертву***» та формує стратегію всієї акції (*тобто, правіла адміністрування контенту, стадії, час і масштаб проведення заходів*)?

В пошуках відповіді ми виходимо на повноваження «***експериментатора***» (*в термінології експерименту про покору*). Враховуючи тенденцію останніх років, до «зрощення» джерел контенту та основних складових ресурсного забезпечення інформаційних систем, вочевидь, що учасниками рольової групи «***експериментатор***», при високих рівнях ієрархічної важливості об'єктів кібертравлі, можуть бути тільки вигодоутримувачі (*або монополісти*) результатів подібного об'єднання. Крім того, незнання «***жертвою***» мережевого цькування факту присутності в схемі атаки (*заходів психологічного тиску*), учасників рольової категорії «***експериментатор***» (*в нашому випадку монополіста інтегрованих ресурсів*), додатково посилює існуючі аналогії з умовами проведення експерименту Мілгрема. При цьому, в заходах мережевого цькування на нижчих рангах ієрархії (*тобто в «традиційному» розумінні випадків кібербулінгу*), в ролі «***експериментатора***», нажаль, можуть виступати представники тимчасових мережевих співтовариств, які визначають локальну інформаційну повістку (*онлайн голосування, рейтингові оцінювання, опитування та ін.*) та формують потрібну для них форму уявлень, про норми мережевої поведінки в «їх» кіберпросторі.

3 Висновки

1. Об'єкти кібертравлі значною мірою корелюють з основними об'єктами впливу в ході ведення сучасних інформаційних операцій.

2. При реалізації кібербулінгу роль «жертви» зводиться до функцій демонстратора можливостей «агресора», стосовно змін мережевого статусу та коригування уявлень про норми мережевої поведінки представників найбільш численної рольової групи - «спостерігачів».

3. Головна мета представників рольової групи «агресор» при реалізації акцій кібербулінгу, це забезпечення абсолютного домінування в ролевій групі «спостерігачів».

4. Рівень ієрархічної значущості представників рольової групи «жертва», обумовлює необхідну ступінь інтеграції (*монополізації*) функцій адміністрування контенту і основних складових ресурсного забезпечення залучуваних інформаційно-комунікаційних систем.

5. Рівень значущості маркованої жертви атаки, в значній мірі визначає необхідний обсяг фінансової складової ресурсного забезпечення заходів кібертравлі.

6. Сучасні акції мережевого булінгу, особливо у випадках високих рівнів значущості об'єктів кібертравлі, мають багаторівневий та багатошаровий характер. Нейтралізація одного або ж відразу декількох шарів «атакуючого» контенту не змінює загального тренду кібертравлі і гарантує збереження необхідної інформаційної повістки.

7. Розмір фінансової складової ресурсного забезпечення агресора, визначає потенційний рівень складності структури заходів кібертравлі.

8. Характер поведінки і ролі основних учасників процесу кібертравлі, багато в чому ідентичні умовам та цілям проведення експерименту Мілгрема.

9. В залежності від фактичного рівня ієрархічної важливості об'єктів кібертравлі, можливі істотні відмінності в представництві групи «експериментатор».

10. При високих рівнях ієрархічної важливості об'єктів кібертравлі, представниками рольової групи «експериментатор», є ***власники*** інтегрованих активів (*перш за все інформаційних і технічних*).

11. Принциповою умовою «успішності» інформаційного впливу, в рамках проведення акцій булінгу в кіберпросторі, є забезпечення потрібного рівня диспаритету можливостей (ресурсів) агресора і жертви.

12. Одночасне використання атакуючою стороною можливостей відразу декількох інформаційно-комунікаційних платформ, є показовим прикладом забезпечення нерівності можливостей агресора і жертви.

Посилання

[1] Цькування [Електронний ресурс]: Wikipedia. Вільна енциклопедія. – Режим доступу: http://surl.li/omyd (дата звернення: 20.01.2021).

[2] What is cyberbullying? [Online]. Available: https://nuedusec.com/blog/cyberbullying/ Accessed on: January 07, 2021.

[3] Интернет-травля [Электронный ресурс]: Wikipedia. Свободная энциклопедия. – Режим доступа: http://surl.li/omyr (*дата обращения*: 29.01.2021).

[4] Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19

[5] Vdovenko, S., Danik, Y., & Faraon, S. (2019). Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. *Комп'ютерні науки та кібербезпека*, (1), 18-30. https://doi.org/10.26565/2519-2310-2019-1-02 (дата звернення: 21.12.2020).

[6] Гайкова, В., & Малахов, С. (2020). Дослідження явища кібербулінгу і шляхів протидії його проявам. *Комп'ютерні науки та кібербезпека*, 1(1), 14-32. https://doi.org/10.26565/2519-2310-2020-1-02 (*дата звернення: 30.12.2020*).

[7] Макаренко С. И. Информационные операции: Фрагмент монографии. [Електронний ресурс] / С. И. Макаренко – Режим доступа: https://psyfactor.org/psyops/makarenko-304.htm. *Дата обращения: Декабрь 31, 2020.*

[8] Інформаційна операція [Електронний ресурс]: Wikipedia. Вільна енциклопедія. – Режим доступу: http://surl.li/onen (*дата звернення: 29.01.2021*).

[9] Ролевая структура кибербуллинга [Электронный ресурс]: Wikipedia. Свободная энциклопедия. – Режим доступа: http://surl.li/ocjv (*дата обращения*: *29.01.2021*).

[10] Овсянникова А. Эксперимент Милгрэма полвека спустя [Электронный ресурс] / А. Овсянникова – Режим доступа: http://surl.li/onca. *Дата обращения: 29.01.2021.*

[11] Експеримент Мілгрема [Електронний ресурс]: Wikipedia. Вільна енциклопедія. – Режим доступу: http://surl.li/oubj (дата звернення: 29.01.2021).

[12] Conducting the Milgram experiment in Poland, psychologists show people still obey. [Online]. Available: https://www.eurekalert.org/pub_releases/2017-03/sfpa-ctm030917.php. Accessed on: January 08, 2021.

[13] Информационное общество [Электронный ресурс]: Wikipedia. Свободная энциклопедия. – Режим доступа: http://surl.li/onlr (*дата обращения: 29.01.2021*).

[14] Информационное общество. Новая философская энциклопедия: в 4 т. / Электронная библиотека Института философии РАН. – Режим доступа: http://surl.li/onnv. *Дата обращения: Январь 29, 2021.*

[15] Террористический акт в редакции Charlie Hebdo [Электронный ресурс]: Wikipedia. Свободная энциклопедия. – Режим доступа: http://surl.li/qzgt *(дата обращения: 29.01.2021).*

[16] Политический кризис в Венесуэле (с 2019 года) [Электронный ресурс]: Wikipedia. Свободная энциклопедия. – Режим доступа: http://surl.li/qyzc *(дата обращения: 29.01.2021).*

[17] Дідух Т.М. Глобальні ризики використання IT-аутсорсингу [Електронний ресурс] / Т. М. Дідух – Режим доступу: http://global-national.in.ua/archive/20-2017/8.pdf. *Дата звернення: 29.01.2021.*
[18] Байден побил рекорд по анонимным пожертвованиям на предвыборную кампанию [Электронный ресурс] – Режим доступа: https://www.rbc.ru/politics/24/01/2021/600cd63c9a794789ada2136a Дата обращения: 29.01.2021.

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

Поступила: Январь 2021.

Авторы:
Валерия Гайкова, студентка магистратуры кафедры безопасности информационных систем и технологий, ХНУ имени В. Н. Каразина, Харьков, Украина. E-mail: valeriagaikova98@gmail.com
Сергей Малахов, к.т.н., с.н.с., факультет комп'ютерних наук, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: mailgate@meta.ua

Анализ факторов и условий реализации кибербуллинга, с учетом возможностей современных информационных систем.

Аннотация. Представлен перечень основных обобщений и факторов, характерных для различных вариантов и условий осуществления акций сетевой травли (кибербуллинга). Предложена аргументация определенных аналогий и совпадений между процессом сетевой травли, а также условиями и целями проведения современных информационных операций. Обращено внимание на то, что условия кибертравли во многом совпадают с парадигмой эксперимента С. Милгрэма. Предложена аргументация сути некоторых аналогий между проявлениями кибербуллинга и основной фабулой эксперимента о повиновении. Подчеркнуто, что уровень иерархической важности объектов кибертравли, обусловливает степень необходимой интеграции функций администрирования контента и основных составляющих ресурсного обеспечения современных информационных систем. Отмечено, что интеграция в одном центре принятия решений основных составляющих ресурсного обеспечения и функций администрирования контента, является серьезной проблемой даже для уровня отдельных государств, не говоря уже о персональном уровне воздействия. Обращено внимание на тот факт, что кибербуллинг может реализовываться, как путем использования возможностей отдельных информационных технологий, так и воплощать концепцию интегрированной атаки. Подчеркнуто, что явление кибербуллинга является значительно недооцененным и поэтому, представляет собой серьезную проблему современности.

Ключевые слова: буллинг; кибербуллинг; информационная повестка; контент; информационные технологии; техническая платформа; сетевое поведение; сетевой статус; эксперимент Милгрэма.

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

Received: January 2021.

Authors:
Valeriia Haikova, Student of the Department of Security of Information Systems and Technologies, V.N. Karazin Kharkiv National University, Ukraine. E-mail: valeriagaikova98@gmail.com
Serhii Malakhov, Ph.D., Senior Researcher, Computer Science Department, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine. E-mail: mailgate@meta.ua

Analysis of factors and conditions of implementation for cyberbullying, taking into account the capabilities of modern information systems.

Annotation. A list of the main generalizations and factors characteristic of various options and conditions for the implementation of actions of network bullying (cyberbullying) is presented. The argumentation of certain analogies and coincidences between the process of network bullying, as well as the conditions and goals of modern information operations is proposed. Attention drawn to the fact that the conditions of cyberbullying largely coincide with the paradigm of S. Milgram experiment. The argumentation of the essence of some analogies is offered between the manifestations of cyberbullying and the main concept of the experiment of S. Milgram's experiment. It is emphasized that the level of hierarchical importance of cyberbullying objects, determines the degree of integration of content administration functions and the main components of the resource support of information systems. It is noted that integration in one decision-making center all major technical resources and content administration functions, is a serious problem even for the level of individual states, not to mention the personal level of exposure. Attention is drawn to the fact that cyberbullying can be implemented, both by using the capabilities of individual information technologies, and embody the concept of integrated attack. It was emphasized that the phenomenon of cyberbullying is significantly underestimated and therefore, represents a serious problem of our time.

Keywords: Bullying; Cyberbullying; Information agenda; Content; Information Technology; Technical platform; Network behavior; Network status; Milgram's experiment.