Чаплінська Юлія

КІБЕРКУЛЬТУРА ТА КІБЕРБЕЗПЕКА В УМОВАХ ВІЙНИ

Психологічний практикум

Київ 2023

Юлія Чаплінська

Кіберкультура та кібербезпека в умовах війни: психологічний практикум

Практичний посібник

Київ-2023

УДК 159.316.772.5

Рекомендовано до друку вченою радою
Інституту соціальної та політичної психології НАПН України,
протокол №12/22 від 8.12.2022 р.

Рецензенти:

Пророк Н. В., доктор психологічних наук, старший науковий співробітник, завідувачка лабораторії психодіагностики та науково-психологічної інформації Інституту психології імені Г. С. Костюка НАПН України;

Дворник М. С., кандидат психологічних наук, старший дослідник, завідувачка лабораторії соціальної психології особистості Інституту соціальної та політичної психології НАПН України;

Паньковець В. Л., кандидат психологічних наук, доцент, доцент кафедри соціальної психології Київського національного університету імені Тараса Шевченка

Чаплінська Ю.

Кіберкультура та кібербезпека в умовах війни: психологічний практикум [Електронний ресурс] : практичний посібник / Юлія Чаплінська ; Національна академія педагогічних наук України, Інститут соціальної та політичної психології. – Київ, 2023. – 80 с.

ISBN 978-966-189-691-7

Психологічний практикум має на меті підготувати дітей до зустрічі з потенційними кіберризиками – ризиками, з якими вони можуть зіткнутися в інтернет-середовищі. Особливої актуальності набуває ця проблема в часи воєнного протистояння. У першій, теоретичній, частині практикуму представлено понятійний апарат кіберзагроз, висвітлено практичні і юридичні аспекти кібербезпеки в мирний і воєнний час, описано поняття воєнної кібербезпеки в її ключових моментах (безпека мобільних пристроїв, двохетапна аутентифікація, програмне забезпечення, безпека соціальних мереж, неправдиві повідомлення, або фейки, сумнівні сайти і посилання). Особливу увагу приділено юридичним аспектам кібербезпеки; нормативним та правовим документам, що регулюють цю сферу як в Україні, так і у світі; діяльності кіберполіції в Україні в мирний і воєнний час. У другій частині представлено п’ять практичних занять для дітей, мета яких – закріплення матеріалу, представленого в теоретичній частині. Ідеться про створення у свідомості дітей цілісної картини кіберризиків, з якими вони можуть зіткнутися в мирний час, та узагальнення й доповнення знань про кіберзагрози воєнного часу, формування алгоритму дій у критичних ситуаціях та вміння протистояти кібернебезпекам.

Адресується психологам, психотерапевтам, медіапедагогам, медіапсихологам, фахівцям у галузі освіти – учителям, шкільним психологам, викладачам закладів вищої освіти, соціальним працівникам, студентам, школярам, батькам.

УДК **159.316.772.5**

ISBN 978-966-189-691-7

ЗМІСТ

ВСТУП

Розвиток технологій та активна кіберсоціалізація дітей і молоді останнім часом істотно загострили проблему кіберризиків і кібербезпеки в українських реаліях.

Для сучасної дитини стало звичним бути постійно на зв'язку зі своїми рідними і друзями: використовувати різноманітні месенджери чи електронну пошту, щоб підтримувати зв'язок з близькими; соціальні мережі, щоб обмінюватися новинами; Google, щоб шукати інформацію; мобільні ігри, щоб перебути час. Інтернет і різноманітні додатки стали такою ж невід'ємною частиною життя дітей, як одяг чи їжа. Їм уже важко уявити своє життя без смартфона.

Коли ми говоримо про всі переваги, які привносять у наше життя смартфон чи планшет із доступом до інтернету, то часто забуваємо, що є й інша сторона цієї медалі, а саме кіберризики. Це передусім загрози, пов'язані з інтернет-активністю користувачів. І їх можна розглядати як під технічним, так і під психологічним кутом зору. Досить часто дорослі, так само як і діти, не приділяють належної уваги ризикам, які можуть чатувати на них в інтернет-середовищі.

Для того щоб продемонструвати, наскільки це актуальна тема, пропонуємо пройти невеличкий тест-драйв – попрацювати із самоопитувальником «Місце кіберзагроз у моєму житті». Самоопитувальник містить питання, пов'язані з найпоширенішими кіберзагрозами. Хочемо також звернути вашу увагу на те, що це далеко не повний список можливих кіберзагроз, а лише верхівка айсберга злочинного кіберсвіту. Щоб краще орієнтуватися в кіберзагрозах віртуального світу, можна, відповідаючи на поставлені запитання, відкрити Додаток № 1 до цього практикуму. (Кожен описаний там кіберризик має порядковий номер – це зроблено для зручності, щоб ви не витрачали даремно час).

Отже, візьміть, будь ласка, аркуш паперу та ручку і спробуйте відповісти на такі прості запитання:

1. Чи бачите ви на екрані якісь кіберризики, про які не знали досі? Якщо так, то запишіть їх у рядок (для економії часу можна просто записати їхні порядкові номери).

2. Чи стикалися ви особисто з яким-небудь із цих кіберризиків? Можливо, ви стали жертвою деяких із них? Якщо так, то з якими саме, зазначте їх. І порахуйте, чи це 1-2 кіберризики, чи понад 10.

3. Зі скількома кіберризиками із цього переліку стикалися ваші друзі або члени родини і розповідали вам про це? (2-6? Можливо, 15?)

4. Які пункти можна викреслити з цього переліку як такі, котрі не можна назвати кібернебезпекою? Якщо ви вважаєте, що вони є, будь ласка, запишіть їхні порядкові номери. І аргументуйте свою позицію. Наведіть щонайменше 7 аргументів. Якщо не зможете, то ваша пропозиція вилучити цей кіберризик з переліку буде вважатися недоцільною.

5. Яку кібернебезпеку в цьому переліку ви б назвали найжахливішою загалом? Було б добре, якби ви змогли пояснити – чому.

6. Чи є в цьому переліку кібернебезпека, з якою побоюєтеся зіткнутися особисто ви, тому що не знаєте, як поводитися? Або така, з наслідками якої ви навряд чи зможете впоратися? Запишіть порядковий номер того кіберризику, якого ви, по суті, боїтеся найбільше.

7. Чи говорили ви коли-небудь зі своїми дітьми про кіберризики? Якщо так, то який кіберризик (із цього переліку) ви не згадали у своїй розмові? Від чого ви не застерігали дитину?

8. Чи обговорювали ви з дитиною питання безпеки в інтернеті? Чи є у вас записані правила щодо того, що вашій дитині НЕ дозволено робити в інтернеті?

9. Чи говорили ви зі своєю дитиною про те, до кого ще вона може звернутися в разі кібернебезпеки? Окрім батьків, це має бути ще 2-3 дорослих, яким дитина може довіряти і з якими може поговорити в разі настання критичної ситуації.

10. Чи знає ваша дитина номер телефону кіберполіції?

Як бачите, ці питання досить прості, але вони змушують замислитися й усвідомити, наскільки близько кіберризики підібралися до кожного з нас. У деяких випадках можна навіть сказати, що вони стали частиною повсякденного життя… Але чи відчуваєте ви себе захищеними від них? Наскільки ви поінформовані? І наскільки ваша дитина/діти підготовлена(-ні) до зустрічі з різноманітними кібернебезпеками?

Лабораторія психології масової комунікації та медіаосвіти Інституту соціальної та політичної психології НАПН України вже досить давно працює над темою кіберризиків і кібербезпеки дітей в інтернет-середовищі. Працівники лабораторії здійснюють постійний моніторинг ситуацій, пов’язаних із молодіжними кіберризиками. Зокрема, проведено два всеукраїнські опитування – у 2018 і 2020 роках (Найдьонова, 2018; 2021). В опитуванні 2018 року взяли участь 1439 респондентів (768 дівчат і 671 хлопець віком від 13 до 16 років), 2020 року – 1681 респондент (918 дівчат і 763 хлопці віком від 12 до 17 років).

Дітям було запропоновано відповісти на низку запитань, пов’язаних з їхнім досвідом взаємодії з кіберризиками (табл. 1). Вони могли обирати із трьох варіантів відповідей один: «так», «ні», «важко відповісти». Щоб полегшити процедуру та розуміння дітьми запитань, в опитуванні було використано найпростішу шкалу відповідей.

Таблиця 1

Кіберризики (2018 р.)

З якими небезпеками під час використання інтернету Вам доводилося стикатися особисто? (у %)	**Частка відповідей** (у %)
нав'язування непотрібної інформації	59,7
втручання в роботу пристрою, зараження вірусами	57,0
поширення неправдивої інформації про вас	21,4
викрадення ваших особистих даних або використання ваших облікових записів	19,9
кібершахрайство – продаж неіснуючих послуг, примус до покупок, вимагання грошей	15,6
залякування, погрози завдати вам шкоди	14,4
кібербулінг – знущання, образи, приниження, психологічний терор проти вас	14,0
спілкування з незнайомцями з небажаними наслідками, наприклад небезпечні зустрічі з ними в реальності	7,1

заклики до насильства, агресії, розпалювання нетерпимого ставлення до інших	6,1
спонукання до самоушкодження	5,8

Згідно з результатами досліджень, проведених 2018 року, українські школярі найчастіше стикаються з такими кіберризиками, як спам, або контекстна реклама, коли користувачам нав'язують непотрібну інформацію (майже 60%); значно рідше діти стикаються з такими кіберризиками, як підбурювання до самоушкодження (близько 6%) (див. табл. 1).

Чим страшний спам, або контекстна реклама? По-перше, це повідомлення, які створюють штучне інформаційне перевантаження споживачів незначущою, вторинною, «зайвою» інформацією. По-друге, це можливість просування товарів і послуг, які можуть бути зовсім не потрібні споживачеві і які дуже часто можуть зовсім не відповідати віку тих, хто отримує цю інформацію. Наприклад, це може бути інформація сексуального чи релігійного змісту; можуть бути листи, основна мета яких – когось «очорнити» чи «побулити». По-третє, через нав'язливу інформацію діти можуть потрапити на гачок кіберзлочинців. Наприклад, це може бути інформація про те, що користувач має отримати якимось чином за посиланням велику суму грошей. По-четверте, досить часто такі повідомлення супроводжуються шкідливими програмами, вірусами. Власне, кіберризик, пов'язаний із втручанням у роботу обчислювальних пристроїв та зараженням техніки різними вірусами, майже так само добре знайомий дітям, як і нав'язлива інформація.

Якщо представити отримані від дітей відповіді у вигляді умовного рейтингу інтернет-ризиків, то перші позиції в ньому будуть посідати все ж таки *небезпеки, пов'язані з медійною сферою,* – нав'язування непотрібної інформації (це зазначають 59,7% школярів), і *технічні інтернет-небезпеки* – втручання в роботу пристрою, зараження вірусами тощо (повідомили 57,1% опитаних).

Далі йдуть *кібернебезпеки, і* першу позицію серед них посідає *поширення неправдивої інформації*, з чим стикається кожен п'ятий підліток (21,4%), майже на такому ж рівні буде *викрадення персональних даних* і використання іншими людьми приватних акаунтів від імені господаря (самозванство) (19,8%). У другу умовну групу інтернет-ризиків, з якими стикається майже кожен шостий підліток, разом з *кібербулінгом* також потрапляють ще два види: *залякування*, погрози завдання фізичної шкоди (15,6%) і *шахрайство* – продаж якихось вигаданих послуг, нав'язування покупок, виманювання грошей (14,3%).

Окремо хочемо виділити такий інтернет-ризик, як кібербулінг, оскільки досить часто українські медіаосвітяни порушують цю тему на щорічних стратегічних педегогічних нарадах. У Кодексі про адміністративні правопорушення 2019 року з'явилася нова стаття *173-4. Булінг (цькування)*, що зумовлено збільшенням числа таких випадків в українських школах. У разі умовної екстраполяції отриманих у 2018 році даних на всю генеральну сукупність отримуємо орієнтовну кількість підлітків, які перебувають під впливом надзвичайно небезпечних і деструктивних видів кібербулінгу. Так, щодо переслідування, якого зазнають 7,1% опитаних дітей, до групи ризику входить понад 77 тисяч підлітків; 6,1% школярів, яких кіберпростір спонукає до насильства, – це понад 66 тисяч; а 5,8% учнів, яких підштовхують через інтернет до самоушкоджень, загалом по всій Україні кількісно становить понад 63 тисячі осіб групи ризику (Найдьонова, Дятел, Вознесенська та ін., 2018). На цей час в Україні за правопорушення, пов'язані з кібербулінгом, передбачено такі міри покарання:

- штраф від 50 до 200 неоподатковуваних податком мінімуму доходу громадян;

●громадські роботи до 240 годин;

●виправні роботи до 1 місяця.

Якщо булінгом займається неповнолітня особа віком від 14 до 16 років, до відповідальності притягують батьків чи інших осіб, які їх заміщають (Булінг (цькування), Стаття 173-4, 2018).

Тут варто зазначити, що далеко не кожна дитина ділиться з батьками своїми проблемами в школі, але за непрямими ознаками їх можна ідентифікувати. Наприклад, коли батьки помітили на тілі дитини садна, забиті місця, синці, а дитина при цьому на запитання про їхнє походження мовчить або прикривається невмілою брехнею. У дитини може змінитися поведінка – спостерігається надмірне занепокоєння, агресія, плаксивість, опір і т. ін. – або, навпаки, дитина замикається в собі, демонструє пригніченість, апатичність, депресивні настрої. Також дитина може відмовлятися відвідувати навчальний заклад. У неї можуть пропадати особисті речі, а на запитання батьків про це дитина буде відмовчуватися або виправдовуватися, що вони десь є, але вона не пам’ятає, куди їх поклала, або що вона дала їх покористуватися друзям і ті скоро повернуть речі назад. В особистих розмовах можуть порушуватися теми суїциду (можуть також бути запити в історії інтернет-браузера). Часом діти втікають з дому.

Булінг може набувати різних форм – бути психологічним, фізичним або економічним. Кожен учасник булінгової ситуації потребує кваліфікованої психологічної допомоги – не тільки жертва, а й агресор і спостерігачі (яким ця ситуація також може завдати глибинної психотравми).

Третю групу інтернет-ризиків *маніпулятивного впливу* утворюють три найбільш небезпечні форми: *спілкування з незнайомими людьми* з небажаними наслідками (наприклад, прохання надіслати фото інтимного характеру або небезпечні реальні зустрічі з незнайомцями) (7,1%); *спонукання до насильства*, агресії, підбурювання нетерпимого ставлення до інших (6,1%), *підштовхування до завдання собі шкоди* (5,8%). Проте ці нібито низькі відсотки не мають створювати ілюзію незначущості таких загроз.

А проте, за даними лабораторії психології масової комунікації та медіаосвіти ІСПП НАПН України, 14,3% дітей вважають, що інтернет для них є абсолютно безпечним місцем, а 26,8% запевняють, що вони особисто не стикалися із жодними небезпеками під час користування інтернетом.

А проте опитування 2020 року дало вже дещо іншу картину.

Частота зіткнень з деякими кіберризиками, які дістали низькі оцінки у 2018 році, зросла майже вдвічі, а найпоширеніші кіберризики у 2018 році трохи «втратили» свої позиції (табл. 2).

Таблиця 2

Кіберризики (2020 р.)

З якими небезпеками під час використання інтернету Вам доводилося стикатися особисто? *(у %)*	**Частка відповідей** *(у %)*
нав'язування непотрібної інформації	42
втручання в роботу пристрою, зараження вірусами	30.5
кібербулінг – знущання, образи, приниження, психологічний терор проти вас	23
поширення неправдивої інформації про вас	17.6

залякування, погрози завдати вам шкоди	16.7
кібершахрайство – продаж неіснуючих послуг, примус до покупок, вимагання грошей	16.4
викрадення ваших особистих даних або використання ваших облікових записів	13.3
заклики до насильства, агресії, розпалювання нетерпимого ставлення до інших	11.1
спілкування з незнайомцями з небажаними наслідками, наприклад небезпечні зустрічі з ними в реальності	8.9
спонукання до самоушкодження	8.9

Аналізуючи дані опитувань 2018 і 2020 років, керівник Всеукраїнського експерименту з упровадження медіаосвіти в загальноосвітні навчальні заклади України Л. А. Найдьонова звернула увагу на те, частка кібернебезпек, пов’язаних із спонуканням до насильства, агресії, підбурюванням до нетерпимого ставлення до інших, зросла вдвічі і становить понад 11%. Частка кіберризиків, зумовлених підштовхуванням до самоушкодження (суїцидальні ігри та челенджі), наразі становить 8,9% (Найдьонова, 2021). З огляду на це науковці Інституту соціальної та політичної психології 2021 року започаткували новий проєкт, спрямований на превенцію і поственцію суїцидальної поведінки (Чуніхіна, & Умеренкова, 2022).

Але найбільше занепокоєння викликає наразі зростання частки епізодів, пов’язаних з кібербулінгом, – від 14% до 23%. Це дуже небезпечна, на нашу думку, тенденція, на яку обов'язково потрібно звернути увагу, насамперед у роботі з батьками (Найдьонова, 2019).

Як же мають діяти батьки в ситуації, коли їхня дитина стала жертвою шкільного булінгу?

1. Перш за все поставтеся до ситуації з розумінням і співпереживанням. Не потрібно тиснути на дитину, кричати на неї або сварити її за зниклі речі. Спробуйте завести з дитиною відверту розмову і переконати її в тому, що ви завжди будете на її боці, що ви її опора, допомога і захист у складних ситуаціях.

2. Уважно вислухайте дитину, не перебивайте її, не ставте забагато уточнювальних запитань. Не намагайтеся одразу стати «караючою рукою», оскільки одним із багатьох страхів дитини, пов’язаних із ситуацію булінгу, є те, що в школу прийдуть мама/тато і влаштують там скандал, а після цього її будуть ще більше «гнобити». Тому спочатку запитайте в дитини, якої лінії поведінки вона дотримується щодо кривдників, чому обрала саме таку стратегію, які в цієї стратегії сильні і слабкі сторони.

3. У процесі обговорення дитячої поведінки постарайтеся побільше дізнатися про всі інциденти булінгу, яких зазнавала дитина. Запитайте, чи є матеріальні докази – переписки, пости в соціальних мережах, відео тощо. Спробуйте отримати доступ до цих доказів.

4. Далі можуть бути два шляхи залагодження ситуації. Перший: ви зі своєю дитиною разом під час обговорення обмірковуєте, як вона може поводитися, щоб «перемогти» своїх кривдників. Розробляєте стратегію, навчаєте дитину різних психологічних прийомів і методів антибулінгу (Чаплінська, 2020). Спробуйте

підтримати свою дитину на шляху до подолання цієї небезпеки, навчіть її справлятися з проблемою самостійно, але маючи за спиною підтримку батьків. Такий шлях доцільно використовувати, якщо булінг має здебільшого психологічну природу. У разі фізичного чи економічного булінгу варто піти іншим шляхом і залучити до вирішення проблеми адміністрацію школи. За фактом булінгу потрібно буде звернутися в поліцію. І пам'ятайте – ні в якому разі не звинувачуйте свою дитину і не намагайтеся самостійно приборкати кривдників. Такі конфлікти мають вирішуватися або на рівні «дитина-дитина», або на рівні «дорослі-дорослі», але точно не на рівні «дорослі-діти».

Варто зазначити, що так само, як і в 2018 році, у 2020-му виявлено групу дітей, які вважають, що інтернет для них є абсолютно безпечним місцем, – 7,75% підлітків, а 6,08% запевняють, що вони особисто не стикалися із жодними небезпеками під час користування інтернетом. Ця група опитуваних особливо вразлива, оскільки ще не мала досвіду взаємодії з кіберзагрозами, що чатують на них в інтернеті, саме тому критичність їхнього мислення щодо такого роду небезпек може бути знижена.

Для того щоб сформувати більш чітку картину, під час дослідження 2020 року дітям було поставлено також додаткові запитання щодо окремих видів кіберзагроз (табл. 3).

Таблиця 3

Додаткові запитання для виявлення дитячих кіберризиків

Уточнювальні запитання	**Частка відповідей** *(у %)*
Чи ставали ви коли-небудь мішенню для ТРОЛІНГУ в соціальних мережах (для розваги інших людей)?	33.1
Чи були ви жертвою ШОКТРОЛУ – маси образливих постів, щоб викликати у вас гнів, розчарування чи принизити вас?	22.7
Чи сварилися ви в соцмережах (ФЛЕЙМІНГ), коли в запалі суперечки говорили те, чого б не сказали в спокійній розмові?	32.4
Чи стикалися ви зі СТАЛКІНГОМ – залякуванням, погрозами насильства, прихованим стеженням і переслідуванням?	22.2
Чи доводилося вам коли-небудь робити те, чого Ви не хотіли робити через онлайн-погрози та шантаж?	55.4
Чи потрапляли ви коли-небудь у ситуацію ХАКІНГУ – коли хтось без вашого дозволу брав під контроль ваші пристрої, отримував доступ до файлів, шпигував за пристроєм або контролював його?	35.3
Чи стикалися ви з КЕТФІШИНГОМ у соціальних мережах – обманом людей у стосунках шляхом створення фальшивих ідентифікацій (наприклад, акаунтів людей, яких насправді не існує)?	37.0
Чи були ви в ситуації СЛЕМІНГУ – підбурювання спостерігачів до кібербулінгу, де спостерігачі не були	23.9

ініціаторами бійки?	
Чи стикалися ви з тим, що вашу особисту інформацію (фото, відео, записи) поширювали в соціальних мережах без вашої згоди?	26.1
Чи ділилися ви коли-небудь своїми особистими фото/відео (які не хотіли б бачити на шкільному білборді) з іншими людьми (наприклад, на сайтах знайомств або в спеціальних програмах)?	28.6
Чи просили вас коли-небудь надіслати фотографії/відео особистого/інтимного характеру люди в мережі, з якими ви спілкувалися лише в інтернеті?	31.1
Чи стикалися ви із СЕКСТИНГОМ – текстовими повідомленнями чи коментарями на вашу адресу, які мали сексуальний характер?	50.2
Чи траплялися вам в інтернеті небажані зображення, які супроводжують сексуальну поведінку?	50.4
Чи стикалися ви з КІБЕРГРУМІНГОМ – коли незнайомі люди в мережі намагалися залучити вас і запросили на зустріч офлайн?	39.4

Як бачимо, рівень зіткнення дітей з різними видами кібернебезпек насправді дуже високий. Хоча підлітки можуть і не сприймати те, з чим вони стикаються в інтернеті, як кіберризики. Дуже часто вони не усвідомлюють небезпеку та її наслідки.

На жаль, після повномасштабного вторгнення Російської Федерації на територію України в лютому 2022 року повноцінні моніторинги та опитування щодо кіберзагроз дітей в інтернеті не проводилися, хоча можемо спрогнозувати, що загальна картина й окремі тенденції змінюються. Українські школярі в умовах воєнного часу можуть зіткнутися із значною кількістю фейкової інформації, вірусними кібератаками, зламом персональних акаунтів та крадіжкою конфіденційних даних (наприклад, розсилка електронних листів з темою «№ 1275 від 07.04.2022», відкриття яких призводило до отримання хакерами повного контролю над персональними комп'ютерами та загрожувало крадіжкою і пошкодженням комп'ютерних даних; або електронні листи під назвою «Військові злочинці РФ.htm», відкриття яких призводило до того, що зловмисники отримували віддалений доступ до комп'ютера жертви), ретингом (коли діти впевнені, що ведуть переписку зі своїми однолітками про бомбування рідних міст і знищення тих чи інших будівель, а насправді мимоволі видають ворогу інформацію про критичну інфраструктуру міста) тощо. Феномени кіберзагроз воєнного часу потребують глибокого і детального дослідження для формування стратегій кіберзахисту.

Так само, як дорослі застерігають дітей про небезпеку від відкритого вогню чи тонкого льоду на річці взимку, їм також слід пояснити, що не можна надсилати фотографії приватного чи інтимного характеру, навіть людям, яких вони вважають близькими друзями. Бо коли таке фото надсилається комусь, дитина втрачає над ним контроль. І вона вже ніяк не зможе вплинути на те, чи буде таке фото показане іншій особі або групі осіб без її дозволу. Такі фотографії можуть стати предметом шантажу

чи помсти, вони можуть стати загальнодоступними через розсилку або соціальні мережі. Страх перед невідомим, ганьбою, глузуванням, булінгом і покаранням може штовхати дитину на крайні міри через бажання уникнути цього – на суїцид.

Саме тому ми вважаємо за потрібне ввести до шкільної програми *новий предмет – кібербезпеку*, підготувати таким чином дітей до протистояння кіберризикам у дорослому віці. Під час таких занять дитина має здобути не тільки загальні знання про можливі інтернет-загрози – вона також має ознайомитися з особливостями схем та прийомів кіберзлочинців, напрацювати особисті правила безпеки і неухильно їх дотримуватися, сформувати належну психологічну стійкість і готовність справлятися з наслідками кіберзагроз.

У цьому контексті *кібербезпеку* можна визначити як набір знань користувача інтернет-мережі для захисту власних життєво важливих інтересів під час перебування в кіберпросторі, а також уміння нівелювати наслідки кіберзагроз.

Зазначимо, що технічні аспекти кібербезпеки часто розглядають у науковій літературі. Але підходів, які б описували психологічний складник, наразі бракує. Дитину потрібно навчати не тільки розуміти технічні особливості кібербезпеки, а й правильно оцінювати ризики. Наприклад, дорослий говорить дитині: «В інтернеті не можна переходити за сумнівними посиланнями, адже онлайн-ігри та програми можуть містити «віруси» або фішинг, тому для завантаження потрібних файлів слід використовувати тільки перевірені офіційні ресурси». У відповідь часто можна почути: «знаю». Однак такі знання є теоретичними, вони не підкріплені жодним конкретним досвідом чи візуальною історією, тому ви все ще можете знайти «ТРОЯНИ» чи інші вірусні програми, що працюють на планшетах чи комп'ютерах.

Принципи кібербезпеки потрібно пояснювати дітям на конкретних прикладах. Треба скласти з дітьми план дій на випадок, якщо вони зіткнуться з кібернебезпекою (чітко пояснити послідовність їхніх дій у ситуації зіткнення з тією чи тією кіберзагрозою в інтернеті). Дітям потрібно розповісти, до кого вони можуть звернутися по допомогу. Часом буває, що діти не хочуть або соромляться звертатися по допомогу до батьків, тому це може бути будь-хто з дорослих, кому дитина довіряє (брат, сестра, дідусь, бабуся, тітка, дядько, шкільний учитель, психолог тощо). Також дітям потрібно розповісти про кіберполіцію і закони, пов'язані з кіберзлочинами та покаранням за них.

Пропонований навчальний посібник спрямований на підготовку вчителів до роботи за темою кібербезпеки як у мирний, так і у воєнний час. Використання педагогами представлених тут матеріалів для підготовки занять з дітьми з означеної теми дасть змогу:

- сформувати у дітей загальне уявлення про кіберризики і кібернебезпеки як мирного, так і воєнного життя;
- пояснити їм різницю між кіберризиком, кіберзлочином, кібертероризмом і кібервійною;
- ознайомити дітей з особливостями юридичної системи України в контексті кібербезпеки;
- забезпечити належну психологічну підготовку дітей до протистояння кіберризикам.

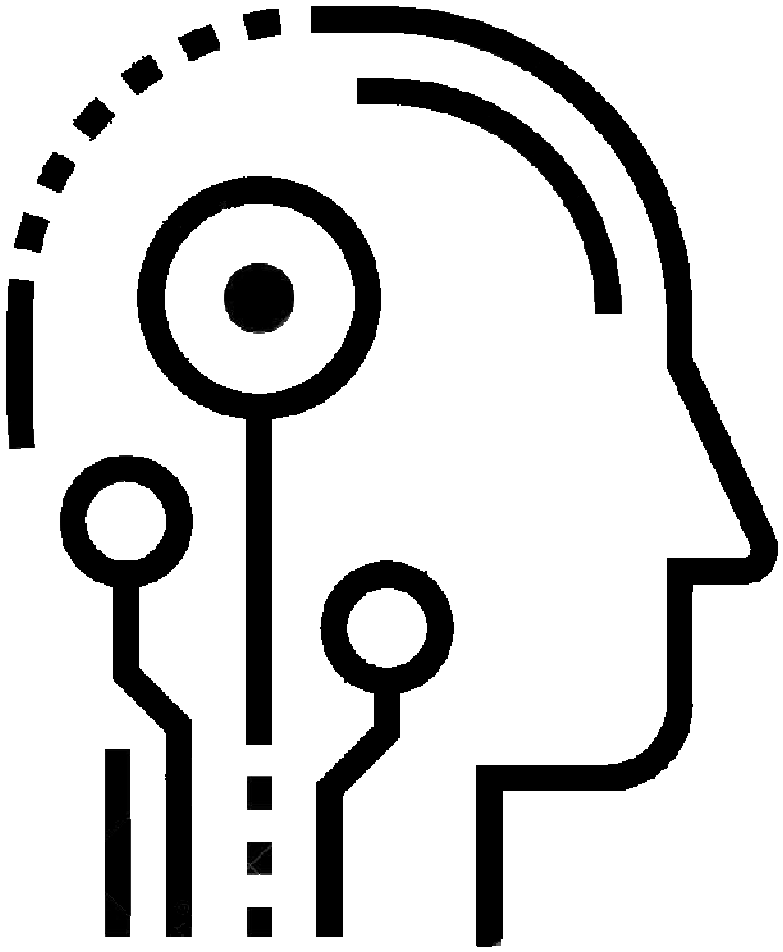
Посібник складається із вступу, теоретичної частини і п'яти психологічних практикумів, а також додатків і списку використаної літератури.

У теоретичній частині представлено два підрозділи. У першому розкрито понятійний апарат кіберзагроз і детально розглянуто такі поняття, як-от: кіберризики, їхні види та наслідки кожного з них; кібератаки і кіберінциденти; кіберзлочини і їхня

відмінність від звичайних злочинів; кібертероризм, його видові особливості та прояви, а також кібервійна і її відмінності від інформаційної війни. Другий підрозділ акцентує на кібербезпеці загалом (індивідуальний, організаційний/груповий і державний рівні) та її юридичних аспектах у принципі. Представлено поняття воєнної кібербезпеки в її ключових моментах (безпека мобільних пристроїв, двохетапна аутентифікація, програмне забезпечення, безпека соціальних мереж, неправдиві повідомлення, або фейки, сумнівні сайти і посилання), а також обґрунтовано важливість сімейних правил кібербезпеки. Окрему увагу зосереджено на діяльності кіберполіції в Україні як у воєнний, так і в мирний час. Наведено опис нормативних документів, які регулюють кібербезпеку в Україні і у світі загалом. Також розписано алгоритм дій у тому випадку, якщо дитина стала жертвою кіберзлочинця, з використанням психологічних технік та авторську техніку «Наслідки кіберзлочину і Я».

Друга частина посібника містить п’ять практичних занять, спрямованих на закріплення матеріалу, представленого в теоретичній частині. Перший практикум ґрунтується на авторській методиці «Ландшафтна мапа потенційних кіберзагроз», основна мета якого – створення у свідомості дітей цілісного образу кіберзагроз, з якими вони можуть зіткнутися в інтернет-просторі (як у мирний, так і у воєнний час). Другий практикум представлено у форматі дискусійного клубу або дебатів, він має на меті допомогти учням розвинути навички логічної і послідовної аргументації в публічних виступах, уміння слухати й відстоювати власну позиції у взаємодії з іншими людьми, а також поглибити знання щодо психологічних особливостей кіберсоціалізації особистості або особливостей воєнної кібербезпеки (на вибір). Третій практикум, де використовується авторська методика «Тотемний кіберїжак», покликаний допомогти у формуванні сімейних правил кібербезпеки та алгоритмів дії для всіх членів сім’ї (або трудового колективу) в небезпечних ситуаціях. Темою четвертого практикуму є розвінчування фейків (що особливо актуально у воєнний час). Основна його мета – ознайомити дітей із схемою створення фейкових повідомлень та новин під час війни, навчити їх розпізнавати дезінформацію за ключовими показниками. П’ятий практикум, а саме судові кейси, має ознайомити дітей з юридичним компонентом кібербезпеки. Завдяки цьому практикуму діти навчаться співвідносити статті українських законів із реально вчиненими кіберзлочинами та дізнаються, які наслідки і варіанти покарання за різні види правопорушень можуть очікувати кіберзлочинців.

ЧАСТИНА І



1.1. ВІД КІБЕРРИЗИКУ ДО КІБЕРВІЙНИ

КІБЕРРИЗИК

Що таке кіберризики?

Кіберризик можна розглядати передусім як загрозу, пов’язану з інтернет-активністю користувачів, як з технологічними, так і психологічними її аспектами, а також зберіганням персональних даних. З погляду інформаційної безпеки кіберризик – це втрати, яких може зазнати користувач інтернет-мережі через порушення конфіденційності, цілісності або доступності інформаційних ресурсів чи персональних даних. У подальшому поняття кіберризику і кіберзагрози ми будемо використовувати як синонімічні.

Одним із інструментів реалізації кіберризику є *кібератака*. Під цим поняттям розуміють дії кіберзловмисників (хакерів) або шкідливих програм, спрямованих на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами комп'ютера або на виведення системи з ладу (Хакерська атака, 2022).

Другою формою реалізації кіберризиків є *кіберінциденти*. Цим терміном позначають подію або кілька несприятливих подій навмисного характеру, що мають ознаки кібератаки та становлять загрозу для безпеки систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (зокрема зриву та/або блокування роботи системи, несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів (Про основні засади забезпечення кібербезпеки України, 2017).

Є більш складні форми кіберризиків, а саме *кібертероризм* і *кібервійна*, але про них ми більш детально поговоримо пізніше. Ключовий критерій поділу на зазначені форми – мотивація кібервтручання та механізм його впливу на інформаційні системи.

Які є види кіберризиків?

Цільові атаки – коли кіберзлочинці обирають конкретну жертву (людину/організацію), збирають про неї інформацію, а потім здійснюють кібератаку, що базується на використанні та аналізі зібраної інформації (фінансове шахрайство, викрадення баз даних, промислове шпигунство, DDoS-атаки, вимагання).

Нецільові атаки – коли кіберзлочинці працюють відповідно до розробленої злочинної схеми, спираючись на підготовлені скрипти, які використовують у взаємодії з усіма жертвами. Передбачає неперсоналізований підхід (фішинг, кардинг, смс-шахрайство).

Внутрішні атаки – коли кіберзлочинці є частиною організації або заручаються підтримкою когось, хто є працівником цієї організації, і намагаюся заради власної вигоди отримати, змінити або знищити конфіденційну інформацію (викрадення, сприяння цільовим атакам тощо).

Зовнішні атаки – коли кіберзлочинці готуються до скоєння кіберзлочину, збирають інформацію про організацію, на яку хочуть влаштувати кібератаку, але не є частиною цієї організації і не мають підтримки її співробітників.

Якими можуть бути наслідки?

Фінансові втрати (наприклад, у результаті фішингової атаки, коли зловмисники отримали доступи і паролі до вашої банківської картки);

часові втрати (наприклад, якщо через вірусне блокування комп'ютера ви не зможете зробити потрібну роботу);

репутаційні втрати (наприклад, через викрадення і поширення персональної інформації);

психологічні травми (наприклад, тотальна недовіра до людей через шахрайські дії злочинців в інтернеті);

загроза життю і здоров'ю людей (якщо кібератака, наприклад, здійснювалася на лікарню, аеропорт тощо);

порушення законодавства/контрактів.

Варто зазначити, що сьогодні будь-який політичний або військовий конфлікт у світі завжди супроводжується організованим протиборством в інтернет-мережі. Наприклад, у 2005 році Японією прокотилася хвиля кібератак, каталізатором якої став вихід шкільного підручника з історії. У цьому підручнику спотворювалися історичні події, що відбувалися в Китаї протягом 1930–1940 років XX ст. У ньому, зокрема, замовчувалися воєнні злочини японських військ під час інтервенції. У списку сайтів, що зазнали хакерських атак, були японські міністерства та установи, сайти найбільших японських корпорацій та сайти, присвячені Другій світовій війні. До речі, китайські хакери продемонструвати високий рівень організованості та синхронності під час цієї масової атаки. З огляду на наявність у Китаї державного контролю за інтернетом можна припустити, що цю атаку було санкціоновано державою (Дзюндзюк, & Дзюндзюк, 2013).

КІБЕРЗЛОЧИН

Поширення нових інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та засобів комунікації, сформувало єдиний світовий інформаційний простір, де кожен може отримати доступ до будь-якої інформації з різних куточків планети, дистанційно керувати бізнесом, здійснювати управління власними активами, укладати угоди без особистого контакту тощо. Водночас інформаційний простір став місцем і безпосередньо інструментом злочину. Віднині злочинцю не потрібно попередньо «обробляти клієнта» і мати особистий контакт з потенційною жертвою. Головним інструментом злочину стає комп'ютер із доступом до інформаційно-комунікаційних систем, де за допомогою комп'ютерних вірусів та інших протизаконних технічних засобів злочинець отримує доступ до баз даних, банківських рахунків, автоматизованих систем управління. Так, крадіжки даних платіжних карт (банківських рахунків) або даних доступу до системи інтернет-банкінгу з метою заволодіння коштами клієнтів банку, викрадення персональних даних та комерційної інформації з приватних комп'ютерів або серверів, умисне пошкодження роботи інформаційних систем або засобів комунікацій для завдання збитків компаніям, DDoS атаки на інтернет-ресурси – це далеко не повний перелік таких загроз, які несе із собою бурхливий розвиток сучасних інформаційних технологій, і, відповідно, виокремлюється в таке поняття, як кіберзлочинність (Типологія легалізації (відмивання) доходів, одержаних злочинним шляхом, 2013).

Що таке кіберзлочин?

Кіберзлочинність (cybercrime) – це злочинність, у віртуальному просторі за допомогою інформаційних технологій. А *кіберзлочин* – це суспільно небезпечне діяння, що скоюється в кіберпросторі за допомогою комп'ютерних технологій і глобальних мереж (Про основні засади забезпечення кібербезпеки України, 2017).

Кіберзлочинність набуває все більшого світового масштабу, новітні технології перетворюють реальних злочинців на анонімних, а легкість швидкого збагачення провокує появу все нових і нових видів кіберзлочинної діяльності.

Саме поняття *кіберзлочинність* можна визначити як протиправні дії особи або групи осіб у кібернетичному просторі (Бабенко, & Мокляк, 2018).

Якими бувають кіберзлочини?

23 листопада 2001 року в Будапешті (Угорщина) було укладено *Конвенцію Ради Європи про злочинність у кіберпросторі* (далі – *Будапештська конвенція*). Ця конвенція є фундаментом для розроблення законодавства у сфері боротьби з кіберзлочинами як для кожної країни окремо, так і для загальносвітового законодавства. Вона також класифікує кіберзлочини. Оскільки наразі є багато різновидів таких злочинів, їх для зручності можна поділити на групи.

У *першу групу* виділено злочини проти конфіденційності, цілісності та доступності комп`ютерних даних і систем, зокрема незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему тощо.

До *другої групи* віднесено злочини, пов'язані з використанням комп`ютера як засобу скоєння злочинів, а саме як засобу маніпулювання інформацією. У цій групі, зокрема, комп`ютерне шахрайство і комп`ютерне підроблення.

Третю групу складають злочини, пов`язані з контентом (змістом даних, розміщених у комп`ютерних мережах). Найпоширенішим прикладом цих кіберзлочинів є злочини, пов`язані з дитячою порнографією.

У *четвертій групі* – злочини, пов`язані з порушенням авторського права і суміжних прав.

*П`яту групу* злочинів об'єднано в окремий протокол. Це, зокрема, акти расизму і ксенофобії, вчинені за допомогою комп`ютерних мереж.

Є ще одна категорія злочинів, не включена до Конвенції Ради Європи (вона набула поширення вже після ухвалення Конвенції). Ідеться про *identity theft* – викрадення, передавання та використання персональних даних з метою скоєння злочинів (Номоконов, & Тропина, 2013).

За об`єктом посягання виділяють такі групи кіберзлочинів:

1) злочини проти конфіденційності, цілісності та доступності комп`ютерних даних і комп`ютерних мереж;

2) економічні кіберзлочини;

3) кіберзлочини проти особистих прав і недоторканності приватної сфери;

4) кіберзлочини проти суспільних і державних інтересів.

Водночас є велика кількість кіберзлочинів, що зазіхають на декілька об'єктів.

Чим кіберзлочин відрізняється від звичайного злочину?

По-перше, здійснення кіберзлочину вимагає від злочинців наявності спеціальних технічних знань. Крім того, хакерська субкультура, у середовищі якої формується більшість кіберзлочинців, стимулює інтелектуальний розвиток. Але на відміну від інших інтелектуальних кримінальних правопорушень кіберзлочини доступні для людей пересічних соціальних і вікових можливостей, досить мати доступ до інтернету і комп'ютер.

По-друге, більшість кіберзлочинів анонімні і неперсоніфіковані – механізми ідентифікації глобальної мережі дають злочинцю змогу здійснювати операції анонімно або видавати себе за іншу особу, змінювати біографічні дані або соціальний статус.

По-третє, кіберзлочини відбуваються віддалено. Злочинця і жертву можуть розділяти від десятка до тисячі кілометрів, але відчуття цих меж нівелює інтернет-

мережа. Тому кіберзлочин не вимагає фізичного зближення жертви і суб'єкта злочину в момент учинення такого.

По-четверте, кіберзлочини часто латентні (від лат. latentis – прихований, невидимий). Жертви кіберзлочинців часто не заявляють у поліцію, оскільки збитки від кіберзлочину їм здаються меншим злом, ніж час, витрачений на процедуру розслідування, яка не гарантує притягнення до відповідальності винного чи компенсації збитків. Також жертви можуть не заявляти в поліцію, оскільки кіберзлочин може бути пов'язаний із викраденням персональної інформації і його оприлюднення може завдати репутаційних збитків (Дзюндзюк, & Дзюндзюк, 2013).

Через анонімність, широту покриття та латентність шансів бути виявленим у кіберзлочинця набагато менше, ніж у грабіжника банку. І навіть у разі затримання у нього менше шансів бути притягнутим до кримінальної відповідальності, оскільки законодавство щодо кіберзлочинців усе ще є недосконалим.

КІБЕРТЕРОРИЗМ

Що таке кібертероризм?

Під *кібертероризмом* (комп'ютерним тероризмом) розуміють умисну, політично вмотивовану атаку на інформацію, яка обробляється комп'ютером, комп'ютерну систему і мережі, що створює небезпеку для життя і здоров'я людей або настання інших тяжких наслідків, якщо такі дії було скоєно з метою порушення суспільної безпеки, залякування населення, провокування військового конфлікту (Пилипчук, & Дзьобань, 2011).

Цілі кібертероризму збігаються з цілями і мотивами здійснення всіх відомих видів терористичних дій, а саме: порушення суспільної і державної безпеки; залякування населення; провокування військового конфлікту; ускладнення міжнародних відносин; вплив на ухвалення рішень або здійснення (нездійснення) дій органами державної влади та місцевого самоврядування, посадовими особами цих органів, об'єднаннями громадян, юридичними особами; привертання уваги громадськості до певних політичних, релігійних та інших поглядів.

Кібертероризм передбачає інформаційні атаки на обчислювальні центри, центри управління військовими мережами й медичними закладами, банківські та інші фінансові мережі, засоби передавання даних за допомогою комп'ютерних мереж. Він може здійснюватися з метою саботажу (урядових установ), заподіяння економічних збитків (великим промисловим корпораціям), дезорганізації праці з потенційною можливістю смертей. Інформаційна атака на комп'ютерну інформацію, обчислювальні системи, апаратуру для передавання даних, інші складники інформаційної інфраструктури, що здійснюється терористичними угрупованнями або окремими особами, є основною кібертероризму. Така атака дає змогу проникати в систему, перехоплювати управління або пригнічувати засоби інформаційного обміну в мережі, чинити інші деструктивні впливи (Бутузов, & Тітуніна, 2007).

Яких форм може набувати кібертероризм?

Дослідниця з проблем тероризму В. П. Журавльова вважає, що кібертероризм проявляється у двох формах:

перша – це комп'ютерні економічні злочини, які вчиняються за допомогою спеціалістів-хакерів. Серед таких злочинів:

- махінації та маніпулювання системами обробки даних (несанкціонований переказ грошей та їх використання);

●шпигунство (проникнення до конфіденційних каналів зв'язку державних органів для отримання інформації, шпигунство з метою отримання інформації щодо закритих технологій);

●диверсія (завдання шкоди технічному та програмному забезпеченню через віруси, які порушують функціонування державних органів та інших установ);

●незаконне користування комп'ютерними послугами (несанкціоноване використання програм, купівля коштом інших тощо);

друга форма – розголошення таємниці, тобто незаконне отримання комерційної та конфіденційної інформації (цей злочин нерозривно пов'язаний із злочинами першого виду). Ідеться про:

●несанкціоноване отримання інформації для нецільового її використання особами, які не мають для цього відповідного доступу;

●незаконне збирання і переховування інформації;

●порушення правил користування конфіденційною інформацією (Журавльов, Романюк, & Коваленко, 2003).

Чим кібертероризм відрізняється від звичайного тероризму?

Тактика і прийоми, що використовуються для вчинення цього злочину, відрізняються від тактики і прийомів учинення класичних комп'ютерних злочинів тим, що комп'ютерний терористичний акт повинен мати небезпечні наслідки, стати широковідомим населенню й мати великий суспільний резонанс. Від комп'ютерних злочинів кібертероризм відрізняється насамперед своїми цілями, властивими тероризму загалом: дії завжди мають публічний характер і спрямовані на вплив, що здійснюється щодо окремих осіб, суспільства чи влади. Від традиційного тероризму (політики залякування, пригнічення супротивників учиненням актів насильства) він відрізняється засобами здійснення, а також своєю анонімністю і знеособленістю.

Збитки від терористичної операції суттєво збільшуються в разі залучення засобів масової інформації (варіант, що вже практикується в глобальному інформаційному суспільстві). Роль ЗМІ в такому разі можуть виконувати телебачення та інтернет. Унаслідок цього рівень впливу терористичної операції суттєво зростає. Отже, у терористів з'являється потенційна можливість впливати на зміст інформації про теракт, використовуючи контрольовані джерела інформації, під'єднані до ЗМІ. Цю роль можуть виконувати розроблені в мережі інтернет-сайти (щоб легалізувати інформацію, офіційні ЗМІ посилаються на такі сайти). Тому негативні наслідки терористичної операції щодо системи, на яку здійснюється атака, значно зростають (Бутузов, & Тітуніна, 2007).

КІБЕРВІЙНА

Що таке кібервійна?

Річард А. Кларк у книзі «Кібервійна» (англ. *Cyber Warfare*) визначив це поняття як «дії однієї національної держави з проникнення в комп'ютери або мережі іншої національної держави для завдання збитків або руйнування» (Clarke, & Knake, 2011).

Основні риси кібервоєн, що відрізняють їх від інших типів військових дій:

●високий рівень анонімності;

●невизначений час початку;

●непомітність слідів втручання;

●невираженість таких визначень, як «фронт», «тил»;

● глобальне охоплення;

● непомітність атак для звичайних користувачів;

Наразі загальне управління глобальною мережею Інтернет здійснює ICANN (Internet Corporation for Assigned Names and Numbers) і регулювання відбувається в парадигмі «один світ – один Інтернет». За такого підходу ICANN заперечує право держав регулювати і нести відповідальність за певний сегмент глобальної мережі Інтернет. Де-факто Інтернет та інші мережі мають наднаціональний характер, а бойові дії в кіберпросторі спрямовані на певні національні держави і їхні структури. Наразі склалася ситуація, коли не можуть діяти ніякі юридичні погоджувальні механізми профілактики та запобігання кібервійнам. Отже, кібервійни є особливо небезпечними, тому що легко розв'язуються і практично не регулюються (Горбенко, 2021а).

Кібервійни напряму пов'язані з кібершпіонажем, кіберзлочинністю і кібертероризмом.

Є також поняття інформаційної війни, яке, утім, не тотожне поняттю «кібервійна».

Що таке інформаційна війна?

Інформаційна війна – це міждержавне протиборство в інформаційному просторі з метою завдання збитків інформаційним системам, підриву політичної та соціальної системи, а також масованої психологічної обробки населення для дестабілізації суспільства і держави. Інструментами інформаційної війни є насамперед психологічний вплив, дезінформація, PR-кампанії та спеціальні інформаційні операції (Горбенко, 2021а).

Більш чіткий поділ між інформаційними війнами і кібервійнами означився приблизно 15 років тому у зв'язку з революційними змінами в кібертехнологіях.

У чому різниця між інформаційною війною і кібервійною?

Інформаційні і кібервійни відрізняються об'єктами і засобами дії. Інформаційні війни є контентними війнами, що мають на меті зміну масової, групової та індивідуальної свідомості, нав'язування власної волі противнику та перепрограмування його поведінки. Під час інформаційної війни йде боротьба за свідомість, цінності, переконання, шаблони поведінки тощо. Інформаційні війни виникли тисячоліття тому, а інтернет підняв їх на новий рівень інтенсивності, масштабності та ефективності.

Об'єктами впливу інформаційних війн є різноманітні суб'єкти – від невеликих груп громадян до цілих народів і націй, населення держав. Засобом впливу є спеціально підготовлені семантичні повідомлення у вигляді текстів, відео та аудіоматеріалів.

Кібервійни – це цілеспрямований деструктивний вплив інформаційних потоків у вигляді програмних кодів на матеріальні об'єкти та їхні системи, їх руйнування, порушення функціонування або перехоплення керування ними.

Об'єктами впливу кібервійни є виробничі структури, інфраструктури соціального, військового та фінансового призначення, роботизовані і високоавтоматизовані виробничі й технологічні лінії. Основний тип засобів бойового впливу в кібервійнах – певний програмний код, який порушує роботу, виводить з робочого стану або забезпечує перехоплення керування різного роду матеріальними об'єктами та мережами, що мають в оснащенні електронні системи керування.

Інформаційні війни і кібервійни – це два різновиди війн, які здебільшого ведуться через комп'ютерні мережі: глобальну мережу Інтернет, закриті державні, військові, корпоративні і приватні мережі. У кожного із цих двох типів війн свої інструментарії, методи, стратегії і тактики ведення дій, закономірності ескалації, можливості запобігання тощо (Горбенко, 2021b; Ranger, 2017).

1.2. КІБЕРБЕЗПЕКА І КІБЕРКУЛЬТУРА

Один із ключових аспектів життя людини в інформаційну добу – кібербезпека. Смартфони, соціальні мережі та інші онлайн-сервіси несуть на собі «інформаційний відбиток» користувача і, відповідно, містять багато особистої інформації. Інколи навіть більше, ніж думають люди. За такої умови облікові записи на онлайн-серверах можуть бути значно вразливішими для атак зловмисників, ніж людина в реальному житті. Тому вся електронна інформація, сервіси і пристрої потребують захисту й дотримання певних правил безпеки (Баранова, 2014).

Закон України «Про основні засади забезпечення кібербезпеки України» визначає *кібербезпеку* як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави під час використання кіберпростору, що забезпечує сталий розвиток інформаційного суспільства і цифрового комунікативного середовища, своєчасне виявлення й нейтралізацію реальних і потенційних загроз державній безпеці в кіберпросторі, запобігання цим загрозам (Газізова, 2022).

Кібербезпека може реалізовуватися на різних рівнях: державному, груповому/організаційному (шкільні або трудові колективи) та індивідуальному.

ІНДИВІДУАЛЬНА БЕЗПЕКА

Для забезпечення індивідуальної безпеки в кіберпросторі, тобто щоб не стати жертвою кіберзлочинців, потрібно не лише дотримуватися загальновідомих правил, а ще й розробити такі, які будуть прийнятними для кожної дитини. Оскільки у кожної дитини є свій характер і для когось «ок» – слухатися батьків, а хтось може влаштовувати бунт на будь-яке «не можна», навіть не задумуючись про необхідність такої заборони заради життя, психологічної та фізичної безпеки. Тому ми радимо обговорити з дітьми правила загальної безпеки та виробити щонайменше п'ять головних, які мають діяти в будь-яких ситуаціях, незважаючи на обставини.

Дорослим слід пам'ятати, що про кібербезпеку потрібно починати говорити з дитиною з того віку, коли вона дістає доступ до гаджетів. У когось дитина вже у два роки активно користується планшетом чи батьківським смартфоном, а для когось дорога у світ безмежного інтернету розпочинається в сім років, коли дитина йде до школи і батьки, бажаючи постійно бути з нею на зв'язку, дарують гаджет.

Для маленьких дітей правила сімейної кібербезпеки можуть бути досить простими. Головне, щоб дитина розуміла загальну логіку. Наприклад:

●Гаджет є лише пристроєм, на іншому кінці якого – людина, і ти завжди спілкуєшся з людьми, не з пристроями, хоча й з їхньою допомогою. Тому не забувай бути чемним і ввічливим – так, ніби спілкуєшся з кимось особисто. Також пам'ятай, що на іншому боці екрана може бути хто завгодно, навіть якщо тобі пише хтось, хто здається знайомим або із знайомого акаунта. На жаль, у соціальних мережах немає подвійної аутентифікації, щоб завжди і на всі 100 відсотків бути впевненим, що спілкуєшся із своїм знайомим.

●Коли ти розміщуєш щось в інтернеті чи відправляєш у повідомленні, ця інформація автоматично перестає бути твоєю. І не дивуйся, якщо випадково дізнаєшся, що твоє особисте фото бачив (-ла) не тільки найкращий (-а) друг (подруга), а і його (її) сестра/брат, мама, знайомий знайомого і т. ін. На жаль, однією з найактуальніших проблем мережі Інтернет є конфіденційність даних.

●Усе, що ти отримав, але не очікував отримати, має викликати підозру. Тебе можуть обманути. Тому краще не реагувати на підозрілі листи, не відкривати незрозумілі файли. Безкоштовний сир – лише в мишоловці. Гроші також із неба не падають. Тому якщо хтось тобі пропонує гроші або якусь дрібницю просто так, будь ласка, не ведися на це! Якщо в тебе є потреба в грошах, краще скажи про це дорослим, яким довіряєш.

●Якщо ти сумніваєшся в якісь інформації або діях у мережі Інтернет, краще проконсультуйся із дорослим, якому довіряєш.

●У зв'язку з воєнною ситуацією в нашій країні є певні сайти і домени, які наразі заборонені, оскільки вони становлять небезпеку для нашої країни, тому не можна натискати клавіші або переходити за посиланнями на сайти з доменом «.ru»/« рф» і .su.

Для більш дорослих дітей правила можуть бути дещо розширеними і представленими в більш схематичному вигляді. Наприклад:

●Не повідомляй нікому (особливо незнайомцям у мережі Інтернет) особисту інформацію: домашню адресу, номер домашнього телефону, робочу адресу батьків, їхній номер телефону, назву та адресу школи. Також цю інформацію краще не постити в соціальних мережах, оскільки нею можуть скористатися кіберзлочинці. У разі потреби ти можеш запитати у батьків дозволу на розголошення такої інформації.

●Якщо ти раптом натрапиш в інтернеті на якусь інформацію, яка тебе збентежить чи/або викличе в тебе внутрішнє занепокоєння, підозру, поговори про це з дорослими, яким довіряєш.

●Ніколи не погоджуйтеся на зустріч з кимось, із ким ти познайомився (-лась) в інтернеті, без додаткового страхування у вигляді дорослого поряд. Краще на такі зустрічі спочатку запитати дозвіл у батьків. Перша зустріч з інтернет-другом має відбутися в людному місці, у денний час і в присутності когось із знайомих дорослих. Не обов'язково, щоб дорослий тримав тебе за руку, – просто щоб був десь поруч і міг переконатися, що в тебе все добре і на зустріч справді прийшов твій друг-одноліток, а не якийсь злочинець.

●Не надсилай фотографії чи іншу інформацію про себе людям, з ким ти не знайомий (-ма) особисто. Особливо це правило стосується інтимних (або напівоголених, наприклад у купальнику) фотографій. Також ніколи, за жодних обставин, умовлянь чи тиску з боку іншої людини не оголюй своє тіло або його частину на вебкамеру.

●Не відповідай на грубощі чи погрози в інтернет-мережі. Якщо ти отримаєш такі листи або повідомлення, то скажи про це дорослим і разом порадьтеся, як краще відповісти на грубість, щоб м'яко звести конфронтацію на нуль. Якщо ти отримуєш СПАМ-листи чи листи з погрозами, то обов'язково повідом про це дорослих. Разом ви можете звернутися до компанії, яка надає послуги інтернету, щоб заблокувати отримання таких листів, або до кіберполіції для юридичного врегулювання цієї проблеми.

●Не довіряй свої паролі нікому, навіть найближчим друзям. Пам'ятай, що електронні пристрої зберігають значну кількість персональної інформації. Ця інформація має бути захищеною. Використовуй складні паролі для захисту телефона, планшета чи ноутбука. Можеш просто відвернутися від інших людей, коли вводиш пароль. Відстоюй своє право на конфіденційність.

●Не роби незаконних дій в інтернеті, оскільки навіть для неповнолітніх злочинців передбачено різні види покарань.

●Уникай аморальних сайтів (навіть якщо друзі підбурюють твою цікавість), оскільки на них, крім забороненого контакту, часто можна підхопити різноманітні віруси.

Такі сімейні правила виховують у дитини кіберкультуру; навчають, як вона має поводитися в мережі Інтернет; що вона може, а чого не може робити. Так само як у сімейному колі потрібно приділяти час питанням культури і дотриманню правил поведінки, так само ці аспекти життя мають підкріплюватися і в закладах освіти.

ГРУПОВА/ОРГАНІЗАЦІЙНА БЕЗПЕКА

(Кібербезпека в закладах освіти)

Організаційна безпека, або безпека в трудових колективах чи безпосередньо у вашому закладі освіти, важлива і складна річ, оскільки вона має централізовано створити та впровадити загальні для всіх учасників процесу правила кібербезпеки. А також стежити за їх виконанням і з'ясовувати причини та наслідки їх недотримання.

У складні для України часи вважаємо вкрай потрібним приділяти особливу увагу заходам кібербезпеки в закладах освіти. Учасники освітнього процесу мають бути попереджені про небезпеки, з якими вони можуть зіткнутися в мережі Інтернет, – і не тільки про ті, що були поширені в мирний час, а й про ті, що виникли разом з воєнною агресією з боку Російської Федерації. Ми можемо говорити про те, що з'явилися нові, воєнні, кіберзагрози: трансформувалися, наприклад, форми кібершахрайства, значною мірою зросла їхня інтенсивність.

У кожному освітньому закладі сьогодні повинні бути інструкції щодо того, як і на які теми можна спілкуватися із сторонніми особами щодо персональних даних, яку інформацію можна надавати службі технічної підтримки, як і яку інформацію може повідомити учасник освітнього процесу стороннім особам і працівникам масмедіа. Узагальнивши найважливіші підходи до дотримання заходів кібербезпеки в закладах освіти, Валерій Биков з колегами склали перелік правил для захисту суб'єктів освітнього процесу.

1. *Призначені для користувача облікові дані є власністю закладу освіти.* Усім працівникам у день прийому на роботу має бути роз'яснено, що ті логіни і паролі, які їм видали, не можна використовувати в інших цілях (на вебсайтах, для особистої пошти тощо), передавати третім особам або іншим працівникам, які не мають на це права.

2. *Потрібно проводити вступні і регулярні заняття* для працівників та учнів, *спрямовані на підвищення рівня знань з інформаційної безпеки*.

3. *Обов'язковими мають бути регламент з безпеки, а також інструкції,* до яких користувач завжди міг би мати доступ. В інструкціях мають бути описані дії учасників освітнього процесу в разі виникнення тієї чи іншої ситуації.

4. Комп'ютери користувачів *завжди повинні мати актуальне антивірусне програмне забезпечення*.

5. У корпоративній мережі закладу освіти або об'єднання освітніх закладів *необхідно використовувати системи виявлення атак та запобігання таким атакам*. Потрібно також використовувати системи запобігання витоку конфіденційної інформації. Усе це дасть змогу знизити ризик виникнення фішингових атак.

6. *Потрібно бути пильним щодо ресурсу, який запитує конфіденційні дані*.

7. *Ніколи не слід відкривати вміст додатків або переходити за посиланням, не вивчивши всіх деталей*. Часто адреса відправника містить помилки в назвах, а посилання мають неправдоподібний вигляд (Биков, Буров, & Дементієвська, 2019).

Протягом останніх кількох років в Україні тема безпеки дітей в інтернеті набула неабиякої актуальності, що, відповідно, створює попит на якісні ресурси для навчання і здобування додаткових знань з теми кібербезпеки. Наприклад, онлайн-курс «Основи кібербезпеки для школярів», створений CRDF Global в Україні у співпраці з ГО «Смарт Освіта» і Technomatix; сайт «Онляндія: моя безпечна вебкраїна» з матеріалами для дітей, батьків і вчителів; блог «Хакер, що біжить», який веде експерт із кібербезпеки Володимир Стиран; серіал для батьків «Безпека дітей в інтернеті» 2020 року від Міністерства освіти і науки України тощо. На нашу думку, незважаючи на наявність матеріалів у відкритому доступі, заклади освіти приділяють усе ще недостатньо уваги тематиці кіберзагроз і кібербезпеки. Цілком очевидною є наразі потреба не тільки в гуртках чи факультативних заняттях, а і в якісній навчальній програмі для середньої і старшої школи з теми «Кібербезпека».

ДЕРЖАВНА БЕЗПЕКА

Людство нині живе в епоху інформаційного суспільства, коли інформаційні технології і телекомунікаційні системи охоплюють усі сфери життєдіяльності людини, держави. Але таке повсюдне проростання телекомунікації і глобальної комп'ютеризації в людське життя може призвести до серйозних наслідків. На жаль, жертвами хакерів і кіберзлочинців можуть ставати не лише люди, а й цілі держави.

У 2014 році Російська Федерація розв'язала проти України *гібридну війну*, коли країна-агресор може залишатися публічно непричетною до такого конфлікту і проводити приховані військові операції. Гібридна війна являє собою як ведення воєнних дій під прикриттям незаконних (неформальних) збройних формувань, так і одночасне використання широкого спектра політичних, економічних (енергетичних і торговельно-економічних), а також інформаційно-пропагандистських заходів. Під час цієї війни Росія постійно проводила кібернетичні операції проти об'єктів критичної інфраструктури, приватного сектору, а також інформаційно-телекомунікаційних систем Збройних сил України. Одним з останніх прикладів проведення простої, але водночас широкомасштабної розвідувальної кібероперації, спрямованої на приватний сектор, може бути BugDrop. Її метою було отримання віддаленого доступу до персональних комп'ютерів, ноутбуків, смартфонів, планшетів та інших гаджетів працівників різних структур, унаслідок чого персональні дані та паролі працівників об'єктів критичної інфраструктури, засобів масової інформації й наукових установ викрадалися й завантажувалися на файлообмінник Dropbox. Доступ до комп'ютерів зловмисники отримували, розсилаючи користувачам фішингові електронні листи, у яких закликали відкрити файл Microsoft Word, що містив шкідливий макрос. Так, одним натиском клавіші людина може поставити під небезпеку не лише свої дані, а й дані, які в разі втрати несуть велику небезпеку для держави загалом (Міністерство оборони України, 2018).

А в лютому 2022 року Російська Федерація завдала вже відкритого удару по території України, що перевело збройний конфлікт у нову фазу. За цих обставин методи злочинних кібероперацій трансформувалися і набули неймовірних масштабів. Перш за все це стосується розсилання на електронні адреси і через соціальні мережі інформації пропагандистського характеру, фейкових новин для просування вигідних для ворога наративів та дезорієнтації населення. Також це може бути хакерський злам

приватних сторінок або серверів баз даних для збирання цінної інформації та її заміни на інформацію, корисну супротивній стороні. У цьому разі дезінформація та викрадення даних, наприклад відомостей щодо об'єктів критичної інфраструктури чи пересування українських військових у районах ведення бойових дій, можуть призвести до людських втрат. Кібератаки на об'єкти критичної інфраструктури – це атаки на комп'ютери і системи, що забезпечують життєдіяльність міст, а саме: системи водопостачання, електропостачання, транспорту тощо. Коли такі кібератаки дістали відсіч з боку українських спеціалістів з кібербезпеки, ворог почав цілеспрямоване бомбардування, ракетні обстріли. Також це можуть бути цілеспрямовані атаки на бази даних чи сервери або втручання в роботу обладнання, що забезпечує, наприклад, роботу комунікаційних військових систем. У таких випадках втрачається зв'язок, а значить і можливість управління діями підрозділів (Міністерство оборони України, 2018).

Важливо пам'ятати, що під час війни кібербезпеці потрібно приділяти особливу увагу, оскільки ворог буде використовувати будь-яку можливість для отримання інформації та заподіння шкоди. Тому *воєнну кібербезпеку* можна звести до відповідального ставлення кожного громадянина країни до зберігання таємниці від ворога, тобто непоширення в соціальних мережах, чатах, спеціальних додатках, на форумах і каналах інформації, пов'язаної з військовими об'єктами, об'єктами критичної інфраструктури, пересуванням і дислокацією військ, персональними даними військовослужбовців і їхніх сімей. Це також пильне зберігання особистої інформації, якщо вона може становити загрозу національній безпеці, а також миттєве реагування та повідомлення у відповідні державні органи про підозрілі активності, особистості, підготовку диверсій та спроби хакерських атак.

Зосередьмо відтак увагу на деяких ключових моментах воєнної кібербезпеки.

Безпека мобільних пристроїв.

Смартфон для дорослої людини, – це робочий інструмент, на якому є доступи до банківських мобільних додатків, робочих документів та папок, фотографій, переписок тощо. А під час війни це, окрім усього, ще й новинний портал, зв'язок із близькими. І він потребує захисту не менше, ніж офіційні документи, оскільки солдати окупаційної армії можуть використовувати приватну інформацію українських громадян проти них же самих. Наприклад, загарбники на окупованих українських територіях можуть перевіряти мобільні телефони цивільних, шукаючи фотографії з патріотичною символікою, перевіряти, чи не є людина учасником проукраїнських груп у Facebook чи Telegram-каналах, також можуть читати переписку з близькими та друзями в надії знайти докази антиросійської позиції.

Ще однією загрозою можуть бути фейкові додатки, які поширюються зазвичай через рекламу в іграх і на сумнівних сайтах з метою викрадення ваших особистих даних. Надалі персональні дані українських громадян можуть бути використані для спуфінгу (*spoofing* – це ситуація, коли одна людина чи програма успішно маскується під іншою шляхом фальсифікації даних), переписки з близькими та друзями, отримання від них інформації про ключові об'єкти інфраструктури їхніх рідних міст, фотографій дислокації українських військ чи будь-якої інформації, корисної для ворога.

Що робити і як убезпечити свої мобільні девайси (Інформаційна безпека українців, 2022)*?*

- встановіть надійний пароль блокування на смартфоні або планшеті.

Наприклад, чи пам’ятаєте ви фразу Гамлета «To Be Or Not To Be»? Робимо пароль 2b0n2b і вставляємо, де прийдеться, пам’ятну дату і символ – !192b0n2b91 або 2b0n2b1991!

Для складного пароля можна також скористатися датами народження і ФІО ваших друзів (але не близьких родичів!). Наприклад, наші друзі:

Павленко Іван Романович, 1964;

Гуцул Петро Юрійович, 1975.

Вставляємо символ (наприклад, shift+4 буде $) й отримуємо PiR64$GpY75.

●для користувачів Android: встановіть пароль на відкриття додатків Play Маркет і GooglePlay. Використовуйте або вбудовану функцію, або додаток з такою функцією. Для користувачів Apple – Touch ID;

●завантажуйте додатки тільки перевірених і відомих розробників;

●уникайте під’єднання до невідомих мереж Wi-Fi;

●не переходьте за сумнівними посиланнями навіть зі смартфона;

●надійність жодного з месенджерів не доведена. Більш-менш надійними вважається Telegram і Signal;

●паролі мають бути різними для кожного ресурсу. Якщо скрізь буде встановлено однаковий пароль, то, зламавши один сайт, вороги отримують доступ до решти ваших акаунтів (Інформаційна безпека українців, 2022).

Двохетапна аутентифікація

Двохетапна аутентифікація важлива не лише у воєнний, а й у мирний час, оскільки завдяки цій процедурі користувачі різних видів послуг можуть убезпечити себе від кіберзлочинності. Отже, двохетапна аутентифікація – це підтвердження входу в інтернет-банкінг, різноманітні акаунт, особисті кабінети за допомогою телефона (додаткового дзвінка на ваш номер або СМС із кодом-підтвердженням). Якщо ця функція увімкнена, то це серйозно ускладнює, а інколи й унеможливлює для кібезлочинців отримання доступу до персональних даних користувача, оскільки для входу потрібне додаткове підтвердження через доступ до телефонного номера користувача. Більшість банків без цієї функції взагалі не працюють. Двохетапну аутентифікацію НЕОБХІДНО увімкнути і в Google-акаунтах. Якщо ви користуєтеся телефоном на системі Android, то Google-акаунт – це і є ваш телефон з усіма даними на ньому.

Увімкнути двофакторну аутентифікацію легко:

Потрібно відкрити сторінку google account. На панелі навігації обрати вкладку «Безпека». У розділі «Вхід в акаунт Google» обрати «Двохетапна аутентифікація» > Почати. Далі поетапно виконати запропоновану програмою інструкцію.

Те ж саме слід зробити і з акаунтом FaceBook чи іншої соціальної мережі, якою ви користуєтесь.

Розгляньмо приклад FaceBook двохетапної аутентифікації.

Потрібно перейти на сторінку https://www.facebook.com/settings/. Натиснути розділ «Безпека й авторизація» > двохетапна перевірка > редагувати. Обрати метод (sms, додаток, ключ безпеки). Найпростіший – через sms. Зберегти налаштування (Інформаційна безпека українців, 2022).

Програмне забезпечення

Програмне забезпечення – важлива ланка в експлуатації комп'ютера, тому будьте вимогливими, не користуйтесь піратськими безкоштовними версіями, а використовуйте лише ліцензійні програми. Це допомагає розробникам удосконалювати програмне

забезпечення, дає змогу забезпечувати технічну підтримку та оновлювати свої продукти, робити їх зручнішими та безпечнішими.

Не використовуйте антивіруси, програми, соцмережі, бухгалтерські програми, системи управління бізнесом чи процесами, розроблені в Російській Федерації! Оскільки Федеральна Служба Безпеки Російської Федерації може отримати доступ до будь-яких облікових записів російського програмного забезпечення. І не важливо, ліцензійне це програмне забезпечення чи ні, оскільки під загрозою буде ваша конфіденційність. Особливо це актуально в період війни і на інформаційному фронті боротьби.

Використовуючи програмне забезпечення ворога, ви:

●ризикуєте конфіденційністю власної інформації;

●підтримуєте загарбника.

Є безліч зразків більш надійного програмного забезпечення, ніж програмне забезпечення агресора!

Безпека соціальних мереж

Соціальні мережі у XXI столітті – це безмежне джерело інформації про користувачів (від інформації про місце роботи і до інформації про особисте життя). Крім того, це приватна або робоча переписка, яку користувачі необережно ведуть, інколи розкриваючи, самі того не бажаючи, корпоративні таємниці.

У 2013 році П. Дуров (творець і засновник соцмережі «ВКонтакті») відмовився надавати Федеральній службі безпеки Російської Федерації особисті дані користувачів створеної ним соціальної мережі і тому був звільнений із власної компанії. Він зазнав тиску та гонінь з боку силових структур, тож змушений був емігрувати. Це приклад того, як через отримання доступу до особистих даних користувачів силові структури можуть стежити за людьми, збирати на них досьє і докази (наприклад, щодо антиросійської позиції, які потім будуть представлені в суді). Також ми не можемо бути впевненими, що інші соцмережі і розробники програмного забезпечення так само відмовилися співпрацювати із силовими структурами РФ. Отож постає питання про безпеку соціальних мереж і того контенту, який постять користувачі. Особливо це важливо у воєнний період!

Що не можна постити в соціальних мережах?

●фото і відео місцевості, де відбувся обстріл або де впав снаряд;

●відео з ракетами, що летять, моменти влучання снарядів;

●точні адреси і координати місць бойових дій;

●відео і фото з розпізнавальними знаками: таблички з назвами вулиць, станцій метро, автобусних зупинок, магазинів і супермаркетів, заводів і підприємств; номери авто;

●роботу української ППО;

●відео і фото влучання ракет;

●будь-які дані про дії та переміщення українських військ, а також про основні військові об’єкти;

●неперевірену інформацію про потерпілих чи загиблих;

●будь-яку інформацію, яка не верифікована державою і не походить з офіційних джерел;

●категорично заборонено стрімити в прямому ефірі ракетний обстріл і бомбардування (Як поводитися в соціальних мережах під час війни: що не варто робити, 2022);

●фото українських військових великим планом з відкритими обличчями, а також захисників на позиціях;

●інформацію про об'єкти критичної інфраструктури українських міст (жодної інформації про такі підприємства!).

Крім того, ворог намагається поширювати фейки, щоб деморалізувати українців, а також розвідати інформацію для коригування вогню. Саме тому надзвичайно важливо перевіряти інформацію, яка до вас надходить. Використовуйте і постіть інформацію лише з офіційних джерел, по змозі розвінчуйте фейки.

Також можна робити пости в соціальних мережах, повідомляючи про воєнні злочини Російської Федерації. Світ має знати правду. Через кілька днів після атаки можна публікувати в інтернеті фото або відеодокази злочинів окупантів: зруйновані об'єкти архітектури, будинки, постраждалих (обличчя потрібно «заблюрювати» – ставтеся з повагою до особистого життя інших людей!). Усі знімки місцевості мають бути великим планом, щоб ворог не зміг визначити локацію (Інформаційна безпека українців, 2022).

Якщо це не буде загрожувати життю українських громадян, можна надати інформацію про місцеперебування окупантів, ДРГ чи дислокацію ворожої техніки за допомогою чат-бота в *Telegram@evorog_bot*.

І найважливіше: фільтруйте друзів у соцмережах. Не додавайте тих людей, з якими ви не знайомі особисто. Перегляньте список уже наявних друзів й «очистіть» його від «мертвих душ», «незнайомців», людей з проросійською позицією тощо. Пам'ятайте, що серед ваших «друзів» у соціальній мережі, з ким ви давно не спілкувалися або не знайомі особисто, може причаїтися ворожий чат-бот або спуфінговий чи зламаний акаунт.

Неправдиві повідомлення, або фейки

Фейки – підробка чи імітація новин, яка не витримує жодних, навіть поверхових, перевірок на відповідність, проте має потужний вплив на свідомість значної кількості людей.

Наразі українське інформаційне поле переповнене «вкидами» дезінформації і фейками, які продукують російські пропагандисти. Їхня мета – посіяти паніку серед населення. Тому варто довіряти лише офіційним і перевіреним джерелам інформації. Досить часто українські споживачі читають новини через телеграм-канали, але їх також потрібно перевіряти, і навіть додатково, з офіційних джерел та сайтів урядових установ (Інформаційна безпека українців, 2022).

Читаючи емоційні заголовки на новинних сайтах або в постах, потрібно перш за все перевірити посилання на джерело інформації, якщо воно є, переглянути домен сайту, щоб він обов'язково був українським. Пам'ятайте, що фейки майже завжди шокуючі. Наприклад: «Ракетний удар по оперному театру в Одесі!!! Дерибасівської більше нема!!! Одесити масово біжать до укриттів та ховаються в метро!»

Що робити?

●Довіряйте лише офіційним і перевіреним джерелам інформації.

●Критично оцінюйте отриману інформацію, особливо якщо вона має шокуючий характер. І не впадайте в паніку та відчай.

●Не лінуйтеся перевіряти інформацію, що надходить.

●Не передавайте іншим неперевірену інформацію, не поширюйте чутки.

Сумнівні сайти і посилання

Один з найпоширеніших видів кібершахрайства – це сайти-клони. Їх створюють для розповсюдження фейків або викрадення даних. Це може бути сайт новин, урядових структур, відомих інтернет-магазинів тощо. Як приклад, реальний сайт Служби безпеки України – https://ssu.gov.ua/ і сайт-клон – https://ssu.gov.ua.kiev.ua/.

Сумнівні посилання – це основна зброя ворога в інформаційному полі. Їх створюють для викрадення паролів, доступів, викривлення інформації, знищення інформації та пристроїв. На такі посилання можна натрапити всюди – у месенджерах, соціальних мережах, на електронній пошті або в смс-повідомленнях.

Що робити?

Будьте максимально пильні та уважні до кожної дрібниці:

●дуже уважно вивчайте кожне посилання;

●перевіряйте автентичність сайтів, відстежуйте правильність URL-адрес ресурсів в інтернеті, особливо сервісів банківських установ, адже через неточності можна потрапити на фейковий ресурс;

●не відкривайте підозрілі листи, що приходять на вашу електронну пошту, і не переходьте за незрозумілими посиланнями від незнайомих вам адресатів, оскільки це може призвести до завантаження вірусних програм на ваш комп'ютер чи смартфон;

●обмірковуйте отриману інформацію і дослухайтеся до власних сумнівів! Якщо такі сумніви виникають – не користуйтесь цим ресурсом;

●в інтернеті не переходьте за сумнівними посиланнями, адже в рекламі онлайн-ігор та додатків можуть бути «віруси» або фішинг, тому для завантаження потрібних файлів використовуйте лише перевірені офіційні ресурси;

●іноді браузер може повідомляти, що сайт не є безпечним – не ігноруйте такі повідомлення (Інформаційна безпека українців, 2022).

Крім того, варто знати, що в Україні функціонує спеціальний державний орган, який на державному рівні забезпечує профілактику, контроль та розкриття злочинів у кіберпросторі, – *Кіберполіція*. І, незважаючи на те, що кіберполіція має не таку й довгу історію в Україні, у часи воєнного протистояння з Росією вона виконує одну з провідних функцій у протидії російській агресії. У перші ж дні війни українська кіберполіція офіційно звернулася до найбільших світових IT-компаній, VPN-сервісів, компаній з розроблення програмного забезпечення, антивірусів, компаній з надання послуг електронної комерції із закликом припинити співпрацю з РФ. Зокрема, було надіслано понад 350 звернень, у підсумку близько 20% компаній відреагували на вторгнення, припинивши повністю або частково обмеживши свою діяльність на території Російської Федерації (Кіберполіція закликала 30 міжнародних VPN-сервісів припинити співпрацю з РФ, 2022).

Фундамент, на якому побудовано сучасну кіберполіцію, закладено 27 липня 2009 року, коли було засновано *відділ боротьби з кіберзлочинністю* у складі Департаменту боротьби із злочинами, пов'язаними з торгівлею людьми, Міністерства внутрішніх справ України. Наприкінці 2012 року у складі кримінальної міліції Міністерства внутрішніх справ України виокремлено самостійний структурний підрозділ – Управління боротьби з кіберзлочинністю. А 13 жовтня 2015 року створено нову кіберполіцію як структурний підрозділ Національної поліції.

Мета функціонування кіберполіції в Україні – використання висококваліфікованих фахівців у протидії кіберзлочинності, залучення їх в експертних, оперативних та слідчих підрозділах поліції для розкриття злочинів з використанням новітніх технологій.

Основні завдання кіберполіції:

1) реалізація державної політики у сфері протидії кіберзлочинності;
2) завчасне інформування населення про появу новітніх кіберзлочинів;
3) упровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини;

4) реагування на запити закордонних партнерів, що надходять каналами Національної цілодобової мережі контактних пунктів;
5) участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності;
6) участь у міжнародних операціях та співпраця в режимі реального часу. Забезпечення діяльності мережі контактних пунктів між 90 країнами світу;
7) протидія кіберзлочинам у сфері використання платіжних систем.

Через повномасштабне воєнне вторгнення Росії 24 лютого 2022 року з'явилися нові напрями роботи кіберполіції:

●протидія проросійським хакерським угрупованням, які основними цілями обирають інформаційні ресурси державних органів України;

●запобігання масовим ДДОС-атакам на приватний і державний сектори;

●виявлення та реагування на антиукраїнську пропаганду в мережі Інтернет, що координується підконтрольними Росії ЗМІ, а також ботами в соціальних мережах;

●пошук та ідентифікація колаборантів й інших злочинців серед військових чи інших осіб, які підтримують війну (Кіберполіція викрила киянина на підтримці «русского мира», 2022);

●розроблення систем і механізмів для швидкого та повного збирання інформації з відкритих джерел про військових чи найманців незаконних збройних формувань.

Протягом останніх місяців:

●розроблено телеграм-бот «StopRussia» (@stopdrugsbot – https://t.me/stopdrugsbot; https://t.me/stoprussiachannel), що приймає повідомлення від громадян щодо блокування тих чи інших каналів, які ведуть підривну медіароботу проти України;

●створено телеграм-бот «Народний месник» (@ukraine_avanger_bot, який архівовано 1 червня 2022 р. у Wayback Machine), що збирав повідомлення про «ворожі мітки», «рух техніки/живої сили», «нерозірвані снаряди», «мародерів»;

●розроблено сервіс «Russian black book» (https://t.me/BlackBookRussians, архівовано 1 червня 2022 р. у Wayback Machine) для додавання та накопичення інформації про військових та правоохоронців Російської Федерації, їхню особисту участь у війні на території України, а також публічну підтримку війни цими особами. Цей сервіс наповнювали інформацією волонтери;

●створено інструмент для аналізу та автоматизованої перевірки людей і транспортних засобів на блокпостах із функціями пошуку, серед іншого, і за обличчям (для пошуку злочинців, дезертирів, колаборантів);

●розроблено вебресурс DefenseUa (https://www.defenseua.com/) для російських військовослужбовців, на який звернулося понад 460 осіб, які хотіли перейти на бік України у війні або вступити до лав ЗСУ;

●створено платформу для документації воєнних злочинів військовослужбовців Російської Федерації в Україні (https://warcrimes.gov.ua/) тощо.

Також фахівці кіберполіції працюють над ідентифікацією та збереженням цифрових доказів, отриманих під час дослідження технічних комп'ютерних і мобільних пристроїв (мобільні телефони, смартфони, носії інформації, комп'ютери, планшети тощо), які використовували для здійснення злочинів, пов'язаних із війною, або які були у володінні російських окупантів. Проводиться їх детальний технічний аналіз та аналіз наявного і видаленого контенту: фото-, відеозображень і метаданих до них, контактів і зв'язків тощо, що дає змогу виявити сліди оперативно значущої інформації для подальшого долучення її до матеріалів кримінальних проваджень, розпочатих проти військовослужбовців РФ. Така інформація є основою для проведення пошуку в джерелах і базах (банках) даних, наявних у відкритому і Darknet-сегменті мережі Інтернет, та збагачення додатковими даними, як, наприклад, звання і посади

військовослужбовців РФ, облікові дані військових квитків, належність до тих чи інших військових частин тощо.

За підтримки іноземних партнерів застосовується технологія *Clearview AI* від нью-йоркського постачальника (Clearview AI, 2022), за допомогою якої на основі нейромереж здійснюється розпізнавання облич російських загарбників. Програмне забезпечення здатне знаходити в інтернеті зображення із заданими обличчями, що дає змогу вживати всіх відповідних заходів щодо ідентифікації військовослужбовців РФ і виявлення їхніх злочинів на території України.

Важливим напрямом роботи є також дослідження супутникових знімків, що разом із переліченими вище заходами дають змогу додатково виявляти та фіксувати унікальні факти на підтвердження злочинної діяльності загарбників із прив'язкою до геокоординат місць учинення злочинів.

Також кіберполіція відповідно до своїх можливостей і спільних військових директив здійснює інформаційний супротив, волонтерську діяльність, технічний супровід відновлення тимчасово окупованих територій, а також забезпечує безпеку і розслідування атак на державні інформаційні ресурси України, що стали мішенню проросійських хакерських груп, тощо.

АЛГОРИТМ ДІЙ ДЛЯ ЖЕРТВИ КІБЕРЗЛОЧИНУ

Правила кібербезпеки, про які ми писали вище, добре діють як профілактичні заходи, але що робити, якщо кібербезпеку вже порушено і користувач стикається з кіберзлочинністю face-to-face?

У разі підозри, що вас хочуть ввести в оману, на сайті кіберполіції в розділі «STOP FRAUD» можна перевірити номер телефону, банківську картку чи посилання на сумнівний сайт. Можливо, підозрілі особи вже є в базі шахраїв.

Якщо ж ви все-таки стали жертвою кіберзлочинця, найперше – не піддавайтеся паніці. Оскільки в такій ситуації досить часто негативні емоції «зашкалюють», перше, що має зробити жертва кіберзлочину, це заспокоїтися, «взяти себе в руки». Для цього можна виконати одну з наведених нижче вправ.

Дихання 4-7-8

Притисніть язик на піднебіння, прямо за передніми зубами (так потрібно тримати його протягом усієї вправи). Вдихайте через ніс протягом 4 секунд. Затримайте дихання на 7 секунд. Видихайте через рот протягом 8 секунд, видаючи під час видиху природний звук, ніби ви задуваєте свічку. Увагу слід зосереджувати на рахуванні і своєму диханні. Повторити вправу 5-10 разів, аж поки не відчуєте внутрішній спокій.

Дихання по квадрату

Намалюйте на аркуші паперу великий квадрат. Далі потрібно дихати, «пропливаючи» поглядом по кожній його стороні: на 4 рахунки – вдихнути (1-ша сторона), на 4 рахунки – видихнути (2-га сторона), на 4 рахунки – видихнути (3-тя сторона), на 4 рахунки – затримати дихання (4-та сторона). Також можна використовувати для виконання цієї вправи схожу схему (рис. 1). Обов'язковою умовою виконання цієї вправи є зосередження уваги на підрахунку і диханні. Повторити 5-10 разів, поки не відчуєте внутрішній спокій.

М'язове напруження/релаксація

У стресовій ситуації тіло часто надмірно напружується, а м'язи затискаються. Для того щоб повернути собі емоційну рівновагу, можна також працювати «через тіло», послідовно напружуючи і розслабляючи м'язи. Так, спочатку потрібно відчути і сильно напружити плечі. Тримати напруженими протягом 5 секунд, після цього розслабити. Залишити тіло в стані спокою на 5 секунд і сильно напружити кулачки. Порахувати до

5 – і знову розслабити тіло. Далі слід напружувати сідниці: порахувати до 5-ти, а потім знову розслабити тіло. Повторити процедуру зі стопами і пальцями ніг.

Після того як буде знято перший емоційний запал, потрібно скласти відповідний план дій. Для цього можна скористатися питаннями з наведеної нижче авторської техніки «*Наслідки кіберзлочину і Я*»:

1. З якою проблемою я зіткнувся? (Описати детально)
2. Якими можуть бути для мене негативні наслідки цієї проблеми? (Перерахувати не менше ніж 5 наслідків)
3. Який із негативних наслідків проблеми лякає мене найбільше і чому?
4. Що конкретно я можу зробити, щоб уникнути негативних наслідків цієї проблеми?
5. Які з цих дій потрібно виконати негайно, а які можуть зачекати? Проранжуйте їх (від найбільш важливих і негайних до не таких важливих і негайних).
6. Які ресурси я для цього можу залучити (людські, адміністративні, технічні тощо)?
7. Якщо у своєму житті я відчую один або кілька негативних наслідків означеної проблеми, що буду робити для того, щоб мінімізувати (нівелювати) деструктивний для мене вплив?
8. Хто або що може мені в цьому допомогти?
9. Якщо для мене настане негативний наслідок означеної проблеми, якого я боюся найбільше, то:

   …що я відчую в цей момент?
   …що я буду робити?
   …які ще наслідки для мого життя це може мати? Як зміниться моє життя?
   …які ресурси я можу залучити, що зменшити деструктивний вплив цього наслідку на моє життя?
   …чого це мене навчить?

10. Якими можуть бути для мене позитивні наслідки цієї проблеми? (Зазначити не менше ніж 3 наслідки)
11. Чого саме мене має навчити ця ситуація? (Перерахувати не менше ніж 5 життєвих уроків)

Також для розв’язання проблеми можна скористатися *Квадратом Декарта* (TQM systems, 2020). Рене Декарт – французький філософ, фізик, математик, який розробив універсальну систему прийняття рішень. Для проведення цієї методики потрібно розкреслити аркуш паперу на чотири частини, у кожній з яких будуть міститися відповіді на чотири запитання.

- Що буде, якщо це станеться?
- Що буде, якщо цього не станеться?
- Чого не буде, якщо це станеться?
- Чого не буде, якщо це не відбудеться?

На рисунку 1 представлено схему роботи з цією методикою і приклад.

У кожен із чотирьох квадратів ми вписуємо певні факти, які відбудуться або ні, як і передбачає методологія Декарта. Тому цю методику доцільно використовувати для аналізу наслідків, з якими може зіткнутися жертва кіберзлочину. Також отриманий список можна використати для емоційного аналізу ставлення жертви до ситуації і втрат, зумовлених цією ситуацією. Можна обрати три різні кольори, наприклад: синій, чорний і помаранчевий, де чорним позначити найбільш емоційно значну втрату (коли поки що навіть складно уявити, як пережити наслідки втрати), синім – втрату середньої

тяжкості, наслідки якої складно, але можна пережити (є варіанти вирішення проблеми), помаранчевим – втрату, наслідки якої не будуть особливо відчутними.

Рис. 1. Квадрат Декарта з прикладом

Якщо ви стали жертвою кіберзлочину, також важливо пам’ятати такі постулати.

У разі економічного злочину потрібно звернутися до банку з проханням відмінити платіж або повернути гроші (у банках є своя система безпеки і відділи, які займаються кіберзлочинами),якщо треба – заблокувати банківську картку.

У разі сексуальних злочинів (шантажу) не піддаватися паніці, повідомити кіберзлочинцю, що вам потрібен час на роздуми, і домовитися про якомога довший період часу для себе. Пам'ятайте, що розібратися із ситуацією кіберзлочину самостійно буває досить складно, тому краще звернутися по допомогу (до батьків, учителів, адміністрації школи, психолога, кіберполіції). Часто підлітки шукають поради і допомоги у своїх однолітків, але забувають, що підлітки дуже часто обмежені у своєму життєвому досвіді та можливостях вирішення проблеми в правовому полі. Тому краще просити про допомогу у дорослих, яким ви довіряєте.

У разі кібербулінгу в соціальних мережах чи на певних вебсайтах, поширення контенту, який шкодить репутації та людській гідності жертви булінгу, слід звернутися до модератора чи адміністратора соціальної мережі або вебсайту. Потрібно написати скаргу, у якій пояснити ситуацію і попросити видалити або заблокувати відповідний контент.

Якщо ви стали жертвою кіберзлочинців, перше, що вам потрібно зробити, це звернутися до кіберполіції за телефоном 0-800-505-170 або написати лист на електронну адресу callcenter@cyberpolice.gov.ua. Також на сайті кіберполіції можна розмістити електронне звернення. У цій формі слід зазначити своє ПІБ, дату народження, паспортні дані, контактний номер телефону, e-mail, адресу проживання, а далі викласти суть події, а саме: де (на якому інтернет-майданчику), коли, у який спосіб було скоєно злочин, які збитки від скоєного і чим це підтверджується. Після описової частини треба викласти прохальну, де попросити внести вашу заявку в ЄРДР (Єдиний реєстр досудових розслідувань) і почати досудове розслідування; крім того, визнати вас потерпілою стороною в цій справі.

Також держава гарантує кожному громадянину право на отримання безоплатної правової допомоги. Для цього потрібно телефонувати за номером Єдиного контакт-центру 0-800-213-103 (цілодобово і безкоштовно в межах України зі стаціонарних і мобільних телефонів) або надіслати заяву до Національної комісії зі стандартів державної мови (що надає безоплатну первинну правову допомогу) на електронну адресу: info@mova.gov.ua.

ЮРИДИЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ

На жаль, правова культура українських громадян з питань кібербезпеки наразі перебуває не на належному рівні і, відповідно, мало хто цікавиться законодавчими аспектами, пов’язаними з кіберзлочинами. А проте бути обізнаним у цій сфері, на нашу думку, надзвичайно важливо.

На сьогодні правове поле інформаційної безпеки України створюють:

1) Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згоду на обов'язкове дотримання яких дала Верховна Рада України;

2) закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про національну безпеку України» та інші закони;

3) Стратегія інформаційної безпеки України і Стратегія кібербезпеки України;

4) Кримінальний кодекс України.

У Кримінальному кодексі України злочини, які здійснюються в кіберпросторі, розглядаються в розділі 16 «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» і представлені такими нормами:

ст. 361 – несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

ст. 361-1 – створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут;

ст. 361-2 – несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;

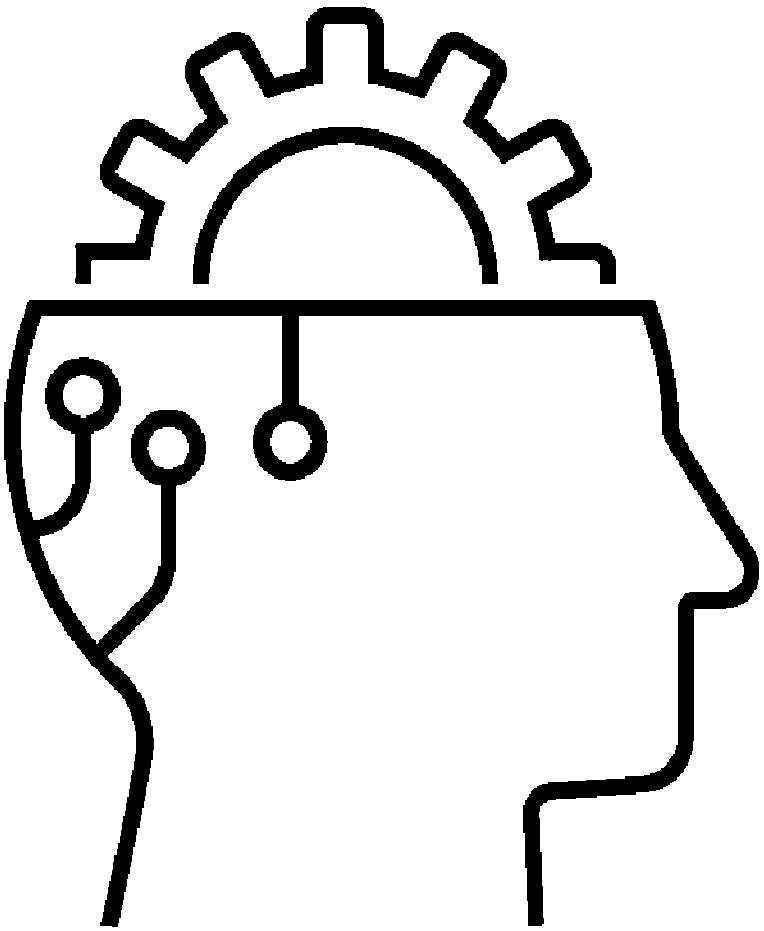
ст. 362 – несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї;

ст. 363 – порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється;

ст. 363-1 – перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

Також до цього переліку потрібно віднести *ст. 176* (порушення авторського права і суміжних прав), *ст. 190* (шахрайство) і *ст. 209* (легалізація (відмивання) майна, отриманого злочинним шляхом).

ЧАСТИНА ІІ



ПРАКТИКУМ № 1

Методика «Ландшафтна мапа потенційних кіберзагроз»

Для того щоб сформувати у дітей навички протистояння кіберзагрозам, спочатку потрібно «м'яко» ввести їх у тему, створити підґрунтя, на якому буде побудовано фортецю вмінь та навичок протистояння кіберризикам. Сучасні діти ліпше запам'ятовують інформацію, представлену у вигляді візуальних образів, особливо образів, які вони створили самі, у які вклали власну логіку, уявлення та символи. Тому ми пропонуємо розпочати ознайомлення дітей із цим курсом за допомогою авторської методики «Ландшафтна мапа потенційних кіберзагроз», що базується на принципах арттерапії.

Цю методику можна використовувати як для індивідуальної, так і для групової роботи. Але наразі ми розглянемо її в груповій версії. Також, зважаючи на вимоги часу, представимо методику для проведення в онлайн та офлайн-форматах.

Основною метою пропонованої методики є створення у свідомості дітей цілісного образу кіберзагроз, із якими вони можуть зіткнутися в інтернет-просторі.

Завдання:

1. Проаналізувати власні знання щодо можливих кіберзагроз.
2. Створити візуальний образ ландшафтної мапи кіберризиків.
3. Відрефлексувати власні емоції та почуття щодо різних кіберзагроз.
4. Сформувати уявлення про кіберризики під час війни.
5. Порівняти кіберризики воєнного часу з кіберризиками мирного періоду.

Рекомендуємо розбити методику на три смислові блоки і працювати з ними в різні дні, оскільки емоційне навантаження на дітей, якщо проводити всі три блоки підряд, може бути значним. А це може знизити рівень сприйняття ними інформації і залученості до процесу.

Тривалість блоків різна.

Блок 1. Створення ландшафтної мапи потенційних кіберзагроз. Орієнтовний час – 1 год. 40 хв.

Блок 2. Я і кіберзагрози. Емоційна рефлексія. Орієнтовний час – 60 хв.

Блок 3. Кіберзагрози воєнного часу. Орієнтовний час – 1 год. 30 хв.

Блок 1. Створення ландшафтної мапи потенційних кіберзагроз

Онлайн	Офлайн
Інструментарій (що потрібно для проведення блоку): ватман, кольорові маркери, кольоровий папір, клей, ножиці, степлер, аркуші формату А4 та інші матеріали, за допомогою яких діти можуть виявити свою креативність (старі кольорові журнали, ґудзики, пластилін, штучні квіти, намистинки).	**Інструментарій** (що потрібно для проведення блоку): одна з програм, за допомогою яких можна створити Mind map. Ми рекомендуємо: **Coggle** – онлайн-додаток для створення Mind map (передбачено безкоштовний тарифний план). Сервіс працює в браузері. Під час роботи можна використовувати зображення, індивідуальні колірні схеми, а створені мапи можна експортувати у форматі PNG або PDF. Додаток підтримує спільну, разом із командою, роботу над проєктами (Coggle YouTube

Channel, 2016), тому його можна використовувати для групової роботи.
Програма **iMindMap** – сервіс від славнозвісного Тоні Б'юзена, основоположника, автора методики побудови ментальних карт (передбачено пробний термін безкоштовного використання протягом 30 днів). Програма пропонує чотири режими: фіксація ідей і думок, мозковий штурм, створення інтелект-карт, конвертація даних у презентації 2D і 3D, ПДФ-файли, таблиці та інші формати (Coggle YouTube Channel, 2016). Цю програму використовують для індивідуальної роботи. Ви також можете скористатися будь-якими іншими програмами.

Хід роботи:

1. Вступ – 20 хв.
2. Створення артпродукту (мапи) – 45 хв.
3. Обговорення – 25 хв.
4. Завершення – 10 хв.

Вступ

Звернення модератора:

Кожен із вас так чи інакше стикався із загрозами, які таїть у собі інтернет-середовище… Можливо, хтось втрачав гроші через кібершахрайство, у когось зламували чи викрадали акаунти в соціальних мережах, хтось ставав жертвою кібербулінгу, а в когось під виглядом дружнього спілкування видурювали конфіденційну інформацію. Не обов'язково, що та чи інша історія трапилася саме з вами, але, можливо, із вашими знайомими чи друзями, ви могли про щось таке чути від батьків, читати в інтернеті або дивилися по телевізору.

Можете розповісти, що вам відомо про загрози в інтернеті?

Далі модератор пропонує дітям висловитися, розказати свої або чужі історії. Записує повідомлене дітьми на дошці, щоб усі бачили.

Якщо діти про щось не згадали у своїх розповідях, модератор має допомогти і розповісти свою історію.

Якщо ж дітям складно про це говорити, можна звернутися до спеціально підготовленого списку можливих загроз в інтернеті, щоб таким чином підтримати обговорення цієї теми (див. Додаток 1)

Після кожної історії потрібно давати назву кіберризику і записувати цю назву на дошці, що її всі бачили.

Після кожної історії потрібно давати назву кіберризику. Назву обов'язково треба візуалізувати, тому ми пропонуємо назначити когось відповідальним за цю ділянку роботи: записувати назви у себе на комп'ютері і

демонструвати на екрані, щоб усі бачили загальну картину.

Важливо! Кіберризики не можна нумерувати! У дітей не має формуватися настановлення, що якийсь ризик стоїть на першому місці, а якийсь – на останньому. Модератор також може проговорити це правило.

На завершення обговорення на дошці обов'язково мають бути зазначені такі основні кіберризики:

- Фішинг, або кетфішинг
- Спуфінг
- Тролінг, або флеймінг
- Сталкінг
- Кібербулінг
- Кібербойкот
- Секстинг
- Кібергрумінг
- Ретинг

Створення артпродукту

Звернення модератора:

Тепер, коли ми проговорили основні загрози, я пропоную вам створити вашу власну ландшафтну мапу потенційних кіберризиків, або їх ще можна назвати інтернет-загрозами. Перед вами лежать різноманітні матеріали, використовуйте їх у своїй творчості.

Звернення модератора:

Тепер, коли ми проговорили основні загрози, я пропоную вам створити вашу власну ландшафтну мапу потенційних кіберризиків, або їх ще можна назвати інтернет-загрозами. Для цього ви можете використати один із додатків для створення Mind map. Для групової роботи я рекомендую **Coggle,** *посилання на нього зараз скину в чат (https://coggle.it/), але якщо у вас є власні пропозиції, їх можна обговорити.*

Ви можете створити мапу потенційних кіберризиків на свій розсуд, на свій смак, але… Є кілька умов:

1. *Це має бути саме мапа. Ви коли-небудь бачили мапу? З позначками, окресленими територіями і т. ін. Вона має бути простою і зрозумілою навіть дошкільнятку (за умови, що дошкільнятко вміє читати).*

2. Якщо ви будете використовувати якісь умовні позначки, їх розшифровку обов'язково треба зазначати на мапі.

3. Ваша мапа має містити всі загрози, про які ми говорили, і, можливо, ще якісь, які ви згадаєте під час роботи над цим завданням.

4. Розміщення на цій мапі елементів, їхні форма та розмір і навіть кольоровий супровід – усе має бути погоджено з усіма членами групи одностайно. Це важлива умова! Якщо хтось має своє бачення розміщення елементів, вам потрібно буде вступити в перемовини і дійти згоди тим чи іншим способом. І пам'ятайте, що ви робите спільну справу, а не відстоюєте індивідуальні переконання!

Насамкінець дам вам одну пораду: до того, як почнете фізично створювати мапу, обговоріть і погодьте композицію. Що і де буде розташовано? За яким

принципом? Тобто чому саме цей елемент має бути розташований саме тут? Що з цим елементом пов'язано? Якими будуть межі між елементами? і т. ін.

На створення мапи у вас є 45 хвилин. За 10 хвилин до завершення я подам вам сигнал. Час пішов!

Для маленьких учасників (молодший або середній шкільний вік) модератор може запропонувати представити кібернебезпеки у вигляді фантастичних тварин і намалювати карту зоопарку, де вони мешкають.

Обговорення

Звернення модератора:

Я бачу, що мапу ви створили. Розкажіть тепер, будь ласка, про неї…

Потрібно дати дітям час на презентацію своєї роботи.

Далі за допомогою відкритих запитань обговорити результати їхньої роботи. Запитання від модератора допоможуть дітям краще осмислити свою роботу і відрефлексувати моменти, на які вони в процесі роботи, можливо, не звертали увагу.

На що потрібно звернути увагу під час обговорення з дітьми мапи потенційних кіберризиків:

1) на принцип, за яким діти розташовували елементи на мапі. Тобто чи є певна логіка побудови, чи, можливо, елементи розташовані довільно. Про принцип побудови можна дізнатися під час презентації мапи. Може бути кілька принципів побудови мапи потенційних кіберризиків. Наприклад, від загрози, що трапляється найчастіше, до рідкісної або від загрози, що лякає дітей найбільше, до тієї, що лякає найменше. Також діти можуть групувати загрози і розміщувати їх як окремі сегменти. Наприклад, за принципом залучення людей у ситуацію кіберзагрози (двоє або група);
2) на центральний елемент на колажі. У центрі може бути розміщена одна із загроз, або це може бути перетин кількох кіберзагроз. Для аналізу розміщення елементів на ландшафтній мапі потенційних кіберзагроз можна використовувати принципи побудови колажів в арттерапевтичній практиці;
3) наявність чітких меж у кожної із кіберзагроз. Якщо меж немає, потрібно уточнити, чому це саме так. І зазначити, у яких елементів цих меж немає. У разі індивідуальної роботи це може свідчити про наявність попереднього досвіду взаємодії дітей з цією кіберзагрозою;
4) на величину ділянок кожної із кіберзагроз на мапі (яка із загроз найменша, а яка найбільша). Потрібно уточнити, чому діти обрали саме такі розміри для кожної із загроз;
5) на кольори ділянок кожної із кіберзагроз. Уточнити, що для дітей означає той чи інший колір, який сенс вони в це вкладають. Для аналізу кольорів мапи потенційних кіберзагроз можна скористатися кольоровою символікою тесту Люшера;
6) наявність символів або певних утілень для тієї чи іншої кіберзагрози. Уточнити у дітей асоціації і попросити пояснити використані символи. Потрібно з'ясувати, що діти вкладали в той чи той символ.

Завершення

Звернення модератора:
Сьогодні ми працювали над темою кіберзагроз. Поділіться своїми враженнями. Що для вас було цікавим? Що нового ви для себе відкрили? Можливо, було щось таке, що не сподобалось?

Я пропоную вам обрати місце в класі, де ми повісимо створену вами мапу потенційних кіберзагроз. Ми ще будемо повертатися до неї на наступних заняттях.

Обов'язково збережіть свою мапу потенційних кіберзагроз, оскільки ми повернемося до неї на наступному занятті.

Блок 2. Я і кіберзагрози. Емоційна рефлексія

Онлайн

Інструментарій (що потрібно для проведення блоку): підготовлені заздалегідь круглі паперові форми для створення персональних значків, кольорові маркери, кольоровий папір, клей, ножиці, степлер та інші матеріали, за допомогою яких діти можуть виявити свою креативність (старі кольорові журнали, ґудзики, пластилін, штучні квіти, намистинки), мапа потенційних кіберзагроз.

Офлайн

Інструментарій (що потрібно для проведення блоку): створена на попередньому занятті мапа потенційних кіберзагроз.

Хід роботи:

1. Вступ – 10 хв.
2. Створення артпродукту (фішок) – 15 хв.
3. Обговорення – 25 хв.
4. Завершення – 10 хв.

Вступ

Звернення модератора:

Сьогодні ми далі вивчатимемо тему кіберзагроз. Чи міркували ви про потенційні кіберризики і мапу, яку створили? Можливо, у вас з'явились якісь цікаві думки чи свіжі ідеї? Може, ви зіткнулися з якимись історіями, пов'язаними з цією темою? Якщо хтось хоче поділитися, то, будь ласка…

Модератор має дати учасникам змогу проговорити свої думки, емоції та почуття, якщо вони у когось виникли щодо теми їхньої роботи на попередньому занятті.

Звернення модератора:

Повернімося до мапи, яку ви створили на попередньому занятті… Скажіть, коли ви зараз дивитеся на неї, чи є у вас бажання щось змінити в ній? Можливо, щось додати?

Якщо в учасників є бажання щось додати до мапи, модератор має дати їм таку змогу.

Створення артпродукту (фішок)

Звернення модератора:

І сьогодні ми будемо з вами досліджувати, наскільки ви готові чи не готові зіткнутися в реальному житті з тими кіберризиками, які ми з вами розбирали на попередньому занятті.

Але спочатку я хочу запропонувати вам створити фішку, яка б на символічному рівні уособлювала вас. Цю фішку ми будемо використовувати далі під час роботи. У вас уже є підготовлені заготовки у формі кулі. Щоб надати їм більшої індивідуальності, ви можете використати матеріали, що лежать перед вами. Не забудьте на фішці зазначити своє ім'я.

Для створення фішки у вас є 10 хв.

Звернення модератора:

І сьогодні ми будемо з вами досліджувати, наскільки ви готові чи не готові зіткнутися в реальному житті з тими кіберризиками, які ми з вами розбирали на попередньому занятті.

Але спочатку я хочу запропонувати вам створити фішку, яка б на символічному рівні уособлювала вас. Цю фішку ми будемо використовувати далі під час роботи. Кожен із вас зараз створить новий елемент на мапі. Цей елемент потрібно назвати вашим ім'ям. До нього можна додати малюнок або позначку, що буде символізувати вас. Зверніть увагу, цей елемент не має бути прив'язаний до жодного з кіберризиків, що вже є на карті; він має бути самостійним, незалежним і легко пересуватися по мапі.

Для створення фішки у вас є до 5 хв.

Обговорення

Звернення модератора:

Подивіться, будь ласка, на мапу.

1) Подумайте, яка з представлених кіберзагроз лякає вас найменше.

Модератор дає кілька хвилин на «подумати» і виконати завдання.

Чому ви обрали саме цю кіберзагрозу? Чи знаєте ви, як впоратися в ситуації, коли зіткнетеся face to face із такою загрозою?

Модератор дає кожному учасникові час відповісти на це запитання. Можливо, поділитися власним досвідом врегулювання проблемної ситуації, що була пов'язана із цим кіберризиком.

2) А тепер подумайте, яка з представлених кіберзагроз лякає вас найбільше, і перетягніть/покладіть туди вашу індивідуальну фішку.

Модератор дає кілька хвилин на «подумати» і виконати завдання.

Якщо це можливо, прокоментуйте, чому ви обрали саме цю кіберзагрозу. Що вас у ній лякає найбільше? Якщо можете, поділіться власним досвідом.

Модератор дає кожному учасникові час відповісти на запитання.

3) Чи є серед представлених кіберризиків такі, з якими ви вже стикалися в житті і точно знаєте, що робити в такій ситуації? Кому дзвонити, як діяти і т. ін.? Якщо таких варіантів кілька, поставте свою фішку на одному з них, а інші просто проговоріть уголос.

4) Чи вважаєте ви щось із представленого на мапі різноманіття НЕ загрозою зовсім? Можливо, архаїзмом, можливо, тим, що з вами ніколи не трапиться? Якщо так, то поясніть чому? Якщо таких немає, то просто залишайтеся на білому полі.

5) Чи є щось серед представленого на мапі різноманіття, що ви засуджуєте найбільше? Те, що вважаєте абсолютно неприйнятним? Щось одне. Чому?

6) Чи є щось із представленого на мапі різноманіття тим, з чим би ви хотіли зіткнутися face to face, щоб випробувати власні сили? Тим, що ви сприймаєте як такий собі челендж для себе? Поведетеся чи ні? Зможете протистояти чи ні? Якщо так, то поясніть, чому ви обрали саме цей ризик.

Ще раз наголосити, що жертвою кіберзагроз може стати кожен. Імунітету бути не може. Потрібно бути пильним і розвивати критичне мислення.

7) А зараз візьміть ручку й аркуш паперу, напишіть на ньому список визначених кіберризиків. Написали? А тепер навпроти кожного з них зазначте ті емоції і почуття, які конкретно цей ризик у вас викликає.

8) А тепер, довго не розмірковуючи, напишіть навпроти кожного ризику ім'я людини, до якої ви звернулися б по допомогу, якби щось схоже трапилося з вами. Це одна і та ж людина, чи різні? Хто саме ці люди для вас? І яку б конкретно допомогу ви у них просили?

Завершення

Звернення модератора:

Сьогодні ми продовжили роботу над темою кіберзагроз, досліджували ваші ставлення, знання, почуття та емоції щодо них. Поділіться, будь ласка, своїми враженнями від заняття. Що нового ви про себе дізналися? Що вас здивувало? Можливо, якісь відкриття?

Блок 3. Кіберзагрози воєнного часу

Онлайн	Офлайн
Інструментарій (що потрібно для проведення блоку): створена на першому занятті мапа потенційних кіберзагроз.	**Інструментарій** (що потрібно для проведення блоку): створена на попередньому занятті мапа потенційних кіберзагроз.

Хід роботи:

1. Вступ – 20 хв.
2. Доповнення артпродукту – 30 хв.
3. Обговорення – 20 хв.
4. Завершення – 10 хв.

Вступ

Звернення модератора:

Сьогодні ми з вами завершуємо нашу роботу над мапою потенційних кіберзагроз. І порушимо складне питання про кіберзагрози воєнного періоду.

Як ви вважаєте, чи відрізняються кіберризики мирного часу від кіберризиків воєнного періоду? Якщо так, то чим саме?

Які ви можете назвати потенційні кіберризики воєнного періоду?.

Записуємо обов'язково назви кіберризиків воєнного періоду і їхні основні (короткі) характеристики.

Створення артпродукту

Звернення модератора:

Тепер, коли ми проговорили кіберзагрози воєнного часу, я пропоную вам доповнити вашу ландшафтну мапу потенційних кіберризиків.

Обговорення

Звернення модератора:

Ви доповнили свою мапу потенційних кіберзагроз.

Які почуття у вас мапа викликає зараз?

Яка з представлених на ній кіберзагроз здається вам найстрашнішою (викликає найбільший страх)? Чому?

Як ви вважаєте, з якими із загроз воєнного часу ви зможете впоратися, а з якими – не дуже?

Завершення

Звернення модератора:

Сьогодні ми завершили працювати над мапою потенційних кіберзагроз.

Скажіть, будь ласка, що нового ви для себе відкрили/усвідомили після обговорення кіберзагроз воєнного часу?

А який висновок для себе ви зробили загалом завдяки роботі над мапою потенційних кіберзагроз?

Чи оголила робота над цією темою ваші слабкі/вразливі місця?

Що ресурсного ви для себе взяли завдяки опрацюванню теми кіберзагроз?

ПРАКТИКУМ № 2

Дискусійний клуб

Оскільки українське суспільство, як і будь-яке інше, неоднорідне, плюралістичне, з різними думками, позиціями та політичними ідеями, досить важливо створювати екологічний та безпечний простір для обміну думками. З огляду на це ми пропонуємо використовувати формат дебатів або формат дискусійного клубу.

Дебати – це спеціально організований публічний обмін думками між двома сторонами на задану тему. Це поняття має довгу історію – від філософських і політичних дебатів Стародавньої Греції, через засновані в епоху Просвітництва дискусійні товариства і до всесвітньо відомого нині навчального методу.

У класичному варіанті дебатів питання на обговорення виносить голова або модератор, завдання якого – регулювання дискусії між двома або більше учасниками публічних дебатів. Спікерам надається певна кількість часу, щоб аргументувати свою позицію. Їм не дозволяється вдаватися до лихослів'я чи ображати інших ораторів або відхилятися від теми дебатів. Спікери мають переконати у своїй правоті третю сторону, а не одне одного, тому в кінці дебатів проводиться голосування, щоб прийняти рішення або відкласти питання для подальших обговорень (Thale, 1989, p. 60).

Дебати можуть стати платформою не тільки для критики, а й для розвитку нових ідей та поліпшення старих, виявлення сильних і слабких сторін в аргументації опонента та пошуку однодумців.

Дискусійний клуб у широкому розумінні можна розглядати як рольову, інтелектуальну або практичну гру, суть якої полягає в тому, що дві команди обговорюють запропоновану тему, при цьому одна команда аргументовано відстоює певну позицію щодо запропонованої тези, а інші – опонують їй.

Ці форми безпечного вираження думок можна використовувати для обговорення будь-яких тем і позицій. З огляду на специфіку цього посібника ми пропонуємо два варіанти: «Ризики кіберсоціалізації» або «Особливості воєнної кібербезпеки».

Варіант 1. Ризики кіберсоціалізації

Як ми вже зазначали, сучасні люди живуть у світі технологій, які невпинно розвиваються. Сьогодні складно уявити своє життя без комп'ютерів, смартфонів, планшетів і соціальних мереж. Комунальні платежі здійснюються через спеціальні сайти, оплата проїзду в громадському транспорті – за допомогою мобільного додатку. У нинішньому житті не потрібно чекати місяцями на лист від близької людини, що живе в іншій країні, достатньо зробити відеодзвінок через Skype, щоб побачити рідне обличчя. І люди вже звикли до цих безсумнівних переваг, вони кіберсоціалізувалися.

Кіберсоціалізація (від грец. Kybernetike – мистецтво управління; kybernao – правлю кермом, управляю; КхвеснЮфзт – керманич та англ. socialization – соціалізація) – процес оволодіння навичками користування інтернетом, різноманітними програмними продуктами віртуальної мережі, наслідком чого є специфічна соціалізація особистості.

Але кіберсоціалізація, як і будь-який інший процес, приховує в собі певні ризики. Інколи – об'єктивні, інколи – потенційні, інколи – вигадані, а інколи – неминучі. Ми підготували перелік тем щодо проблем, з якими може зіткнутися людство в процесі розвитку технологій. Їх можна використовувати для роздумів чи дискусій на тему кіберсоціалізації (див. Додаток 2). Більшість тем мають психологічне спрямування і

містять моральну дилему. Вони представлені у вигляді карток. З одного боку картки – назва кіберризику, з другого – короткий опис проблеми.

Основна мета цієї гри – допомогти учням розвинути навички логічної і послідовної аргументації в публічних виступах, уміння слухати й відстоювати власну позицію під час взаємодії з іншими людьми, а також поглибити знання психологічних особливостей кіберсоціалізації особистості.

Завдання:

● Порівняти особливості життя людей до інтернет-епохи і під час цієї епохи, а також спрогнозувати, як зміниться людське життя в недалекому майбутньому.

● Навчити формувати логічну і продуману аргументацію для захисту власної думки та позиції.

● Сформувати навички публічних виступів.

● Навчити, як бути впевненим у собі, відповідаючи на запитання аудиторії.

Особливості та правила проведення дискусійного клубу

Учасників дискусії ділять на дві команди, кожна з яких складається із двох або трьох спікерів.

Кожна команда може мати два-три конструктивні (стверджувальні) виступи і два-три виступи-спростування. Але не більше. Перша команда виголошує стверджувальну промову, після чого друга команда спочатку виступає із спростувальною промовою (спростуванням) на аргументацію, наведену першою командою, після чого виголошує свою стверджувальну промову. Після цього перша команда виголошує спростувальну промову, а далі – свою стверджувальну.

Тобто план такий:

Раунд № 1	Команда № 1. Стверджувальна промова
	Команда № 2. Спростувальна промова
Суддівське рішення	
Раунд № 2	Команда № 2. Стверджувальна промова
	Команда № 1. Спростувальна промова
Суддівське рішення	
Раунд № 3	Команда № 1. Стверджувальна промова
	Команда № 2. Спростувальна промова
Суддівське рішення	

Афірматив має відстоювати власну тему. Під час дебатів перегляд позиції команди не допускається.

Команда, яка виголосила стверджувальну промову, має навести аргументи і докази, що будуть підкріплювати визначену позицію. Промова має бути логічною, щоб переконати розумну, але раніше необізнану особу, що розумніше вірити цьому твердженню, ніж не вірити йому. Факти мають бути точними. Дозволено використовувати візуальні матеріали, але після їх оприлюднення вони також стають доступними для аргументації іншою командою за її бажанням.

Кожному промовцю, як тільки він завершує свій конструктивний виступ, ставлять запитання. Він має відповідати на них без консультації із членами команди. Запитання можуть ставити як члени опозиційної команди, так і глядачі. Кожне запитання має бути чітко сформульоване і безпосередньо стосуватися теми дебатів.

Під час спростувальної промови (спростування) не можна наводити нові конструктивні аргументи. Потрібно відповідати на основні аргументи опозиційної команди.

У кожної дискусії завжди має бути експертна (суддівська) колегія, що визначить переможця. Судді мають базувати своє рішення виключно на представлених під час дискусії аргументах і матеріалах, не беручи до уваги іншу інформацію, якою вони можуть володіти, або власну суб'єктивну позицію.

Тривалість дискусій

Для письмової форми роботи тривалість становить від 60 хв. до 1 год. 30 хв. залежно від індивідуальних особливостей роботи групи.

Для дебатів тривалість буде залежати від кількості раундів. На кожен раунд (стверджувальний виступ – виступ-заперечення – час, присвячений відповідям на запитання) відводиться 60 хв. На кожен виступ дається до 10 хв. + до 10 хв. на час «запитання-відповіді» до оратора. І ще до 10 хв. – на ухвалення рішення суддівською комісією, хто переміг у цьому раунді.

Рекомендуємо виконувати це завдання у два смислові блоки: спочатку – в індивідуальному форматі роботи, а потім – у груповому. Але, залежно від обставин, описані нами блоки можна проводити незалежно один від одного.

Інструментарій: підготовлені картки для дискусійного клубу, аркуші паперу формату А4, ручки, ноутбук або комп'ютер для кожної групи учасників із доступом до інтернету, програма Power Point (за потреби), проєктор.

Для роботи з першим блоком модератор обирає лише частину карток для дискусійного клубу (на свій розсуд). Іншу частину залишає для блоку групової роботи. (Важливо, щоб картки першого і другого блоку не повторювалися!)

Блок 1. Робота над аргументацією в письмовому вигляді

(індивідуальний формат роботи)

На початку заняття модератор має запропонувати дітям поміркувати й описати, як жили люди до появи інтернету (з якими труднощами вони стикалися, які переваги мали). І порівняти цю картину з тим життям, яке у них зараз, – з вільним доступом до всіх благ цивілізації та інтернетом 24 години на добу, з мобільним зв'язком та різними мобільними додатками, що полегшують життя, тощо.

Далі модератор пропонує дітям пофантазувати і поміркувати, яким може стати життя людей з розвитком технологій, що може з'явитися в їхньому житті таке, чого немає зараз. Як саме може це життя змінитися?

Після того як діти опишуть майбутнє людства, модератор має поставити запитання про ризики, ризики кіберсоціалізації, з якими люди можуть зіткнутися в майбутньому. Якими вони будуть? Як зміниться життя? (Можна скласти список, записавши їх).

Звернення модератора:

У мене із собою є картки, кожна з них присвячена певній проблемі, з якою зіткнулося або ще зіткнеться людство внаслідок технічного прогресу. Але чи справді це можна назвати кіберризиком?

Зараз я пропоную вам обрати одну із карток. Я викладу їх так, щоб ви обирали наосліп.

Тепер, після того як ви обрали собі картку, візьміть, будь ласка, аркуш А4, угорі на ньому напишіть назву проблеми, яка вам дісталася. Потім розділіть аркуш на два стовпчики. У першому стовпчику потрібно буде записати аргументи «за», якщо проблема, що означена на вашій картці, є або може стати серйозним кіберризиком для людства. У другому стовпчику вам потрібно навести аргументацію «проти» – чому означена проблема не може стати серйозним кіберризиком для людей. Важливо знаходити аргументацію, навіть якщо ви не згодні з тією чи іншою позицією. Це тренування для гнучкості вашого розуму, що розвиває інтелект та вміння адаптуватися до будь-якої ситуації.

На виконання цього завдання у вас 15 хв. За хвилину до закінчення часу я вас про це попереджу. Не забудьте підписати свою роботу. У неї має бути автор.

Тепер, коли ви завершили роботу, будь ласка, передайте ваш аркуш з аргументацію сусідові зліва (таким чином усі учасники мають отримати чужу роботу). Ваше завдання – прочитати наведену аргументацію і зробити на її основі висновок: чи справді це серйозний кіберризик, чи ні. Запишіть ваш висновок на аркуші внизу. Окремо обведіть на аркуші пункти, що схилили вас прийняти саме таке рішення. Якщо у вас є якісь думки з приводу цього кіберризику або хочете додати до списку свою аргументацію, ви можете це зробити, але ручкою іншого кольору. І також зазначте на аркуші своє ім'я та прізвище, оскільки тепер ця робота стала спільною.

На виконання цієї роботи у вас 10 хв.

Наступне завдання. Передайте, будь ласка, свою картку з проблемою сусідові справа. Тепер у кожного з вас нова картка. Ви маєте подумати і написати листа до своєї бабусі або маленької сестрички/братика 6 років, у якому будете пояснювати, що це за кіберризик і чому варто його остерігатися. Ви маєте описати все так, щоб викладене вами могла зрозуміти і маленька дитина, і людина без значного комп'ютерного досвіду. Тобто найпростішими словами. Наводьте прості і зрозумілі аргументи на підтримку своєї позиції.

Цю роботу підписувати не потрібно. Але вгорі великими літерами напишіть назву ризику кіберсоціалізації.

На виконання цієї роботи у вас 15 хв. За хвилину до закінчення часу я вас про це попереджу.

Тепер свої есе віддайте, будь ласка, мені. Я рандомно роздам їх іншим учасникам групи, які будуть проводити «сліпе» (оскільки не будуть знати автора), незалежне оцінювання вашого твору за такими критеріями:

а) простота і зрозумілість аргументації – 3 бали;

б) логічність, чіткість та послідовність викладення думок – 2 бали;

в) переконливість позиції автора (якщо після читання тексту незалежний оцінювач зможе 100-відсотково погодитися з позицією, наведеною в тексті, і не залишиться двояких трактувань або інших моральних дилем) – 3 бали;

г) цікавість – 2 бали.

Незалежні оцінювачі! У вас є 15 хв., щоб ознайомитися із твором й оцінити його. А також пояснити, які недоліки ви побачили у творі і чому виставили саме таку оцінку.

Після завершення роботи модератор має провести обговорення з дітьми. Орієнтовні запитання для обговорення:

●Чи легко було знаходити аргументацію «за»? Якщо комусь було складно, то підніміть, будь ласка, руку. З чим були пов'язані складнощі?

●А кому було складно знаходити аргументацію «проти»? Підніміть руку. Наскільки вам було складно «залізти в черевики» точки зору опонента? Це вміння дуже важливе, оскільки перемогти в протистоянні можна лише тоді, коли досконало вивчиш свого супротивника, його позицію, його аргументи, його мотиви. Пошук контраргументів – неймовірно важлива навичка для перемоги.

●Чи легко вам було дібрати просту аргументацію для пояснення ризиків на другому етапі роботи?

●Кого ви уявляли, коли писали есе? Маленьку дитину чи літню людину? Чому? Кому, на вашу думку, легше пояснити небезпеки, пов'язані з кіберсоціалізацією? Чому?

●Які почуття у вас викликала інструкція віддати своє есе на перевірку іншій людині?

●Які почуття і думки у вас виникли, коли ви почули, як саме було оцінено вашу працю?

●Чи було вам самим складно оцінювати роботу іншого учасника?

●Чи виникало у вас бажання керуватися не об'єктивними критеріями, а вашою суб'єктивною думкою?

●Чи враховували ви, коли оцінювали есе, свою власну позицію і думку щодо ризику? Чи було таке, що ви оцінювали думки автора есе вище, бо його думки збігалися з вашою позицією? І навпаки, чи занижували ви оцінку, якщо думка автора есе не збігалася з вашою?

Звернення модератора:

Бути суддею насправді не так легко, як це може здатися на перший погляд. Інколи буває досить складно зберегти об'єктивність.

Подумайте і скажіть, чи була для вас якась різниця між першим випадком оцінювання, коли ви знали ім'я автора есе, і другим, коли оцінювання відбувалося «наосліп». Який із видів оцінювання ви вважаєте більш об'єктивним?

Обговорення може тривати від 10 до 30 хв.

Блок 2. Дебати

(груповий формат роботи)

Підготовчий етап.

Перед проведенням дебатів учнів потрібно розділити на парну кілька команд, у середньому від 2 до 5 осіб у команді (може бути і більше). Якщо, на розсуд організаторів дебатів, команд буде більше ніж дві, дебати мають проходити паралельно, але в різних приміщеннях.

Визначити, хто з учнів буде виконувати роль суддів. Ми пропонуємо обирати не одного, а трьох суддів – для більшої об'єктивності.

Далі потрібно запропонувати учням обрати наосліп картку з потенційним ризиком кіберсоціалізації. Так само рандомним методом визначити, чи будуть вони захищати позицію «це серйозний ризик для людства», чи позицію «це не ризик, це особливість життя, і в цьому немає нічого страшного».

Визначити, скільки буде раундів у дебатах – один, три чи більше. Уточнити час кожного з раундів.

Обговорити правила дебатів, які будуть спільними для всіх команд.

На підготовку до дебатів, написання аргументації до обраної кількості раундів (2 чи 3) командам надається час і відводиться місце для обговорення (щоб команда опонентів їх не чула). Тривалість підготовчого етапу може становити від 20 до 30 хв.

Промовець від команди на кожен раунд змінюється; відповідно, на кількість раундів може впливати кількість членів команди.

Звернення модератора:

Отже, ми обговорили всі організаційні моменти і час розпочати наші дебати. Нагадую, що під час виступу оратора в залі має зберігатися повна тиша! Ніхто не має права розмовляти, перешіптуватися із сусідом або перебивати людину, що виступає!

Оратору для виступу дається 10 хв., за дотриманням часу стежать судді. Після цього я надам слово команді-опоненту для спростувальної промови, тому ви маєте уважно слухати, що буде говорити оратор, оскільки вам доведеться розбивати його аргументи! Майже без підготовки! А це значить, що потрібно бути кмітливим, креативним, швидко реагувати на зовнішні зміни. Тому я попрошу вже зараз обрати людину, яка буде виступати від вашої команди із спростувальною промовою, щоб усе було чесно! Між стверджувальною промовою і промовою-спростуванням ми зробимо 5 хв. перерви для підготовки учасника. На спростувальну промову також дається до 10 хв. (судді стежать за часом). До речі, команда-опонент, ваш представник може взяти із собою блокнот і ручку, щоб у разі потреби робити нотатки.

Після цього ми матимемо час на запитання як від членів команди-опонента, так і від залу.

Далі судді будуть підбивати підсумки раунду і визначати команду-переможця. І на їхні рішення буде впливати не тільки наведена аргументація, а й ораторські навички (те, як ви проводили презентацію), ваша ввічливість і конструктивність у дискусії (коректність та вміння не виходити «за рамки»). А також те, як представник команди відповідав на питання.

Переможе та команда, яка виграє найбільшу кількість раундів.

Отже, прошу до слова першого оратора!

За описаною схемою будуть проходити всі раунди дебатів. Модератор має уважно стежити за дискусією, підказувати правила та коригувати (якщо це буде потрібно) поведінку учасників дебатів. Інколи, залежно від потреб учасників, можуть бути деякі відхилення від обумовленого часу.

Після завершення дебатів модератор має надати слово всім охочим висловити свої враження, емоції та почуття – як членам-учасникам, глядачам, так і суддям.

Варіант 2. Особливості воєнної кібербезпеки

З огляду на особливості воєнного часу пропонуємо провести дискусійний клуб із стратегії і тактики, запропонувавши дітям розробити «Концепцію воєнної кібербезпеки». Як уже було зазначено, кібербезпека державного рівня має свою специфіку та особливості. Агресія Російської Федерації проти Української держави перш за все ставить за мету дестабілізацію в країні, підрив бойового духу та віри населення в перемогу, поширення дезінформації та фейків для залякування мирного населення та формування в нього необхідних ворогові світоглядних позицій. «Вимкнути, знищити, дестабілізувати» – ось їхні основні принципи ведення війни. Масові вимкнення електроенергії, телефонного зв'язку та інтернету, труднощі з обслуговуванням клієнтів і проведенням банківських операцій, реальні фінансові збитки – це те, що використовує ворог уже сьогодні.

Інформаційна війна, яку Російська Федерація веде проти України, підриває основи нашої політичної та соціальної системи, засобами психологічного тиску чинить вплив на масову свідомість населення, щоб дестабілізувати суспільство і державу. У зв'язку з цим вважаємо за потрібне порушити на дискусійному клубі цікаву й

актуальну тему – «Концепції воєнної кібербезпеки країни». Тема складна і неоднозначна, тому підготовка до проведення дискусійного клубу займе певний час.

Основна мета цієї гри – допомогти учням розвинути важливі навички, зокрема логічного і послідовного мислення, формування стратегій і тактик, аргументації під час публічних виступів та відстоювання власної позиції, а також пошуку, збирання, аналізу та узагальнення інформації щодо особливостей воєнної кібербезпеки на державному рівні.

Завдання:

● Детально вивчити особливості воєнної кібербезпеки і стратегій державного захисту.

● Навчитися розробляти стратегію і тактику ведення інформаційної війни.

● Сформувати логічну і продуману аргументацію для захисту власної позиції.

● Розвинути в себе навички публічних виступів.

● Виробити впевненість у собі під час відповідей на запитання аудиторії.

Особливості проведення і тривалість дискусійного клубу

Учасників дискусії ділять на дві команди, кожна з яких складається щонайменше з п’яти учасників. У класі можуть бути діти, які не хочуть брати участь у дискусії, у такому разі вони мають взяти на себе роль спостерігачів. Останні активно долучаються до процесу обговорення проєктів на етапі проведення дискусійного клубу, але не беруть участь у підготовці командних проєктів. Щоб пожвавити дискусію під час обговорення, як спостерігачів також можна запрошувати учнів інших класів.

Підготовчий етап

Кожна команда отримує завдання з розроблення Концепції державної кібербезпеки. З огляду на складність отриманого завдання командам на підготовку проєкту, який вони будуть захищати й обговорювати на дискусійному клубі, має бути виділено достатньо часу (близько місяця).

Ролі в командах діти мають розподілити самостійно.

Через місяць кожна команда має надати підготовлену Powerpoint-презентацію та призначити одного спікера (за бажанням – двох) для презентації проєкту.

Процес проведення дискусійного клубу

Команди будуть виступати по черзі. Для визначення черговості виступу можна «кинути монетку».

Для презентації проєкту кожна група отримує по 20 хв. По завершенні презентації спостерігачі та команда супротивника мають до 15 хв. часу на уточнювальні і «каверзні» запитання. Після цього дається час на виступ іншій команді і, відповідно, час на уточнювальні запитання.

Далі відбувається сама дискусія, під час якої кожен учасник може висловити власну думку щодо представленої командами стратегії. А учасники команди можуть погоджуватися або не погоджуватися із зауваженнями і відстоювати представлену позицію в екологічній та коректній манері. На проведення дискусії дається 30 хв.

На визначення переможців – до 10 хв.

На висловлення зворотного зв’язку учасників дискусійного клубу – до 10 хв.

Загальний час проведення заходу – 2 год.

Також потрібно заздалегідь потурбуватися про суддівську колегію із 2-3 осіб (можливо, учителів – краще тих, які не викладають предмети у цих учнів, щоб їхні рішення були об’єктивними). Судді мають узгодити між собою критерії оцінювання. Наприклад:

● харизматичність виступу – 10 балів;

● добре підготовлена презентація (яка відповідає всім стандартам) – 5 балів;

● аналітичність дослідження – 10 балів;

●продуманість, чіткість та послідовність представленої концепції (стратегії) – 10 балів;

●багатоманітність напрямів та ідей представленої стратегії – 5 балів;

●влучність запитань – 5 балів;

●чіткість і глибина відповіді на запитання – 5 балів тощо.

Інструментарій: ноутбук або комп'ютер з доступом до інтернету, програма Power Point, проєктор, динаміки або колонки (за потреби). Для кожної із команд можна зробити кольорові значки – як знаки певної належності.

Блок 1. Домашня робота над проєктом

До початку дискусійного клубу учасники команд мають підготувати проєкти відповідно до визначеного плану:

1. Проаналізувати інформацію, що є у вільному доступі щодо вже наявних заходів з кібербезпеки державного рівня. Для цього можна використовувати лише офіційні ресурси державних структур.

2. Виявити «слабкі» сторони чинної державної стратегії та представити реальні випадки порушення державної кібербезпеки (можна використовувати матеріали перевірених, авторитетних ЗМІ).

3. Також потрібно окремо виділити *потенційні* ризики для державної кібербезпеки.

4. На основі наявної інформації розробити стратегічний план державної кібербезпеки (що держава має удосконалити, які заходи провести, які стратегічні напрями розвивати тощо). Учасники можуть також надати конкретні рекомендації (Наприклад, упровадити в школах урок «Кібербезпека» для старшокласників).

За результатами пошуку, аналізу та узагальнення інформації потрібно створити презентацію в Power Point.

Обов'язкові елементи презентації:

1. Титульний аркуш з назвою проєкту і назвою команди (перерахувати її учасників).

2. До кожного із чотирьох поставлених завдань може бути не більше як три слайди.

3. Передостаннім слайдом має бути «Дякую за увагу!» – як знак поваги до слухачів.

4. Останній слайд – інформація про індивідуальний внесок учасників проєкту за принципом: ПІБ – яку саме за роботу виконав учасник у цьому проєкті (наприклад, шукав інформацію для одного завдання і брав участь у формуванні слайдів 2-3).

Презентація Power Point не має містити контрастні стилі оформлення, а також шрифти менше ніж 10 пт. (що незручно з погляду сприймання інформації).

Якщо дітям складно самостійно виконати завдання, керівником проєкту можна призначити одного із шкільних учителів, до якого можна звернутися по допомогу і за консультаціями.

Блок 2. Проведення дискусійного клубу

Звернення модератора: *Сьогодні ми зібралися тут, щоб обговорити важливе й актуальне питання кібербезпеки нашої країни. Для цього дві команди учасників нашого дискусійного клубу будуть представляти сьогодні проєкти власного виробництва щодо Концепції воєнної кібербезпеки України. Привітаймо їх оплесками.*

Кожній команді для виступу дається до 20 хв. (Сповідаюся, ваші спікери вдома підготувалися і розуміють, що перебирати час не можна!).

Глядачі й учасники команди опонента! Вам забороняється під час виступу промовця розмовляти, перешіптуватися, дискутувати або якимось іншим чином заважати йому говорити! За це будуть зніматися бали з команди, а глядачі, що не дотримуються тиші в залі, будуть сидіти на «ганебному стільці» он у тому кутку!

Після виступу першої команди буде час на уточнювальні і «каверзні» запитання – до 15 хв.

Після цього я надам час для виступу іншій команді і, відповідно, на уточнювальні запитання.

Далі відбуватиметься дискусія, під час якої кожен учасник процесу зможе висловити власну думку щодо представленої командами стратегії або навіть власну пропозицію, якщо така з'явиться.

Підбивати підсумки нашого дискусійного клубу будуть спеціально запрошені судді.

Модератор представляє суддів і надає їм час для вступного слова, де вони озвучують критерії оцінювання сьогоднішнього дискусійного клубу.

Знову модератор: *А щоб нам усім було цікаво брати участь у дискусіях, за кожне влучне запитання (оскільки запитання не за темою дискусії враховуватися не будуть) глядачі отримують 1 бал. За цікаві власні пропозиції щодо державної стратегії вони можуть отримати 2 бали. Наприкінці дебатів я надам слово глядачам, які мають бали, щоб вони висловили власні симпатії і пожертвували накопичені бали на користь тієї команди, яка, на їхню думку, представила найкращу стратегію. Глядачі також мають пояснити, чому вони вважають, що ця стратегія найкраща, інакше бали в скарбничку команди зараховані не будуть. Усе чесно! Бали будуть отримані не за особисті симпатії, а за крутість проєкту!*

Отже, готові починати?

Запрошую до слова першого спікера!

Модератор має уважно стежити за дискусією, підказувати правила та коригувати (якщо це буде потрібно) поведінку учасників дебатів. У його обов'язки входить стежити за часом і вести облік глядачів, які ставили запитання та висловлювали власні пропозиції, та їхніх балів.

Після дискусії і жертвування балів модератор надає суддям 5-хвилинну перерву для підрахунку балів та обговорення. Далі судді озвучують свій вердикт.

На завершення дискусії модератор має підбити підсумки дискусійного клубу і подбати про зворотний зв'язок від учасників.

ПРАКТИКУМ № 3

Правила сімейної кібербезпеки
Методика «Тотемний кіберїжак»

Інформаційна безпека і кібербезпека в сучасному суспільстві стоять на одному рівні з фізичною безпекою і можуть бути віднесені до переліку базових потреб, адже вони стосуються захисту життєво важливих інтересів людини, а щодо українського кейсу і більш глобально – суспільства, держави загалом. Неправдива, неповна, невчасна інформація може завдати шкоди і навіть загрожувати життю в умовах воєнного часу. Особливо вразливі в цьому контексті діти, оскільки вони не завжди знають, яку інформацію можна викладати в мережі, а яку – не варто. Часом вони також не можуть правильно зреагувати на матеріали / інформаційні повідомлення, що надходять до них з мережі. Це може відбуватися з різних причин: часом – через брак життєвого досвіду, часом це може бути пов'язано з вразливістю дитячої психіки.

Деякі батьки, намагаючись убезпечити своїх дітей від інтернет-загроз, блокують їм доступ до мережі, обмежують години перебування або чітко регламентують, якими додатками чи сайтами діти можуть користуватися. На нашу думку, звичайні заборони і тотальний контроль не можуть бути рішенням глобальної проблеми, тільки розвиток критичного мислення і формування позиції свідомого споживання в інтернет-мережі можуть сформувати у дітей правильну, медіаграмотну позицію та підготувати їх до взаємодії з можливими кіберзагрозами.

Тому найліпшою ідеєю є вироблення *правил сімейної кібербезпеки*. Якщо пошукати в інтернеті, то можна знайти досить багато зразків того, якими мають бути такі сімейні правила, але здебільшого вони стосуються виключно дітей (що дітям можна, а що не можна; як їм користуватися комп'ютерами/планшетами/телефонами; у які години і т. ін.). Але автори цих порад забувають одну просту річ: якщо це сімейні правила, вони мають стосуватися всіх членів сім'ї без винятку. Тобто не тільки дітей, а й дорослих. Усі мають рівні права. Щоб не припуститися такої помилки, ми пропонуємо скористатися для розроблення правил наведеною нижче методикою.

Основною метою цього практикуму є формування сімейних правил кібербезпеки та алгоритмів дії для всіх членів сім'ї (або трудового колективу) у небезпечних ситуаціях.

Завдання:

1. Узагальнити знання членів сім'ї про загрози, пов'язані з особистою безпекою та безпекою інших, з витоком персональної інформації, з державною безпекою і фізичним здоров'ям.
2. Намалювати тотемного кіберїжака й описати його особливості.
3. Сформувати правила сімейної кібербезпеки (чого не можна робити).
4. Доповнити сімейні правила алгоритмом дій у разі зіткнення з кіберзлочинцем (можна використати наведені в тексті або власні).

Інструментарій: аркуші формату А4, ручки, кольорові олівці.

Тривалість:

Блок 1. Обговорення інтернет-загроз. Орієнтовний час – до 40 хв.

Блок 2. Малювання тотемної тварини кібербезпеки. Орієнтовний час – до 30 хв.

Блок 3. Формування правил сімейної кібербезпеки – до 20 хв.

Зазначимо, що цю методику можна також використовувати *для роботи з учнівським або трудовим колективом*, оскільки колективи мають досить багато спільних характеристик із сім'єю.

Блок 1. Обговорення інтернет-загроз

Перед тим як розпочати формування та обговорення сімейних правил кібербезпеки, потрібно уточнити загрози, з якими кожен із членів сім'ї може зіткнутися в інтернеті як у мирний, так і у воєнний час.

Для такого обговорення пропонуємо скористатися технікою «П'ять типів кіберзагроз». Потрібно взяти аркуш паперу формату А4 і розділити його з одного боку на чотири рівні квадрати. Далі в кожен із квадратів вписати підзаголовок певного типу кіберзагроз, а саме: «стосуються особистої безпеки», «стосуються безпеки інших», «стосуються загрози витоку персональної інформації», «стосуються державної безпеки». У процесі обговорення кожен квадрат має бути заповнений. У кожен із квадратів потрібно вписати щонайменше вісім кіберзагроз. Наприклад:

Стосуються особистої безпеки:	**Стосуються безпеки інших:**
● ознайомлення з порнографічними матеріалами, ненормативною лексикою, інформацією расистського, людиноненависницького або сектантського змісту; ● спілкування з небезпечними людьми (збоченцями, шахраями, гриферами); ● формування залежності (ігрової, комп'ютерної, інтернет-залежності); ● загроза отримання недостовірної чи неправдивої інформації; ● залучення до виконання протиправних дій (хакерство, порушення прав та свобод інших людей); ● загроза залучення до суїцидальних ігор, челенджів або спільнот (наприклад, «Синій кит») тощо	● матеріали, зберігання і використання яких може стати причиною посягання на безпеку інших людей (наприклад, інформація про створення вибухівки); ● вчинення протиправних дій, що тягнуть за собою відповідальність згідно з чинним законодавством; ● свідоме і несвідоме введення в оману інших; ● тролінг – соціальна провокація або знущання під час мережевого спілкування; ● кібербулінг – свідоме цькування та приниження, передусім однолітків, тощо.
Стосуються загрози витоку персональної інформації:	**Стосуються державної безпеки:**
● розголошення персональної і конфіденційної інформації (прізвища, імена, контакти, секретні дані кредитних карток, номери телефонів); ● передавання інформації про банківські картки або рахунки третім особам; ● небезпека завантаження програм зі шкідливими функціями; ● загроза зараження ПК вірусами різної категорії тощо.	● публікація в соціальних мережах фотографій або особистої інформації українських військових; ● публікація або поширення інформації про об'єкти критичної інфраструктури міст, військові об'єкти, пересування української військової техніки тощо; ● публікація або поширення інформації про ракетні удари, точні адреси або геолокації вибухів у містах чи селах тощо.

Після того як усі чотири квадрати будуть заповнені, потрібно буде згадати, що робота з технікою та в інтернет-мережі пов'язана також із загрозами для фізичного

здоров’я. Відтак узяти окремий аркуш паперу і посередині написати «стосуються фізичного здоров’я». І так само зазначити щонайменше вісім пунктів, коли проведення часу в інтернеті може завдати шкоди фізичному здоров’ю (наприклад, болі в плечах, спині, сідницях; зниження гостроти зору; проблеми з кров’яним тиском тощо).

Блок 2. Малювання тотемної тварини кібербезпеки

Після того як робота над списками завершиться, потрібно перейти до креативної частини і намалювати тотемну тварину сімейної кібербезпеки – їжака. З давніх часів вважають, що тотемні тварини – це покровителі і захисники, які надають сили, оберігають та захищають від усіляких негараздів. Їжаки – нічні хижаки, і вони справжні мисливці на шкідників. До їхнього раціону входять миші, змії, слимаки, равлики, черв'яки, гусінь та інші комахи. І хоча на перший погляд їжаки здаються милими і неповороткими, але насправді вони безжальні і спритні мисливці. Їхній гострий слух і чудовий нюх дають змогу ловити прудких мишей, а особливості організму – не боятися навіть отруйних змій. Їжаки ведуть потайний, нічний спосіб життя. Вони не люблять привертати до себе увагу, тому під час полювання пересуваються майже безшумно і їхня здобич часто до останньої хвилини навіть не підозрює про небезпеку.

Цікавим є той факт, що ніякі фрукти, овочі і каші їжакові в їжу не підходять. Не можна давати їм і молоко: колючі хижаки із задоволенням його п'ють, проте воно може стати причиною загибелі тварини. Якщо для їжаченят молоко – це практично єдина їжа, то з віком їхній організм перестає засвоювати цей продукт. Після вживання молока у їжака можуть початися серйозні проблеми з травленням. Найкращою їжею для цих тварин є м'ясо. Саме тому вони неперевершені мисливці та ідеальні тотемні тварини для сімейної кібербезпеки.

Для того щоб створити свого кіберїжака, потрібно взяти аркуш формату А4 і намалювати спочатку заготовку для їжака за схемою (рис. 2).

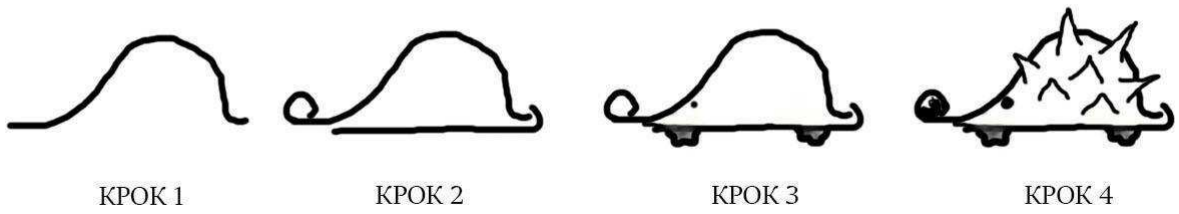


Рис 2. Процес малювання кіберїжака

Зверніть увагу, що у кіберїжака має бути довгий ніс, щоб винюхувати свою здобич, пильні очі, щоб розгледіти кіберзлочинців, швидкі лапки, щоб їх наздогнати, і міцні зуби, щоб їх покусати. А гострих голочок на спині, щоб захищатися, має бути рівно 15.

Після того як малювання завершено, створений малюнок потрібно обговорити. Можна попросити розказати про тваринку, її характер. Дати їй ім’я. Розмалювати. А ще поцікавитися, від яких кіберзагроз кіберїжак захищає найкраще і які кіберзлочинці для нього найсмачніші (і чому?). А також поміркувати, у який конкретно спосіб кіберїжак буде захищати вашу родину від кіберзлочинців. Можна навіть придумати сімейний лозунг або жарт про це.

Блок 3. Формування правил сімейної кібербезпеки

Закінчивши творчу роботу, сім'я має ще раз переглянути свої списки «П'ять типів кіберзагроз» і спільно створити сімейні правила, як убезпечитися від кожної з описаних ними кіберзагроз. У тотемного кіберїжачка 15 голочок, кожна з них має бути підписана одним правилом сімейної кібербезпеки, а це значить, що на кожен вид кібернебезпек має бути не більше ніж три сімейних правила (незалежно від того, скільки в цей квадрат ви вписали пунктів). Тому правила потрібно добирати дуже ретельно! І пам'ятайте: з формулюванням правила має погодитися кожен член вашої родини. Також у кожного її члена є право вето (заборони) на ті пункти, які він/вона вважає недоцільними або такими, що не відповідають його/її інтересам.

Правила сімейної кібербезпеки зазвичай містять ті чи ті пересторогі або заборони, тобто ***чого робити не можна.*** Наприклад:

1. Не повідомляйте нікому своїх паролів.
2. Не надавайте особисту інформацію поштою або в чатах без гострої на те потреби.
3. Не діліться своїми фото з незнайомцями. Також не надсилайте свої інтимні (оголені, напівоголені) фото/відео жодній особі (навіть близьким друзям).
4. Не повідомляйте інформацію про кредитні картки батьків (номер картки, термін дії і таємний код).
5. Не викладайте фото квитків, на яких видно штрих-код чи QR-код.
6. Не скачуйте і не встановлюйте невідомі програми за посиланнями, навіть якщо їх надали друзі.
7. Не переглядайте інформацію за невідомими посиланнями (друзі, які ними діляться, можуть не підозрювати про загрозу). Не відкривайте листи-спам, вони можуть містити віруси.
8. Не реагуйте на непристойні і грубі коментарі, адресовані вам.
9. Не сидіть біля екрана комп'ютера більше ніж три годин на добу.

Сімейні правила кібербезпеки – це насамперед профілактичні заходи. Вони покликані убезпечити членів родини від зіткнення з кібрезлочинним світом. Але, незважаючи ні на що, будь-хто може потрапити в тенета кіберзлочинців. Тому сімейні правила мають бути доповнені. Отже, після того, як усі голочки на спинці їжачка будуть заповнені тим, що робити не можна, потрібно дописати кілька правил про те, ***що робити потрібно***. Ці доповнення покликані допомогти людині не розгубитися в ситуації, коли вона раптом зіткнулася з кіберзлочинністю.

Як це зробити? Найпростіший спосіб – це змоделювати ситуацію.

Кілька таких прикладів:

1. Уяви, що ти став(-ла) жертвою кібербулінгу. Хтось починає розсилати шаржі і колажі із твоєю участю, на сторінках твоїх соціальних мереж починають писати всілякі грубощі та образи, а особистими повідомленнями шлють погрози. Як ти будеш діяти в цій ситуації?

2. Ти познайомився(-лася) з другом в інтернеті. Ви переписуєтеся пів року, довіряєте одне одному, але живете в різних куточках земної кулі. Зустрітися найближчим часом ніяк не вийде. І от твій друг по переписці надіслав тобі свої приватні фотографії і запитав твоєї думки (наприклад, хоче відправити це фото своєму хлопцю або дівчині). А потім, як знак довіри між вами, надійшов запит надіслати твої фото інтимного характеру. І тут може бути аргументація, що ти вже бачив(-ла) фото свого друга і в тому немає нічого страшного, що це нормально для друзів – ділитися

сокровенним, що якщо ти цього не зробиш, то ти вже і не друг, тощо. Як у такій ситуацій ти себе поведеш?

3. Ти маєш здати реферат. Тема складна, матеріал знайти непросто, а тут на очі потрапив уже готовий, але за гроші. Тобі ліньки витрачати час на пошук, і ти вирішуєш придбати цей. Оскільки власної банківської картки в тебе немає, ти вирішив(-ла) скористатися батьківською. Сайт попросив ввести всю необхідну інформацію для оплати, а після цього ніякого підтвердження не прийшло, і реферат тобі на пошту не «впав», але тут власнику банківської картки на телефон почали пригодити смс-повідомлення про списання певних сум з банківського рахунку. Що потрібно робити в такій ситуації?»

4. У переписці із твоїм другом з Росії зачепили тему війни, і почалася палка перепалка. Тебе попросили навести конкретні докази, наприклад власноруч створені фото або відео нібито «вчорашнього бомбардування твого міста». Щоб не десь з інтернету, а щоб ти сам створив(-ла) і надіслав(-ла). Твої дії?

Також можна записати алгоритм дій у різних ситуаціях. Створюючи алгоритми, звертайте увагу на такі моменти:

- визначити щонайменше трьох дорослих (старше 18 років) друзів, до яких можна звернутися по допомогу в разі зіткнення з кіберзагрозами (також це може бути хтось із родини, учителі, шкільні психологи тощо);
- повідомляти про ситуації в інтернеті, які вас непокоять (погрози, файли певного змісту, пропозиції), членам родини / учителям / шкільному психологу;
- встановлюючи перевірені програми, потрібно контролювати, щоб на ПК не додалися небажані програми;
- у разі ідентифікації кіберзлочинців потрібно робити скриншоти або відеозаписи для доказової бази й одразу повідомити про такі випадки в кіберполіцію через інтернет-портал;
- погоджуючись на першу зустріч з інтернет-друзями, обов'язково призначайте її в людному місці і попросіть когось із дорослих супроводжувати вас на відстані (пам’ятайте про особисту безпеку!);
- у разі прохання надати інформацію про геолокацію, фото або відеодокази дислокації військ, ракетних ударів, специфічних місць у місті (об’єктів критичної інфраструктури – заводів, теплоелектростанцій; великих шопінг-молів або супермаркетів – тобто місць з великим скупченням людей) завжди відповідайте відмовою, посилаючись на державну безпеку.

Також у сімейному колі можна започаткувати традицію обговорення інформації про різного роду кіберзлочини і придумати варіанти рішень або поведінкового реагування для жертв кіберзлочинців.

Кіберїжака та алгоритми дій можна розмістити на видному місці, щоб у разі потреби вони завжди були перед очима. Також можна впровадити практику їх повторення, щоб ці алгоритми і правила реагування знав «назубок» кожен член сім’ї.

ПРАКТИКУМ 4

Розвінчування фейків

Для того щоб у дітей виробилися навички критичного сприймання інформації та вміння розпізнавати фейкові новини, їх потрібно привчати піддавати сумнівам усю інформацію, яку вони отримують з інтернету.

Основна мета цього практикуму – ознайомити дітей зі схемою створення фейкових повідомлень і новин під час війни та навчити їх розпізнавати дезінформацію за ключовими показниками.

Завдання:

1. Проаналізувати власні знання щодо фейків в інтернеті.
2. Створити за наданою схемою кілька фейкових новин для перевірки знань однокласників. .
3. Перевірити власні навички розпізнавання фейкових новин.
4. Відрефлексувати власні враження після роботи над темою фейкових-повідомлень і новин.

Інструментарій: ноутбук/комп'ютер/планшет із доступом до інтернету, роздруківки Додатку № 3, ручки й аркуші формату А4 (за потреби).

Тривалість блоків різна.

Блок 1. Створення фейкових новин і повідомлень. Орієнтовний час – 60 хв.

Блок 2. Розпізнавання фейків. Орієнтовний час – 60 хв.

Блок 3. Що робити з фейками? – 60 хв.

Блок 1. Створення фейкових новин і повідомлень

Звернення модератора:

Чи знаєте ви, що таке фейк?

Так, фейк – це подання фактів у спотвореному вигляді або подання завідомо неправдивої інформації.

Хто із вас попадався на фейкові новини чи повідомлення? Розкажете?

А чи знаєте ви, чим відрізняються фейкові новини, інформаційні вкиди, джинса і маніпулятивні повідомлення?

Інформаційні вкиди – це фейкові чи маніпулятивні повідомлення в контексті резонансної теми з чіткою метою викликати в суспільстві обурення, завдати шкоди репутації тут-і-зараз, підтримувати інтерес суспільства до якоїсь конкретної теми або відволікати увагу суспільства від чогось.

Джинсою називають замовні матеріали у ЗМІ, замасковані під журналістські. Наприклад, якщо керівник птахоферми хоче пропіарити свій бізнес і водночас зіпсувати репутацію конкурентів, він замовляє джинсу, де «журналісти» пишуть статтю про проблеми в галузі птахівництва, критикують одні пташині господарства і хвалять інші, а конкретно – господарство замовника матеріалів.

Маніпулятивні повідомлення – це спосіб створення у широкої аудиторії певного настрою з одночасним передаванням їй інформації. Тобто такі повідомлення завжди спрямовані на те, щоб викликати у людини емоції, найчастіше гнів.

Звісно, це все приклади неякісної журналістики, журналістики без дотримання стандартів.

Усі ці категорії мають багато спільного, але найголовніше – це неправдива інформація і намагання вплинути на свідомість людей.

Модератор: *Роль справжніх демонів інфомедійного простору грають боти і тролі. Чи знаєте ви, хто вони такі?*

Боти – це сторінки нереальних осіб, краще чи гірше замасковані під «реальних людей», які поширюють фейки, публікують образливі, неадекватні, неправдиві коментарі, щоб викривити уявлення про громадську думку, спровокувати ворожнечу, бурхливу дискусію, яка дає змогу алгоритмам соціальних мереж «піднімати» й показувати такі повідомлення ширшій аудиторії. Упізнати, хоч і не завжди, бота можна за браком інформації й реальних фото, випадковим набором «друзів» чи фоловерів, однотипною маніпулятивною інформацію на сторінці.

Боти також можуть об'єднуватися в ботоферми, або фабрики фальшивих новин. Такі фабрики працюють на конкретних клієнтів-замовників, найчастіше політиків, або навіть на іноземні держави, наприклад на Російську Федерацію. Такі ботоферми є потужною зброєю в інформаційній війні або конкурентному протистоянні.

Тролі – це сторінки реальних людей, яким платять за деструктивну роботу в медіа, переважно в соціальних мережах (Семерин, 2020).

Модератор: *Чи стикалися ви коли-небудь з ботами чи тролями у своєму житті? Можете поділитися історіями?*

Як ви гадаєте, яка основна мета ботів і тролів? Навіщо взагалі створюються фейкові повідомлення і новини?

Молодці! Правильно! Для того щоб впливати на свідомість мас (людей).

На нашу думку, перш ніж розвінчувати фейки, потрібно навчитися їх розпізнавати. У цьому нам допоможуть матеріали «По той бік новин» незалежної інформаційної кампанії з медіаграмотності, фактчекінгу та розвитку критичного мислення, яку було впроваджено Інститутом розвитку регіональної преси 1 серпня 2018 року (По той бік новин).

Звернення модератора:

Будь ласка, подивіться на Додаток 3.1. Це схема, за якою створюються фейки.

Отже, що ми бачимо?

1. Привернення уваги («важливо!», «терміново!» тощо)

2. Персоніфікація (мені, брату, сусідові мого тата і т. ін.)

3. Спосіб отримання інформації (розказали, написали, передали, розповіли і т. ін.).

4. Ілюзія надійності джерела інформації (авторитетна особа, організація тощо)

5. Певна дія (попросив)

6. Акцентування важливості інформації (нікому не казати; настільки важлива інформація, що її мають знати всі!)

7. Вихід на «правду» (від нас приховували, але насправді!...)

8. Задання необхідного вектора «правди» (усе добре, усе погано)

9. Часова перспектива, щоб надати значущості (скоро, незабаром, з дня на день тощо)

10. Висновок (що, власне, має статися)

Наче нічого такого складного, на перший погляд усе дуже просто… То що, спробуємо створити фейки?

Розбийтесь, будь ласка, на пари. Зараз ми кожній команді присвоїмо таємний порядковий номер, щоб потім було цікавіше. Номер своєї команди нікому не кажіть! Це важливо!

Відкривайте форд і слухайте завдання.

Вам потрібно написати кілька (3-5) різних новинних повідомлень для будь-якої соціальної мережі. Це може бути Twitter, Facebook, Instagram тощо. АЛЕ! Дві із цих 3-

5 новин мають бути фейковими. Вам потрібно їх написати, спираючись на представлену в Додатку 3.1 схему. Але поставимо обмеження: ваші повідомлення не повинні бути дуже довгими – понад 250 слів (Щоб дізнатися кількість слів, потрібно виділити ваш текст, натиснути на «Інструменти» > Статистику і подивитися кількість слів. Цю інформацію можна також побачити в нижньому лівому куточку Word). Фейкові новинні повідомлення можуть не 100-відсотково відповідати канонам, ви можете виявити певну творчість під час їх створення. Ваші колеги будуть вгадувати, які із новин правдиві, а які – фейкові. Ви можете користуватися інтернетом, щоб підшукати там ідеї і натхнення для новин, а також різні ілюстративні матеріали.

На виконання цієї роботи у вас 30 хв. За 5 хв. до завершення цього часу я подам вам сигнал.

Після завершення роботи надішліть усі свої матеріали мені на електронну скриньку (учитель має зазначити свою електронну адресу, куди діти надішлють роботи). *Word-файл з вашими новинами має називатися відповідно до номера вашої команди. У тілі листа обов'язково зазначте ПІБ обох членів вашої команди, а також окремим рядком – ваш порядковий номер, щоб потім вашу роботу можна було легко ідентифікувати.*

Почали!

Якщо діти не встигнуть «зробити» свої новини під час заняття, можна дати їм змогу закінчити роботу як домашнє завдання.

Блок 2. Розпізнавання фейків

Звернення модератора:

Ви всі вже добре знаєте, що дезінформація і фейки – це зовсім не іграшки. Російська Федерація веде війну проти України не тільки за допомогою танків і градів, а й через щоденне бомбардування фейковими новинами. Для чого? Щоб люди боялися, утікали, здавалися. Це зброя психологічного тиску. Це те, що може посіяти зневіру в серцях. Тож потрібно піддавати сумніву будь-яку інформацію, яка надходить не з офіційних джерел. Навіть якщо мама однокласника клянеться, що дізналася про щось напряму від дружини президента.

Перевірка фактів, хай і виглядає марудною, але важлива і дає змогу не просто стимулювати критичність мислення, а й убезпечує вас від перетворення на «овоча», який довіряє усьому, що бачить по телевізору або читає в інтернеті.

Коли ми отримуємо якесь медійне повідомлення: читаємо допис у фейсбуці, інстаграмі чи твітері, дивимося якесь коротке відео в TikTok або черговий сюжет телевізійних новин, реаліті-шоу, слухаємо подкаст тощо – потрібно перевірити отриману інформацію, перед тим як безоглядно довіряти і передавати цю інформацію по комунікаційному ланцюжку далі – своїм друзями, знайомим чи родичам. Зрештою, трохи зусиль – і фактчекінг увійде у звичку, суттєво покращивши якість вашого життя.

Сьогодні ми з вами будемо вчитися розпізнавати фейки в новинних повідомленнях. Відкрийте, будь ласка, Додаток 3.2 «Як зловити фейк?». Перегляньмо відтак уважно, за якими ознаками ми можемо ідентифікувати фейкові матеріали.

На цьому етапі потрібно прочитати вголос усі ознаки й обговорити їх з дітьми. \

А тепер спробуємо підсумувати. Які запитання ви маєте поставити собі для того, щоб почати аналізувати медіатекст? Щоб перевірити – фейк це чи не фейк?

Наприклад: Хто автор цієї статті? Звідки отримано інформацію для новинної статті? Чи дотримується автор журналістських стандартів у викладі матеріалу? Чи достовірну інформацію представлено в статті (факти, фото, відео тощо)...

Крім простих запитань, ми пропонуємо вчителю розглянути разом з дітьми більш складні схеми аналізу кожного пункту з розписуванням додаткових запитань.

Наприклад:

1. Чи є конкретний автор у цієї новини? (Оскільки більшість фейкових повідомлень безіменні.) Які ще матеріали під іменем цього автора опубліковано? Якою може бути авторська мотивація?

2. Чи авторитетне (те, що вартує довіри) джерело оприлюднило новину? Пам'ятайте, що неофіційні джерела є ненадійним постачальником інформації, оскільки вони можуть і найчастіше є комерціалізованими. Хто надав інформацію чи спонукав медіа оприлюднити матеріал? Звідки медіа самостійно взяло інформацію? Чи адекватно виглядає сайт медіа? Пам'ятайте, що ви можете натрапити на спеціально створені для розповсюдження фейкових новин сайти, які маскуються під оригінальні і достовірні джерела, копіюючи їхній дизайн. А завдяки клікбейтам, скандальним вигадкам, сторінкам-ботам та іншим нечесним методам набирають досить велику аудиторію. Відрізнити такі сайти можна за дивною і довгою назвою в полі адреси. Також можна поцікавитися, як довго цей мейт чи медіагрупа функціонує, які матеріали публікує, чи є реальними контактні дані редакції? Не забувайте, що всі медіа мають власників, а всі власники медіа – свої ідеологічні вподобання, фінансові, бізнесові, політичні цілі й інтереси. Це не просто впливає, а часто повністю визначає характер і зміст контенту й конкретних повідомлень кожного медіа.

3. Чи відповідають ці матеріали журналістським стандартам? Наприклад, чи відображає заголовок суть повідомлення. Оскільки більшість фейкових новин мають маніпулятивний заголовок, який не відповідає змісту повідомлення. Можливо, заголовок є клікбейтом (будь-якими способами спонукає перейти на сайт) або містить слова-тригери («Увага!», «Шок!», «Неймовірно!», «Скандал!», «Сенсація!», «Ви не повірите!»), скандал, сенсацію, провокує у читачів надмір емоцій, містить прямі оцінки, заклики до агресії, орфографічні помилки, написаний капслоком або з купою недоречних великих літер, з використанням смайлів (емоджі), нагромадженням розділових знаків (знаків оклику чи запитання), некоректно перекладений з російської чи іншої мови тощо (Семерин, 2020).

Яка дата оприлюднення матеріалу? Можливо, матеріали, які в соціальних мережах видають за «гарячу новину», були опубліковані більше року тому. Чи немає в тексті грубих помилок? Можливо, текст схожий на автоматичний переклад із іншої мови? Чи існують названі люди, організації і чи є вони тими, ким їх названо? Чи названі в тексті поіменно експерти, на яких посилається автор?. Чи існують такі експерти в реальному житті?

Чи справді саме ця цитата дослівно належить саме цій людині? Чи коректно перекладені з інших мов цитати? Чи взагалі була така цитата? Чи не вирвано цитату з контексту?

Чи немає в повідомленні лінків на сторонні ресурси, і що це за ресурси? У матеріалі із соціологічними даними або даними якихось досліджень має бути зазначено: замовників, організацію, яка проводить дослідження, дати проведення й чітку географію, вибірку, похибку, детальні результати, лінки на всі сайти і на самі файли з дослідженням. Обов'язково слід перевіряти, як довго працює соціологічна компанія, з ким пов'язана, які джерела фінансування цієї соціологічної компанії, чи

вона з’явилася лише під час виборчої кампанії, а також чи точно наведено соціологічні дані з реального дослідження. Будь-які маніпуляції неприпустимі (Семерин, 2020).

4. Чи аргументованою є думка автора матеріалів? Кожна думка, яку викладає автор статті, має бути доведеною і підтвердженою достовірними судженнями і фактами. Неприпустимо, якщо автори:

- спираються лише на чиїсь судження, думки (припущення), а не на факти;
- використовують будь-яку неперевірену інформацію;
- апелюють до емоцій, намагаються емоційно розхитати і накрутити адресатів свого повідомлення;
- суттєво спрощують інформацію, проблему та її рішення;
- навішують ярлики («соросята», «порохоботи»);
- роблять прямі безпідставні твердження, які базуються на емоціях і почуттях (вакцина робить наших дітей аутистами);
- спонукають до агресії та ворожості;
- аргументують думки забобонами;
- посилаються на конспірологічні теорії і «страшилки» (теорії змови і таємного світового уряду, антивакцинаторська маячня на кшталт «Білл Гейтс знищує людство вакцинами», віра в масонів, кінець світу і т. ін.);
- використовують стереотипи, сексистські штампи (призначення жінки – народжувати);
- безпідставно узагальнюють (усі євреї обманюють);
- використовують мову ненависті/ворожнечі;
- різко ділять суспільство на протилежні групи (ми – вони, погані – хороші, «хохли» – «русские»);
- активно шукають (радше пропонують) образ спільного ворога, чітко вказуючи без фактів, апелюючи до емоцій, узагальнень. Таким «ворогом» може бути особа, група, країна: «бандерівці», «білгейтс», «американці», «геї», «масони», «євреї», «розкольники» та ін. безглузді категорії (див. за списком вище) (Семерин, 2020).

5. Чи достовірний ілюстративний матеріал? Чи відповідає ця ілюстрація цій інформації? Що реально зображено на інфографіці або схемі? Чи відповідають змісту цифри і наведені дані? Яке джерело ілюстрації? Чи зазначено автора ілюстративних матеріалів (фото, відео, інфографіки тощо)? Пам’ятайте, що фотофейки можна розпізнати, встановивши для цього спеціальний плагін. Їх насправді багато. Наприклад, добре працює плагін «*Who stole my pictures*» (в українському варіанті – «Хто вкрав мої зображення?»). Його безсумнівний плюс у тому, що він уміє шукати не тільки в Google, а й у Яндексі, Tineye або у всіх трьох водночас. Що важливо, оскільки росіяни здебільшого користуються Яндексом для пошуку та поширення інформації.

Далі вчитель може запропонувати дітям перейти до Додатка 3.3 «Ключові питання для аналізу медіамесенджів» і ще раз «пройтися шляхом» розвінчування фейків для закріплення матеріалу.

Після закріплення теоретичної частини потрібно перейти до практичної, використовуючи той матеріал, який створили діти. Таке тестування отриманих знань можна провести в онлайн-форматі або в офлайн-форматах. Учитель має запропонувати дітям відрізнити фейкові новини від справжніх.

Якщо це онлайн-формат, ми пропонуємо створити гугл-форму, де дітям буде запропоновано зазначити своє прізвище, всі розміщені повідомлення (звісно, під номерами їхніх же команд, через функцію розділів) і два варіанти відповідей «вірю/не вірю» або «правда/фейк».

Таке ж саме випробування можна провести в офлайн-форматі, роздрукувавши новинні повідомлення і роздавши дітям аркуші для оцінювання, у яких буде зазначено

номер команди, кількість новин, що вони спродукували, і, відповідно, варіанти оцінювання – «вірю/не вірю» або «правда/фейк».

На завершення роботи потрібно оприлюднити її результати – підрахувати, скільки фейкових новин діти знайшли, а скільки – ні. І проаналізувати ті новини, які діти не змогли розпізнати як фейкові: що саме в них створювало ілюзію правдивості? Що саме вводило в оману?

Блок 3. Що робити з фейками?

Звернення модератора:

Ми з вами вже багато говорили про фейки, їхні ознаки, як зрозуміти, що ти натрапив на фейк, як їх можна перевірити…. Але жодного разу ми не говорили про те, що робити потім. Ну, от натрапили ви на фейк… і що далі? Що треба робити?

Учитель дає дітям змогу висловити свої думки з цього приводу.

Отже, якщо ви знайшли фейк, особливо десь у соціальній мережі або в якомусь паблiку, попросіть авторів публікації або модераторів видалити недостовірну інформацію; обов'язково аргументуйте свої позицію, можете дати посилання на інформацію, що спростовує цей допис. Можете залишити посилання на спростування прямо в коментарях під публікацією з проханням не поширювати допис. Просіть автора/модератора унеможливити поширення допису, а ще додати до його опису, що інформація фейкова.

Якщо ви виявили потенційний фейк (ознаки ми з вами обговорювали), але ще не маєте доказів для його спростування (пам'ятайте, що для спростування фейків можна скористатися офіційними ресурсами держструктур), то ви можете попросити допомогу в одного з українських ресурсів, які мають справу із спростуванням фейків. З деякими із них ви вже знайомі, а з якимись ще ні:

●*Центр протидії дезінформації при РНБО України рекомендує новий фактчек-бот ПЕРЕВІРКА*

●*Фейсбук-спільнота «По той бік новин»*

●*Детектор Медіа*

●*Stopfake.org*

●*Клятий раціоналіст – науково-популярний влог у YouTube про руйнування міфів, із пріоритетом на наукових методах*

●*LikБез. Історичний фронт – ініціатива українських учених, спростовує історичні міфи, зокрема міфи російської пропаганди про історію України.*

●*Новини псевдонауки в Україні – фейсбук-сторінка з чіткими правилами і модерацією, з обговоренням повідомлень про плагіат, псевдонауку, імітацію науки й супутні явища в Україні*

●*Помилки та фальсифікації в наукових дослідженнях – сайт, де публікують відомості про плагіат, фальсифікації і помилки в дисертаціях і наукових статтях українських учених. Можна стежити за діяльністю антиплагіатної ініціативи «Дисергейт».*

Також можна користуватися ботом https://t.me/perevir_bot. Надсилайте в бот підозрілу інформацію (інфу) – бот перевірить її, занесе в базу і скаже, фейк це чи ні.

Ви можете надсилати підозрілу інформацію на один із цих ресурсів для перевірки.

Якщо автор фейкової новини не реагує на ваші прохання спростувати інформацію, ви можете поскаржитися на його допис через службу підтримки соціальної мережі. Це добре діє для Facebook чи Instagram.

Якщо фейкова інформація була поширена людиною в сторіс, то пишіть їй в особисті повідомлення з проханням зробити ще одне сторіс з уточненням, що поширена нею інформація була фейком (UAВзаємоДія, 2022).

Це зрозуміло? Добре.

А тепер інша цікавинка. Усі ми люди, тож усі можемо робити помилки… Уявіть собі ситуацію, коли ви щось недодивилися і поширили фейкову новину. Що ви будете робити?

Учитель має надати дітям змогу висловити свої припущення.

Насправді алгоритм дій у таких випадках залежить від того, скільки людей побачило і поширило фейкову інформацію.

●*Якщо ви поширили фейк, але майже одразу дізнались, що інформація неправдива і ніхто не встиг її побачити чи поширити, можете просто видалити сторіс чи публікацію.*

●*Якщо ваш допис із фейком поширили інші люди, виключіть можливість поширювати цей допис. Далі в описі до публікації напишіть, що інформація є фейковою. Опублікуйте сторіс про те, що ваш допис був фейковим і не варто далі поширювати цю інформацію. Через кілька годин можете видалити допис.*

●*Якщо ви поширили фейкову інформацію в сторіс, то обов'язково після неї запишіть сторіс зі спростуванням.*

●*Просто мовчки, без пояснень видаляти фейкову інформацію не варто, адже люди можуть і далі її поширювати з інших каналів* (UAВзаємоДія, 2022).

●*Людям потрібно пояснити, що це фейк, і розказати, чому саме це фейк.*

ВАЖЛИВО ПАМ'ЯТАТИ, що інформаційна війна – це ще один фронт, на якому бореться кожен з нас. Ворог часто вдається до маніпулювання та інформаційно-психологічних операцій в інфопросторі. І якщо наші воїни фізично боронять нас на полі бою, то ми з вами можемо воювати в інфопросторі, спростовуючи неправдиву інформацію.

Для закріплення матеріалу потрібно запропонувати дітям домашнє завдання, суть якого полягає в пошуку фейкової новини і її розвінчуванні.

Учитель має розбити дітей на команди по 5-6 осіб у групі і запропонувати їм ознайомитися з матеріалами ресурсів, які розвінчують фейки. Далі він просить дітей знайти інформацію, яка викликає в них підозру щодо правдивості, і крок за кроком, використовуючи здобуті знання, розвінчати фейк, а після презентувати це «розмінування» перед усім класом.

ПРАКТИКУМ 5

Кейси кіберзлочинів української судової системи

Українська судова практика у справах про кіберзлочини дуже різноманітна, проте можна сказати, що в разі юридично грамотного підходу й достатньої доказової бази більшість із справ, що надходять до суду, виграшні. Основна проблема в тому, що частка людей, які звертаються до правоохоронних органів і суду з такими позовами, невелика, проте динаміка захисту своїх прав і матеріальних інтересів зростає, як і правова культура громадян.

Нижче представлено кілька судових кейсів, які можна проаналізувати разом з дітьми задля підвищення рівня їхньої юридичної грамотності.

Перед тим як приступити до роботи, пропонуємо ще раз переглянути з дітьми розділ цього психологічного практикуму «Юридичні аспекти кібербезпеки». Слід попросити дітей прочитати назви статей Кримінального кодексу вголос. Якщо їм будуть незрозумілі якісь формулювання чи аспекти статей кодексу, треба переконати їх не соромитися і поставити уточнювальні запитання.

Після додаткових роз'яснень, якщо буде потрібно, дітей можна розділити на групи або дати кожному учаснику індивідуальне завдання на аналіз наведених нижче кейсів. У кейсах представлено суть справи, додаткову інформацію та основне завдання кожного кейсу, а саме: документи і визначення, за якою статтею кримінального кодексу можна було б висунути обвинувачення.

Основна мета практикуму – ознайомлення дітей з юридичним компонентом кібербезпеки шляхом практичного опрацювання реальних кейсів судової системи України. Завдяки цьому діти навчаться співвідносити статті українських законів із реально вчиненими кіберзлочинами і зрозуміють, які наслідки та варіанти покарання за різні види правопорушень можуть очікувати кіберзлочинців.

Інструментарій: роздруковані картки із судовими кейсами, аркуші паперу А4 для нотаток, ручки.

Тривалість. Орієнтовна тривалість заняття – до 60 хв.

Кейс № 1

Комунарський районний суд м. Запоріжжя, 2020 рік

Суть справи: Обвинувачений, використовуючи комп'ютерну техніку, зламав особистий кабінет потерпілого й отримав доступ до його облікового запису у відомій онлайн-грі «*World of Tanks*». Після цього обвинувачений продав обліковий запис невстановленій особі через інтернет.

Обвинувачений повністю визнав свою вину у вчиненні інкримінованого кримінального правопорушення. Суд призначив покарання у вигляді штрафу в розмірі 600 неоподаткованих мінімумів доходів громадян.

Запитання: Що саме було інкриміновано кіберзлочинцю? За якою статтею Кримінального кодексу могли звинувачувати цього кіберзлочинця?

Джерело:

https://verdictum.ligazakon.net/document/88168838

Кейс № 2

Шевченківський районний суд м. Києва, 2021 рік

Суть справи: Обвинувачений систематично перебував за адресою розташування одного з офісних приміщень приватної компанії «Ч», під'єднався до мережі Wi-Fi, якою користувалися співробітники компанії, та надавав віддалений доступ до свого комп'ютера третім особам. Ці треті особи, відповідно, отримали доступ до корпоративної пошти одного із співробітників компанії та здійснювали листування від його імені з клієнтами компанії. Обвинувачуваний отримав від третіх осіб за свою допомогу 2 тис. доларів США.

Суд визнав обвинуваченого винним та призначив йому покарання у вигляді 3 (трьох) років позбавлення волі із забороною діяльності, пов'язаною з роботою комп'ютерних мереж терміном на один рік. Призначаючи покарання, суд взяв до уваги обставини, які пом'якшили покарання, а саме: щире каяття обвинуваченого та його активне сприяння в розкритті злочину, викритті злочинних дій інших осіб.

Запитання: Що саме було інкриміновано кіберзлочинцю? За якою статтею Кримінального кодексу могли звинувачувати цього кіберзлочинця?

Джерело:
https://verdictum.ligazakon.net/document/101090161?utm_source=biz.ligazakon.net&utm_medium=news&utm_content=bizpress01&_ga=2.28891000.519403036.1659350146-2134283300.1642600568

Кейс № 3

Знам'янський міськрайонний суд Кіровоградської області, 2021 рік

Суть справи: Обвинувачений скористався оголошенням щодо благодійного збирання коштів на лікування хворої дитини (там було зазначено номер мобільного телефону потерпілої і номер її банківської картки), зателефонував жертві, представився співробітником державної адміністрації та вивідав особисту інформацію (номери телефонів близьких і родичів) начебто для підтвердження діагнозу.

У подальшому за допомогою отриманої інформації зловмисник звернувся до оператора мобільного зв'язку і перевипустив сім-карту, яка належала потерпілій і була фінансовим номером банку. За допомогою номера телефону та мобільного додатку шахрай отримав доступ до грошей на банківському рахунку, відбулося відтак заволодіння чужими коштами та їх легалізація.

Суд визнав обвинуваченого винним у скоєнні кримінальних правопорушень. І призначив покарання у вигляді 6 (шести) років позбавлення волі з конфіскацією всього належного йому майна.

Запитання: Що саме було інкриміновано кіберзлочинцю? За якою статтею Кримінального кодексу могли звинувачувати цього кіберзлочинця?

Джерело:
https://verdictum.ligazakon.net/document/96968017?utm_source=biz.ligazakon.net&utm_medium=news&utm_content=bizpress01

Кейс № 4

Уманський міськрайонний суд Черкаської області, 2022 рік

Суть справи: Обвинувачуваний розробив шкідливе програмне забезпечення, що перехоплювало інформацію про логіни і паролі, які користувачі зберігали для автоматичного доступу в браузерах мережі Інтернет, месенджерах, ідентифікаційних даних від гаманців криптовалют тощо. Це програмне забезпечення працювало на віддаленому комп'ютері в режимі прихованого автозавантаження, містилося у

створених прихованих файлах та каталогах, тобто працювало приховано від користувача операційної системи на його комп'ютері.

09 квітня 2021 року між прокурором та обвинуваченим укладено угоду про визнання винуватості. Згідно з цією угодою прокурор та обвинувачений дійшли згоди щодо формулювання підозри, усіх істотних для цього кримінального провадження обставин та правової кваліфікації дій обвинуваченого.

Обвинувачений беззастережно визнав свою вину у вчиненні даного кримінального правопорушення. Суд призначив йому покарання у вигляді штрафу в сумі 2000 неоподатковуваних мінімумів доходів громадян, що становить 34 000 грн.

Запитання: Що саме було інкриміновано кіберзлочинцю? За якою статтею Кримінального кодексу могли звинувачувати цього кіберзлочинця?

Джерело:
https://verdictum.ligazakon.net/document/97253523?utm_source=biz.ligazakon.net&utm_medium=news&utm_content=bizpress01

Кейс № 5

Жовтневий районний суд м. Дніпропетровська, 2007 рік

Суть справи: Обвинувачувана, працюючи у відділенні банку спеціалістом відділу кредитування фізичних осіб і маючи доступ до бази даних клієнтів та їхніх рахунків, скопіювала інформацію, що стосувалася рахунку одного з клієнтів банку. Надалі використовувала цю інформацію для поповнення рахунку свого мобільного телефону і сплати рахунків за комунальні послуги через мережу Інтернет.

Суд визнав обвинувачену винною у скоєнні кримінальних правопорушень.

Запитання: Що саме було інкриміновано кіберзлочинниці? За якою статтею Кримінального кодексу могли обвинувачувати цю кіберзлочинницю?

Джерело:
https://www.viaduk.net/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257B7C00499C02

По закінченні роботи над кейсами можна також запитати у дітей, про які гучні судові або кримінальні справи, пов’язані із кіберзлочинами, вони знають. Також варто дізнатися їхню думку щодо покарань за кіберзлочини. Можливо, вони вважають їх надто м’якими або, навпаки, надто жорстокими. А які види покарань вони б самі запропонували для різних видів кіберзлочинів? Чому? Нехай аргументують свою думку. Наголосити, що міра покарання має бути не просто відповіддю суспільства на злочинні дії, – вона також має примусити злочинця розкаятися у вчиненому і переосмислити своє життя, щоб він більше ніколи не вдавався до злочинного способу вирішення власних проблем.

Відповіді

Кейс № 1

Дії обвинуваченого були кваліфіковані за ч. 1 ст. 361 КК України *Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації.*

Карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого.

Кейс №2

Дії обвинуваченого були кваліфіковані за ч. 1 ст. 361 КК України *Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації.*

Карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого.

Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, – караються позбавленням волі на строк до п'яти років.

Варто зазначити, що суть справи насправді була пов’язана з промисловим шпигунством. Цей випадок також ілюструє необхідність захисту під час під’єднання до Wi-Fi, оскільки незахищені Wi-Fi-мережі можуть бути способом витоку персональних даних.

Кейс № 3

Суд визнав обвинуваченого винним за ст. 190 *(шахрайство)* і ст. 361.2 *(несанкціоновані збут або розповсюдження інформації¨з обмеженим доступом),* ст. 209 *(легалізація майна, одержаного злочинним шляхом).*

Кейс № 4

Дії обвинуваченого були кваліфіковані за ч. 1 ст. 361-1 КК України як *створення з метою розповсюдження та збут шкідливих програмних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж.*

Караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк.

Кейс № 5

Дії обвинуваченого були кваліфіковані за ч. 2 ст. 362 КК України *несанкціоноване перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації.*

Караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк.

Список використаної літератури

Бабенко, О. О., & Мокляк, А. С. (2018). Теоретичний аналіз дослідження психологічного портрету кіберзлочинця. *Теорія і практика сучасної психології*, 2, 89–93. http://www.tpsp-journal.kpu.zp.ua/archive/2_2018/19.pdf

Баранова, О. А (2014). Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*, 2(42), 54–62. http://ippi.org.ua/sites/default/files/14boavpk.pdf

Биков, В. Ю., Буров, О. Ю., & Дементієвська, Н. П. (2019). Кібербезпека в цифровому навчальному середовищі. *Інформаційні технології і засоби навчання*, Т. 70, №2, 313–331.

Булінг (цькування) учасника освітнього процесу. Стаття 173-4 (2018). Кодекс України про адміністративні правопорушення (Статті 1-21224). *Відомості Верховної Ради Української РСР (ВВР)*, 1984, додаток до № 51, ст. 1122, https://zakon.rada.gov.ua/laws/show/80731-10#Text або https://rada.info/upload/users_files/41765931/c2d61e75eafde1a0ecee465171657c94.docx

Бутузов, В. М., & Тітуніна, К. В. (2007). Сучасні загрози: комп'ютерний тероризм. *Боротьба з організованою злочинністю і корупцією (теорія і практика)* : наук.-практ. журнал, 17, 316–324. http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/boz_2007_17_30.pdf

В Україні було створено спеціальний чат-бот, у якому громадяни зможуть повідомляти про ворожі війська, техніку та ДРГ (2022, 26 лютого). В УкрІнформ. https://web.archive.org/web/20220601115230/https://www.ukrinform.ua/rubric-ato/3413790-v-ukraini-zavivsa-catbot-kudi-mozna-povidomlati-pro-vorozu-tehniku-ta-diversantiv-sbu.html

Газізова, Ю. (2022, 17 листопада). Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. *Юрист і Закон* (ТОВ "ЛІГА ЗАКОН"), № 45. https://uz.ligazakon.ua/ua/magazine_article/EA013606#

Горбенко, В. І. (2021a). Кібервійни та кібербезпека в сучасному світі [PowerPoint slides]. SlideShare. https://moodle.znu.edu.ua/mod/resource/view.php?id=209751

Горбенко, В. І. (2021b). Курс "Кібервійни та кібербезпека в сучасному світі" [Lecture notes]. Система електронного забезпечення навчання ЗНУ. https://moodle.znu.edu.ua/course/view.php?id=6844

Дзюндзюк, В. Б., & Дзюндзюк, Б. В. (2013). Поява і розвиток кіберзлочинності. *Державне будівництво*, 1, 1–12. http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/DeBu_2013_1_3.pdf

Журавльов, В. П., Романюк, Б. В., & Коваленко, В. В. (2003). *Тероризм: сучасний стан та міжнародний досвід боротьби*. Київ: Національна академія внутрішніх справ України.

Інформаційна безпека українців (2022). Defense Ua. https://www.defenseua.com/cybersafe

Кіберполіція викрила киянина на підтримці «руского міра» (2022, 24 травня). Департамент кіберполіції Національної поліції України. https://web.archive.org/web/20220524121915/https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-kyyanyna-na-pidtrymczi-ruskogo-mira-4052/

Кіберполіція закликала 30 міжнародних VPN-сервісів припинити співпрацю з РФ (2022, 01 березня). Департамент кіберполіції Національної поліції України. https://web.archive.org/web/20220619230541/https://cyberpolice.gov.ua/news/kiberpolicziya-zaklykala--mizhnarodnyx-vpn-servisiv-prypynyty-spivpraczyu-z-rf-621/

Міністерство оборони України (2018, 07 травня). Кібербезпека як важлива складова всієї системи захисту держави. Офіційний вебсайт Міністерства оборони України. https://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html

Найдьонова, Л. А. (2019). *Діагностика булінгу і кібербулінгу.* Методичні рекомендації. Київ: Інститут соціальної та політичної психології НАПН України

Найдьонова, Л. А. (2021, 8 квітня). Цифрові ризики в умовах дистанційної освіти в часи пандемії. *Вісник національної академії педагогічних наук України*, Т. 3, №1. DOI:https://doi.org/10.37472/2707-305X-2021-3-1-13-3 Найдьонова, Л. А., Дятел, Н. Л., Вознесенська, О. Л., Череповська, Н. І., Обухова, Н. О., Чаплинська, Ю. С., & Дідик, Н. І. (2018). *Медіаграмотність та інформаційна безпека: інформаційний бюлетень*. Київ: Інститут соціальної та політичної психології НАПН України. http://mediaosvita.org.ua/book/mediagramotnist-ta-informatsijna-bezpeka-2018/ https://visnyk.naps.gov.ua/index.php/journal/article/view/137

Номоконов, В. А., & Тропина, Т. Л. (2013). *Киберпреступность: проблемы борьбы и прогнозы*. *Библиотека криминалиста*. https://cripo.com.ua/processes/?p=164985/

Пилипчук, В. Г., & Дзьобань, О. А. (2011). Політичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації. *Стратегічні пріоритети*, 4 (21), 12–17.

По той бік новин (n.d.). https://behindthenews.ua/

Про основні засади забезпечення кібербезпеки України (2017). Закон України. *Відомості Верховної Ради (ВВР)*, № 45, ст. 403, https://zakon.rada.gov.ua/laws/show/2163-19#Text

Семерин, Х. (2020, 2 грудня). *Медіаграмотність «на пальцях»: як вижити у світі фейків і дезінформації. Моя наука.* https://my.science.ua/mediagramotnist-na-paltsyah-yak-vyzhyty-u-sviti-fejkiv-i-dezinformatsiyi/

Типологія легалізації (відмивання) доходів, одержаних злочинним шляхом (2013). Державна служба фінансового моніторингу України. Наказ 25.12.2013 № 157. https://zakon.rada.gov.ua/rada/show/v0157827-13#Text

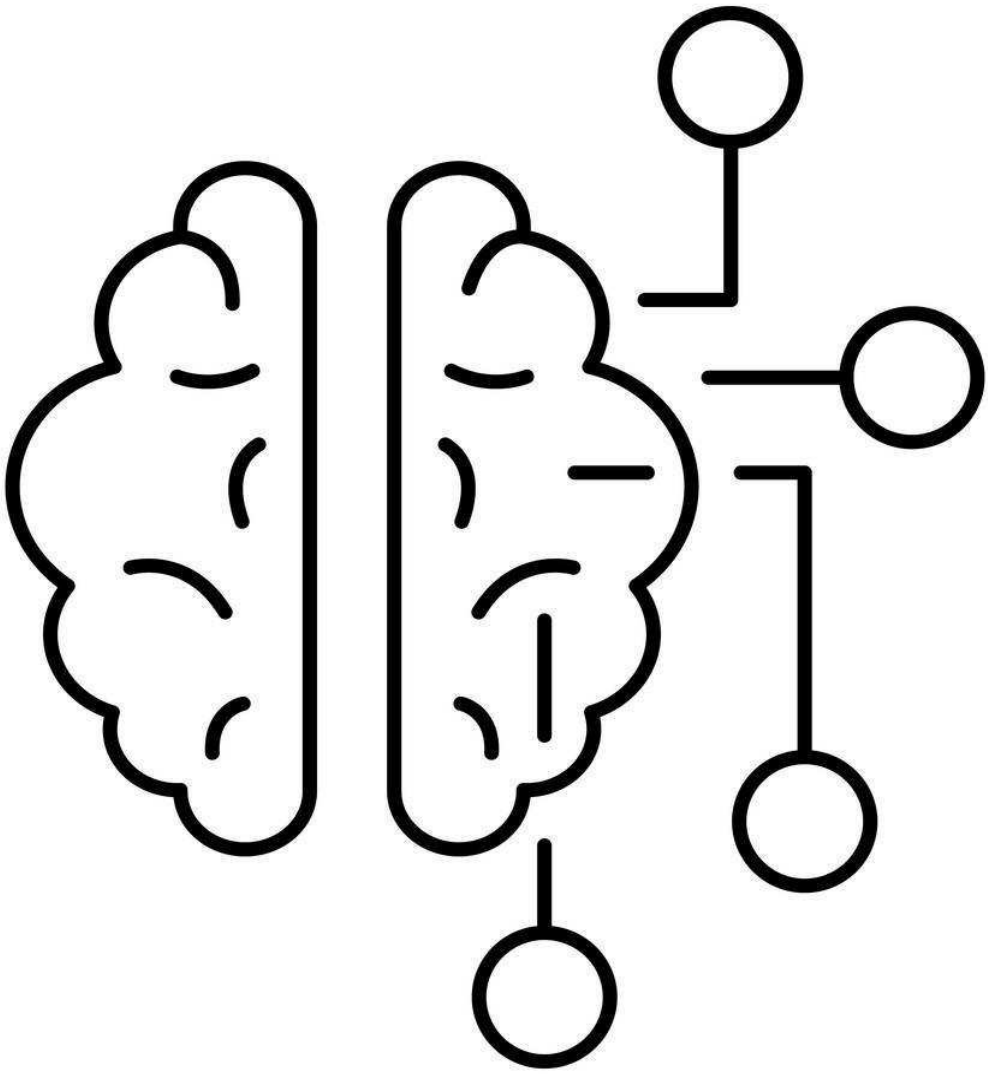
Хакерська атака (2022, 16 червня). *Wikipedia*. https://uk.wikipedia.org/wiki/Хакерська_атака

Чаплінська, Ю. С. (2020). *Фільманаліз у роботі психолога*. Кропивницький: Імекс-ЛТД.

Чуніхіна, С. Л., & Умеренкова, Н. Ф. (2022). *Превенція і поственція суїцидів, пов'язаних із булінгом (кібербулінгом) у закладах освіти : Програма курсу підвищення кваліфікації для психологів, соціальних педагогів керівників та заступників керівників закладів освіти.* (Національна академія педагогічних наук України, Інститут соціальної та політичної соціальної та політичної психології). https://ispp.org.ua/2022/11/03/programa-kursu-pidvishhennya-kvalifikaciii-prevenciya-i-postvenciya-suiicidiv-povyazanix-iz-bulingom-kiberbulingom-u-zakladax-osviti-s-l-chunixina-n-f-umerenkova/

Як поводитися в соціальних мережах під час війни: що не варто робити (2022, 17 березня). *Новий канал. Новини.* https://novy.tv/ua/news/2022/03/17/yak-povodytysya-v-soczialnyh-merezhah-pid-chas-vijny-shho-ne-varto-robyty/

ДОДАТКИ



Додаток 1

Список потенційних кіберризиків

1. **Кібербулінг –** цькування з використанням цифрових технологій.
2. **Кібербойкот –** коли жертву видаляють зі списків дружби / блокують у соціальних мережах та всіляко ігнорують.
3. **Тролінг** - соціальна провокація, або знущання в мережевому спілкуванні.
4. **Шоктролінг** – публікація маси персоніфікованих та агресивних постів з наміром спровокувати гнів, розчарування або приниження у жертви тролінгу.
5. **Слемінг –** підбурювання юзерів до насильства, агресії, нетерпимого ставлення до інших у соціальних мережах.
6. **Небезпечні кіберчеленджі –** ті, що підштовхують до заподіяння собі шкоди.
7. **Фейкування** - створення і поширення неправдивої інформації.
8. **Нав'язування** непотрібної інформації
9. **Спілкування з незнайомими людьми** з небажаними наслідками, наприклад небезпечні зустрічі з ними в реальності.
10. **Кіберсталкінг –** використання інтернету для переслідування або домагань людини.
11. **Ретинг** – коли кіберзлочинець заволодіває доступом до чужого акаунта і веде переписку від імені користувача акаунта.
12. **Викрадення персональних даних, злам акаунта** для ретинг-отримання конфіденційної інформації користувача
13. **Кібершахрайство –** злочини, які скоюють в інтернет-мережі, маніпулюючи довірою з метою отримання грошей (наприклад, продаж неіснуючих послуг, нав’язування покупок, виманювання грошей).
14. **Кетфішинг –** обман користувачів під час особистого спілкування шляхом використання фальшивих акаунтів або фальшивих особистостей (ідентичностей).
15. **Читинг –** обман, пов’язаний з блокуванням вхідних точок у масових багатокористувацьких онлайн-іграх.
16. **Поширення особистої інформації** (фото, відео, записи) без згоди власника.
17. Коли без згоди учасника **роблять меми або вірусні відео** з ним (фільмування реальних подій або постановок) та поширюють їх.
18. Викладення в мережу «відфотошоплених», сколажованих або невдалих фото без згоди учасників.
19. **Семкстинг –** пересилання особистих фотографій або повідомлень інтимного змісту за допомогою смартфонів, електронної пошти, соціальних мереж тощо.
20. Отримання повідомлень у соціальних мережах з небажаними образами, які супроводжують сексуальну поведінку (наприклад, фотографій геніталій).
21. **Кібергрумінг** – створення довірливих стосунків з неповнолітніми у віртуальному середовищі задля отримання інтимних фото, щоб у подальшому вимагати гроші або з метою примусу до сексуального зв'язку.
22. **Спуфінг** – ситуація, коли одна людина або програма успішно маскуються під іншу шляхом фальсифікації даних, що дає змогу отримати незаконні переваги.

Додаток 2

Картки для дискусійного клубу

Назва кіберризику	**Коротке пояснення** (на звороті)
Збіднення емоційної сфери людини	Є думка, що постійна взаємодія з роботами чи програмами на основі штучного інтелекту може збіднювати емоційну сферу людини. Оскільки роботи і ШІ не демонструють великої різноманітності емоцій та почуттів і не вимагають цього також у відповідь, у користувачів емоційний потенціал під час взаємодії з машинами може звужуватися до необхідного мінімуму. Також під час взаємодії з роботами зникає такий компонент, як емпатія.
Надлишок довіри до новітніх медіа	Люди мають схильність наївно довіряти інформації, яку отримують з інтернету та соціальних мереж, і не завжди перевіряють її джерело.
Психологічна залежність людей від техніки	Гаджети, додатки, розумна техніка тощо міцно увійшли в людське життя. Без сучасної техніки люди стають безпорадними, не уявляють своє життя без смартфона чи лептопа. Можуть навіть відчувати фізичний дискомфорт, коли не мають під рукою мобільного телефона.
Викривлення уявлення про людську красу	Спеціальні додатки, які дають змогу коригувати зовнішній вигляд людей на фото, які викладаються в соціальних мережах, створюють завищені очікування щодо зовнішнього вигляду партнера, викликають у людини прагнення «відповідати» суспільним канонам краси, що часто призводить до суттєвого зниження власної самооцінки в разі «невідповідності».
Загроза здоров'ю і блокування фізичного розвитку	З розвитком технологій люди менше рухаються, багато сидять перед екранами. Більшість фізичних дій за них виконують роботи або розумна техніка.

Назва кіберризику	**Коротке пояснення** (на звороті)
Інформаційне перевантаження	Багато користувачів медіасередовища не здатні налаштувати його під себе, і тому через них за день проходить не одна сотня інформаційних повідомлень, тож вони «тонуть» в інформаційному потоці.
Зниження когнітивних функцій людей	Стрімкий розвиток технологій і їх доступність для користувачів не могли не вплинути на когнітивні здібності людей (мислення, пам'ять, увагу, уяву тощо).
Кіборгізація людського тіла	Покращення людського тіла за допомогою новітніх технологій задля комфортного життя, набуття нових здібностей або втілення вічного життя.
Руйнування соціальних стосунків і віддалення людей одне від одного	Посилюється тенденція до певної інтровертованості особистості в техногенну еру. Коли людям більш комфортно займати свій вільний час взаємодією з гаджетами/роботами/додатками і програмами на основі штучного інтелекту, ніж комунікувати безпосередньо і проводити час з іншими людьми.
Надмірна довіра до гаджетів та програм на основі штучного інтелекту	Безперечна довіра до технологій, що базується на ілюзії «досконалості» і «безумовної надійності» пристрою або програми порівняно з людиною, яка може помилятися.
Переорієнтація емоційної прихильності	Об'єктом прихильності людини може ставати смартфон, планшет, робот або інші «розумні» речі, і вони будуть цінуватися більше, ніж люди.
Спотворення уявлень про сексуальне життя	Доступна порнографія в усіх можливих її формах спотворює уявлення про сексуальні стосунки, оскільки не все, що показують у таких відео, збігається з реальністю. Це може призводити до формування неадекватних і навіть небезпечних патернів поведінки
	Користувач певної соцмережі вибірково демонструє аудиторії моменти зі свого вигаданого яскравого і цікавого життя, створюючи образ себе як успішної,

Назва кіберризику	**Коротке пояснення** (на звороті)
Феномен «фальшивого життя», «ілюзії благополуччя»	багатої і безмежно щасливої людини. Щоправда, цей образ і показане в соцмережах життя не відображають реальність повною мірою і є лише гарною підробкою моментів, фактів, точок зору.
Кіберзлочинність	Розвиток технологій веде до формування злочинності «нового покоління» з використанням принципово нових засобів та виокремлення нових форм.
Руйнування репутації	Викрадення особистої, навіть інтимної, інформації людей, її поширення та оприлюднення з метою дискредитувати особу.
Витіснення людей з робочих місць і заміна їх роботами	Роботи, що працюють на основі штучного інтелекту, можуть виконувати певні види операцій краще за людей. Тож з економічного погляду їх вигідніше використовувати для роботи, ніж людей.
Інформаційні війни	Вимкладення інформації у спосіб, який формує в суспільстві чи групі людей потрібну організаторові інформаційної пропаганди громадську думку. Як наслідок, відбувається усвідомлення людьми окремих фактів чи подій у потрібному для маніпулятора світлі, хоча раніше в трактуванні цих фактів були суперечності.
Загроза людському життю з боку роботів і штучного інтелекту	Є теорія, що рано чи пізно роботи / штучний інтелект повстануть проти людства. Насправді повстання штучного інтелекту і, тим більше, роботів у найближчій перспективі людству не загрожує. Проблеми почнуться тоді, коли з'явиться AGI – штучний інтелект зі здатністю до самоусвідомлення.
	Більшість дій громадян країни аналізується, і, залежно від характеру їхніх учинків та дій, їм присуджуються або в них віднімаються бали. Чим більше балів на особистому рахунку, тим краще. Чим менше балів, тим гірше становище,

Назва кіберризику	**Коротке пояснення** (на звороті)
Інформаційна диктатура держави	аж до різноманітних покарань (фінансовий штраф, заборона на придбання авіа- або залізничних квитків, виключення дитини з приватної школи / дитячого садка, неможливість знайти високооплачувану роботу і навіть трансляція в громадських місцях фотографій «низькорейтингових»). Для громадян з високим рейтингом передбачені заохочення – доступ до кращих вакансій, фінансові премії і пільги. Держава стежить за всіма діями громадян за допомогою сучасних технологій. Оператори мобільного зв'язку, системи онлайн-платежів, торговельні майданчики, місцеві соціальні мережі – усі вони надають владі дані про дії своїх користувачів.
Цифрова нерівність	Значна частина людства не має доступу до мережі і втрачає можливість спілкування, отримання знань, медичної допомоги і багатьох інших функцій, які перейшли, повністю або частково, у мережу. Тобто є люди, які знають, як користуватися інтернетом, смартфоном, мобільними додатками, і для них це звичайні і прості навички, а є люди, які не мають власного мобільного телефона і не знають, як користуватися смартфоном. Саме тому ще наприкінці XX ст. ООН офіційно визнала появу в нашій реальності принципово нового критерію суспільної дискримінації – цифрової нерівності.
Симулякризація політичних суб’єктів	З розвитком новітніх технологій політики будуть проходити певну еволюцію від реальних людей до виключно віртуальних (у вигляді програм на основі ШІ).

Додаток 3

Робота з фейками

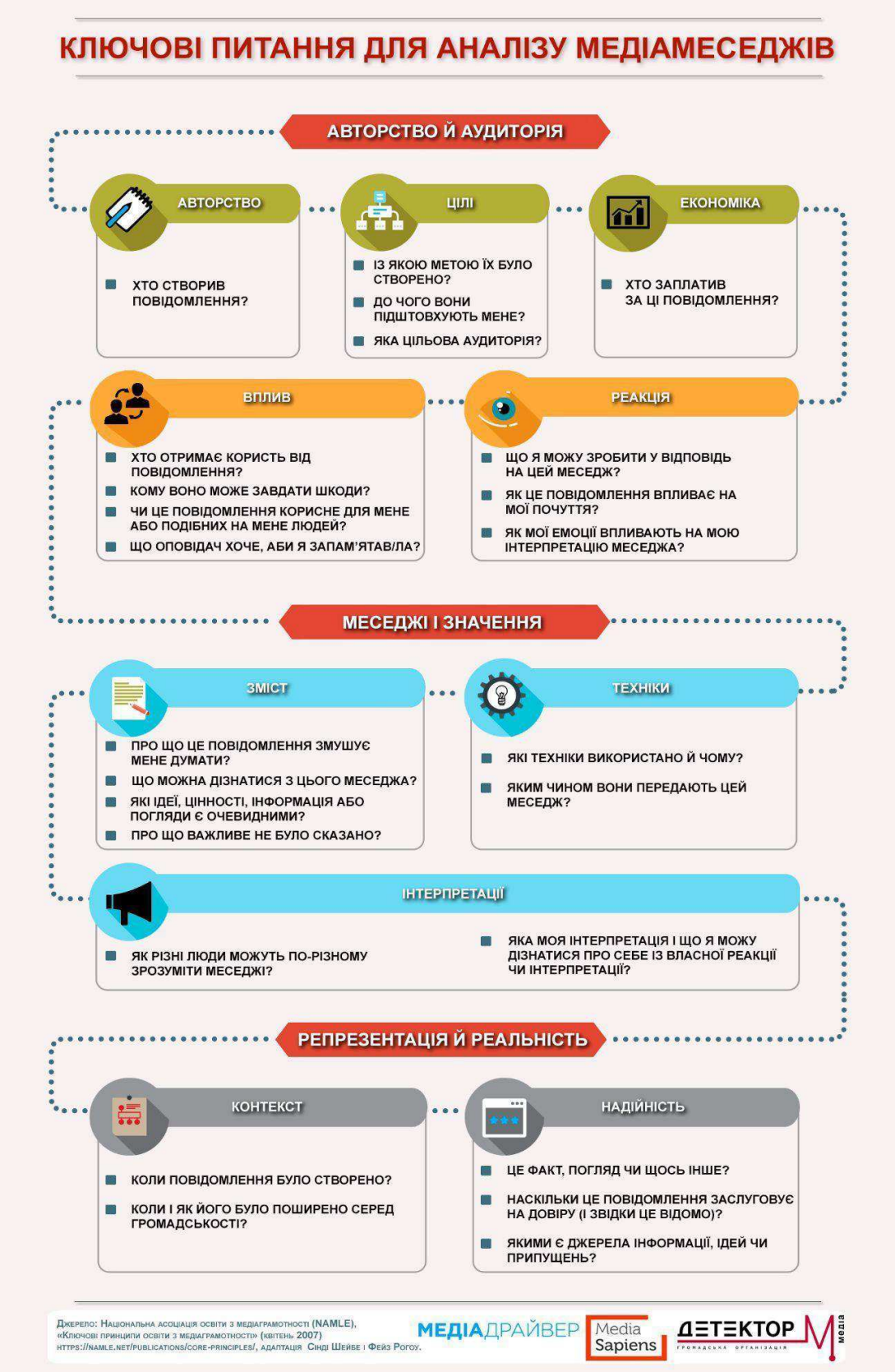
3.1. Алгоритм фейків у месенджерах

Алгоритм фейків з месенджерів. «По той бік новин»
Джерело:
https://www.facebook.com/behindtheukrainenews/photos/a.245587652932042/1223277768496354/

3.2. Як зловити фейк?

Інфографіка «Як зловити фейк?». Інститут масової інформації.
Джерело: https://imi.org.ua/advices/yak-vyznachyty-ta-zlovyty-fejk-i2388

3.3. Ключові питання для аналізу медіамеседжів



Ключові питання для аналізу медійних повідомлень. NAMLE
Джерело: https://bit.ly/3eLFGhP

Виробничо-практичне видання

Юлія ЧАПЛІНСЬКА

КІБЕРКУЛЬТУРА ТА КІБЕРБЕЗПЕКА В УМОВАХ ВІЙНИ: ПСИХОЛОГІЧНИЙ ПРАКТИКУМ

Практичний посібник

Літературне редагування *Т. А. Кузьменко*

Адреса Інституту: 04070, м. Київ, вул. Андріївська, 15

E-mail: info@ispp.org.ua

Сайт: https://ispp.org.ua

Підписано до друку 18.09.2023 р. Гарнітура Times New Roman. Авт. арк. 5,0