СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. З досвіду роботи «Використання хмарних технологій та сервісів в освітньому процесі». НаУрок : вебсайт. URL: https://naurok.com.ua/z-dosvidu-roboti-vikoristannya-hmarnih-tehnologiy-taservisiv-v-osvitnomu-procesi-6840.html.
2. Концепція нової української школи. Інститут модернізації змісту освіти : вебсайт. URL: https://imzo.gov.ua/osvita/nush/.

НЕБЕЗПЕЧНЕ СПІЛКУВАННЯ ОНЛАЙН: РИЗИКИ, ПРАВИЛА, МЕХАНІЗМИ ЗВЕРНЕННЯ ПРО ДОПОМОГУ Й ЗАХИСТ

ІДЕНТИФІКАЦІЯ НЕБЕЗПЕК ТА РОЗВИТОК СТРАТЕГІЙ ЗАХИСТУ У ВІРТУАЛЬНОМУ СВІТІ

Ольга ЛУНГОЛ, Павло ТОРГАЛО

Онлайн-спілкування молоді займає центральне місце в їхньому повсякденному житті, визначаючи нові форми взаємодії та спілкування. З розвитком технологій та поширення Інтернету, молодь активно використовує онлайн-платформи для обміну інформацією, вираження своїх поглядів, взаємодії з оточуючими та розвитку власної ідентичності.

Соціальні мережі, чати, месенджери та інші онлайн-середовища стали не лише засобом спілкування, але і платформою для вираження творчості, розваг та освітнього розвитку. Молодь використовує ці інструменти для обговорення актуальних тем, створення власного контенту, знаходження подібно мислячих людей та розвитку власної соціальної мережі.

Онлайн-спілкування впливає на формування соціальних навичок та розвиток міжособистісних стосунків. Взаємодія в Інтернеті дозволяє молодому поколінню ефективно виражати свої емоції, розвивати комунікативні навички та будувати стосунки в цифровому просторі. Збільшенню часу перебування молоді у віртуальному світі спонукали спочатку карантинні обмеження внаслідок активного розповсюдження гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2, а зараз – повномасштабного вторгнення росії в Україну.

Онлайн-спілкування молоді, хоча й має численні позитивні аспекти, також пов’язане із певними ризиками та небезпеками. Проаналізувавши матеріали з сайту Кіберполіції України [1], інформацію Computer Emergency Response Team of Ukraine та дослідження вітчизняних науковців Агішевої А.В. [3], Кошової-Куклішини Л.С. [4], Денисюк О.М. [4], Іванюк Г.І. [5], Бовсунівської Д.В. [5] та ін., ми виокремили основні небезпеки онлайн-спілкування молоді:

- Кібербулінг – молодь може стати жертвою кібербулінгу, коли вони піддаються онлайн-засудженню, погрозам, образам або іншим формам психологічного впливу. Кібербулінг може призвести до розвитку стресу, психологічних проблем та соціальної ізоляції.

- Порушення онлайн-приватності. Недостатня поінформованість щодо захисту особистої інформації може призвести до її неправомірного використання або витоку. Зловмисники можуть використовувати цю інформацію для шахрайства, стеження чи інших проявів злочинної діяльності.
- Перегляд неприпустимого контенту. Молодь може ненавмисно потрапляти на онлайн-сайти або матеріали, які містять агресивний, неприязний чи шкідливий контент, що може впливати на їхнє емоційне та психічне здоров'я.
- Онлайн-залученість. Зайвий час перебування в Інтернеті може призвести до залученості та зневаження реального світу, що може негативно впливати на академічну, соціальну та фізичну діяльність молодого покоління.
- Онлайн-залежність. Занадто інтенсивне користування Інтернетом та соціальними мережами може викликати залежність, що впливатиме на психічне здоров'я та взаємовідносини в реальному житті.
- Шахрайства та обман. Молодь може стати жертвою інтернет-шахрайств, фішингу або обману, що може призвести до втрати особистої інформації чи фінансових втрат.

Захист від небезпек онлайн-спілкування для молоді важливий для їхньої цифрової безпеки та психологічного благополуччя. Серед стратегій захисту від небезпек онлайн-спілкування молоді ми в першу чергу виділяємо важливість інформування молоді про потенційні загрози онлайн, формування вмінь розпізнавати шахраїв, уникати фішингу та управляти власною приватністю в Інтернеті. Слід навчати молодь обережно ставитися до розголошення особистих даних, таких як адреса, номер телефону чи шкільна інформація. Батькам необхідно встановлювати розумні обмеження по часу, який неповнолітні проводять в Інтернеті, щоб уникнути перевантаження та залежності. Контролювати, що молодь використовує безпечні та довірені онлайн-платформи та додатки, які пропонують належні заходи безпеки. Освітянам та батькам слід вчити підростаюче покоління розпізнавати та повідомляти випадки кібербулінгу, навчати бути ввічливими та поважати інших онлайн. За можливості, батьки мають встановлювати фільтри та контроль за контентом, щоб обмежити доступ до неприйнятного або небезпечного матеріалу. Підкреслювати важливість уникання особистого спілкування чи обміну інформацією з незнайомцями в Інтернеті.

Загалом, онлайн-спілкування молоді визначає новий спосіб взаємодії та створює цифровий аспект їхнього соціального життя, що відображається в різноманітних сферах, від освіти та розваг до соціально-політичної активності. Проте, ідентифікація потенційних небезпек у віртуальному світі є першочерговою задачею для забезпечення безпеки користувачів. Розуміння ризиків, пов'язаних із кібербезпекою, кіберзлочинністю та іншими аспектами віртуального середовища є ключовим етапом. Основою для захисту від небезпек у віртуальному просторі є розробка та впровадження ефективних стратегій захисту. Це включає в себе використання технологічних засобів, розвиток цифрової грамотності, освіту та психологічну підтримку користувачів. Для успішного впровадження стратегій захисту важлива співпраця між громадськістю, бізнесом, урядом та освітніми установами. Освіта та

інформаційна кампанія щодо кібербезпеки мають займати важливу роль у підвищенні обізнаності та усвідомленості молоді.

З урахуванням постійної еволюції технологій та зміни характеру кіберзагроз, стратегії захисту повинні піддаватися постійному вдосконаленню. При розробці та використанні стратегій захисту важливо дотримуватися етичних стандартів та забезпечувати конфіденційність даних.

Узагальнюючи, можна зазначити, що ефективна ідентифікація небезпек та розробка стратегій захисту вимагає комплексного підходу, включаючи технічні, освітні та психологічні аспекти. Взаємодія всіх зацікавлених сторін та постійне вдосконалення заходів забезпечать стійку безпеку в віртуальному світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кіберполіція України : офіційний сайт. URL: https://cyberpolice.gov.ua.
2. Computer Emergency Response Team of Ukraine. Урядова команда реагування на комп'ютерні надзвичайні події України : вебсайт. URL: https://cert.gov.ua.
3. Лунгол О.М., Агішева А.В. Технології створення та застосування систем захисту інформаційно-комунікаційних систем. *The 2 nd International scientific and practical conference «Topical aspects of modern scientific research»* (October 26-28, 2023) CPN Publishing Group, Tokyo, Japan. 2023. p. 255.
4. Кошова-Куклішина Л.С., Денисюк О.М. Формування у старшокласників навичок спілкування у соціальних мережах. *Соціальна підтримка сім'ї та дитини у соціокультурному просторі громади:* матеріали IV Всеукраїнської науково-практичної конференції. 2022. С. 141-143.
5. Іванюк Г.І., Бовсунівська Д.В. Безпека дитини в інформаційному просторі: проблеми та шляхи вирішення. *The 14 th International scientific and practical conference «Actual problems of science and practice»* (27-28 April, 2020). Stockholm, Sweden 2020. P. 191.

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ВПЛИВИ У ФОРМІ ЦИФРОВОГО ГАЗЛАЙТИНГУ У СОЦІАЛЬНИХ МЕРЕЖАХ ТА СПОСОБИ ЗАХИСТУ

Єлизавета МЕЛЕШКО

Газлайтинг є методом інформаційно-психологічного впливу, спрямованого на примушення об'єкту впливу сумніватися у своїй здатності адекватно сприймати реальність та на виникнення бажання віддати контроль над собою суб'єкту впливу, що досягається застосуванням брехні, заплутування, залякування, звинувачень, знецінення та різних комбінацій цих стратегій [1-3]. Газлайтер змушує свою жертву сумніватися у власній пам'яті, емоційній стабільності та адекватності, знецінює її почуття і думки, навіює їй уявну нікчемність, звинувачує у речах, які вона не робила, заперечує свої попередні слова і дії тощо. Виділимо такі різновиди газлайтингу: *побутовий*, *соціальний*,