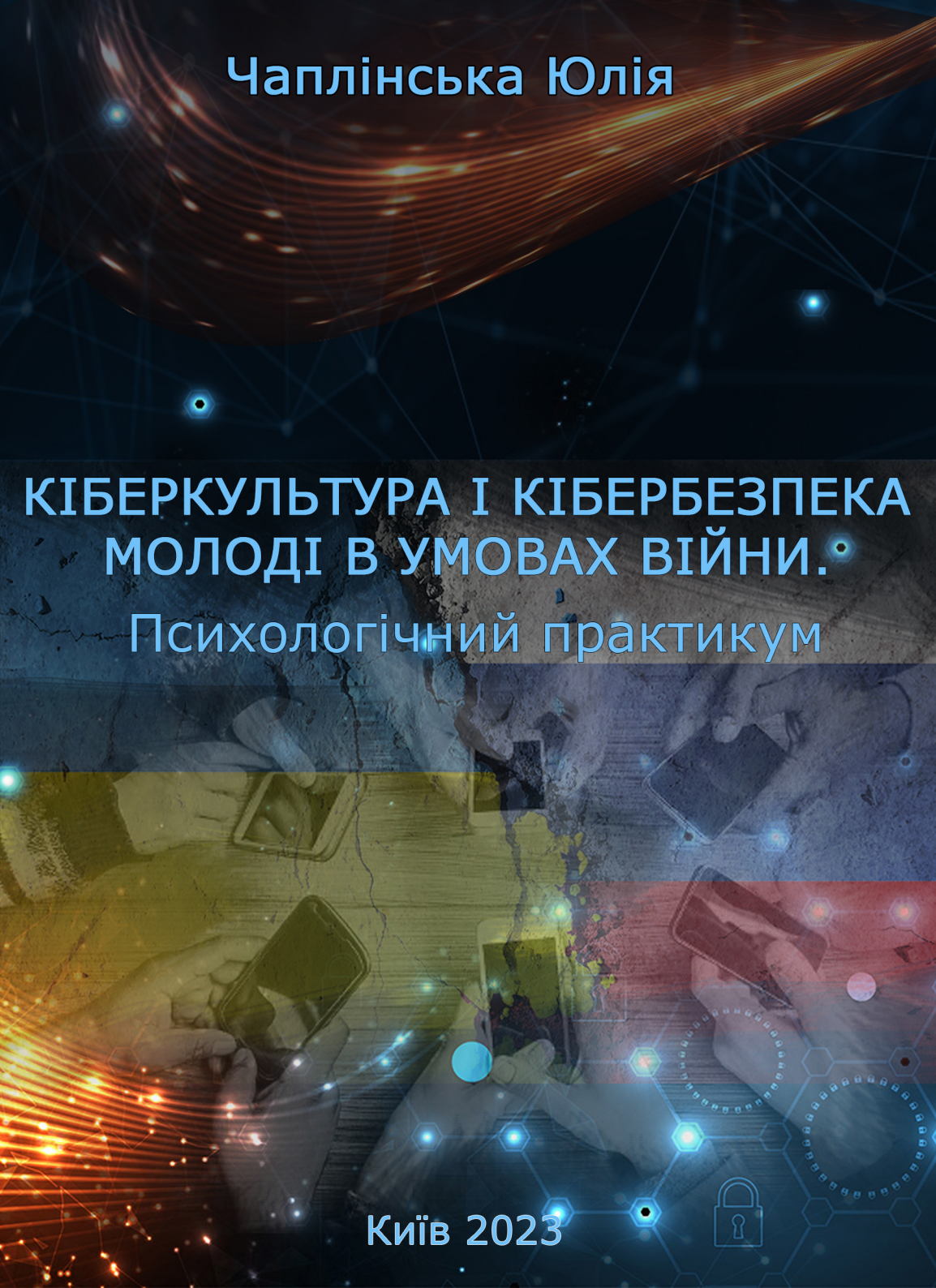
Чаплінська Юлія

# КІБЕРКУЛЬТУРА І КІБЕРБЕЗПЕКА МОЛОДІ В УМОВАХ ВІЙНИ.

## Психологічний практикум



Київ 2023

**Чаплінська Юлія**

# Кіберкультура і кібербезпека молоді в умовах війни. Психологічний практикум

**2023 рік**

**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 науковий 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.С. (2023). *Кіберкультура і кібербезпека молоді в умовах війни. Психологічний практикум*. Національна академія педагогічних наук України, Інститут соціальної та політичної психології, 79 с.

ISBN

Психологічний практикум має на меті підготувати дітей до зустрічі із потенційними кіберризиками з якими вони можуть зіткнутися в інтернет середовищі. Особливо це актуально стає за воєнних часів. Практикум складається із двох частин. В першій, теоретичній, частині представлено понятійний апарат кіберзагроз та розписані практичні та юридичні аспекти кібербезпеки у мирний та воєнний час. Також описано поняття воєнної кібербезпеки та її ключових моментах (безпека мобільних пристроїв, двоетапна аутентифікація, програмне забезпечення, безпека соціальних мереж, неправдиві повідомлення або фейки, ненадійні сайти та посилання). Окремо зосереджено увагу на юридичних аспектах кібербезпеки, нормативних та правових документах, що регулюють дану область, як в Україні, так і в світі. Також розписана діяльності кіберполіції в Україні, як у воєнний, так і у мирний час.

У другій частині представлені п’ять практичних занять для дітей, направлених на закріплення матеріалу, представленого у теоретичній частині. Вони покликані створити у свідомості дітей цільну картину кіберризиків з якими вони можуть зіткнутися у мирний час і узагальнити та доповнити знання про кіберзагрози воєнного часу. Особлива увага приділяється питанню протистоянню кібернебезпекам та формуванню алгоритму дій у критичних ситуаціях.

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

УДК **159.316.772.5**

ISBN

Видано державним коштом. Продаж заборонено

**Зміст**


**ВСТУП** 5

**ЧАСТИНА І** 14

**1.2. ВІД КІБЕРРИЗИКУ ДО КІБЕРВІЙНИ** 15

Кіберризик 15

Кіберзлочин 16

Кібертероризм 18

Кібервійна 19

**1.2. КІБЕРБЕЗПЕКА ТА КІБЕРКУЛЬТУРА** 21

Індивідуальна безпека 21

Групова/організаційна безпека 23

Державна безпека 24

Алгоритм дій жертви кіберзлочину 31

Юридичні аспекти кібербезпеки 33

**ЧАСТИНА ІІ** 35

**ПРАКТИКУМ № 1.** Методика “ЛАНДШАФТНА МАПА ПОТЕНЦІЙНИХ КІБЕРЗАГРОЗ” 36

Блок 1. Створення ландшафтної мапи потенційних кіберзагроз 36

Блок 2. Я та кіберзагрози. Емоційна рефлексія 40

Блок 3. Кіберзагрози військового часу 42

**ПРАКТИКУМ № 2.** Дискусійний клуб 44

Варіант 1. Ризики кіберсоціалізації 44

Блок 1. Робота над аргументацією у письмовому вигляді 46

Блок 2. Дебати 48

Варіант 2. Особливості воєнної кібербезпеки 49

Блок 1. Домашня робота над проєктом 51

Блок 2. Проведення дискусійного клубу 51

**ПРАКТИКУМ 3.** Правила сімейної кібербезпеки. Методика “ТОТЕМНИЙ КІБЕРЇЖАК” 53

Блок 1. Обговорення Інтернет-загроз 54

Блок 2. Малювання тотемної тварини кібербезпеки 55

Блок 3. Формування правил сімейної кібербезпеки 56

**ПРАКТИКУМ 4.** Розвінчання фейків 58

Блок 1. Створення фейкових новин та повідомлень 58

Блок 2. Розпізнавання фейків 60

Блок 3. Що робити з фейками? 63

**ПРАКТИКУМ 5.** Кейси кіберзлочинів української судової системи 65

**ДОДАТКИ** 69

Додаток 1. Список потенційних кіберризиків 70

Додаток 2. Картки для дискусійного клубу 71

Додаток 3. Робота з фейками 75

**Список використаної літератури** 78

# ВСТУП

Розвиток технологій та активна кіберсоціалізація дітей та молоді в останні роки зробили гострою тему кіберризиків та кібербезпеки в українських реаліях.

Для сучасної дитини стало звичним бути постійно на зв'язку із своїми рідними та 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 скоротати час. Інтернет і різноманітні додатки стали такою ж невід'ємною частиною життя дітей, як одяг чи їжа. Людям вже важко уявити своє життя без смартфона.

Говорячи про всі переваги, які приносить у життя смартфон чи планшет із доступом до Інтернету, люди часто забувають, що є й інша сторона медалі, а саме – кіберризики. Це в першу чергу загрози, пов'язані з інтернет-активністю користувачів. І їх можна розглядати як з технічної, так і з психологічної точки зору.

Досить часто дорослі, так само як і діти, не приділяють достатньої уваги ризикам, які можуть чатувати на них в Інтернет-середовищі. Для того, щоб продемонструвати наскільки це актуальна тема, ми пропонуємо провести невеликий тест-драйв. Ми пропонуємо вам пройти *самоопитувальник "Місце кіберзагроз у моєму житті"*. У даний самоопитувальник входять питання, пов'язані із найрозповсюдженішими кіберзагроз. Хочемо також звернути вашу увагу, що це не повний список, а лише верхівка айсбергу злочинного кіберсвіту. Для того, щоб допомогти вам орієнтуватися у кіберзагрозах віртуального світу при відповідях на поставлені запитання, ви можете відкрити Додаток № 1 до цього практикуму. Кожен кіберризик, який там описаний має порядковий номер, це зроблено для вашої зручності. Щоб ви не втрачали час при відповіді на поставлені нижче запитання.

Отже, візьміть, будь ласка, аркуш паперу та ручку та дайте відповідь на наступні прості запитання.

1) Чи є на екрані якісь кіберризики, про які ви не знали до цього моменту? Якщо так, то запишіть їх у рядок (можна просто записати їх порядковий номер для економії часу)?

2) Чи стикалися ви особисто з будь-яким 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 більше 10?

3) Зі скількома кіберризиками із цього списку стикалися ваші друзі або члени родини та розповідали вам про це? 2-6, може 15?

4) Який пункт із цього списку можна викреслити як те, що не можна назвати кібернебезпекою. Якщо ви вважаєте, що вони є, будь ласка, запишіть його порядковий номер. І аргументуйте свою позицію. Приведіть, що найменше 7 аргументів. Якщо не зможете, то ваша пропозиція, викреслити даний кіберризик із списку буде вважатися недоцільною.

5) Яку кібернебезпеку з цього списку ви б назвали найжахливішою в цілому? Було б чудово, якби ви могли пояснити чому.

6) Чи є в цьому списку кібернебезпека, з якою боїтеся зіткнутися особисто ви, тому що не знаєте, як себе поводити? Або є така, з наслідками якої ви навряд чи зможете впоратися? Запишіть порядковий номер того кіберризика, якого ви, по суті, боїтеся.

7) Чи говорили ви коли-небудь зі своїми дітьми про кіберризики? Якщо так, то який кіберризик (з цього списку) 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 у разі кібернебезпеки? Окрім батьків, дитина має дати ще 2-3 дорослих, яким може довіряти та з якими може поговорити у випадку настання критичної ситуації.

10) Чи знає ваша дитина номер телефону кіберполіції?

Як ви бачите, ці питання досить прості, але вони заставляють задуматися і зрозуміти наскільки близько кіберризики підібралися до кожного з нас, у деяких окремих випадках можна навіть сказати, що вони стали частиною повсякденного життя… Але чи відчуваєте ви себе захищеними від них? Наскільки ви поінформовані? І на скільки ваша дитина/діти підготовлена 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 та кібербезпеки дітей в Інтернет-середовищі. Працівники лабораторії регулярно проводять моніторинг ситуацій, пов’язаних із молодіжними кіберризиками. У 2018 році (Найдьонова, 2018) та 2020 році (Найдьонова, 2021) вже було проведено два Всеукраїнські опитування. В опитуванні 2018 року взяли участь 1439 респондентів, 768 дівчат і 671 хлопчиків, віком від 13 до 16 років. А опитування 2020 року нараховувало 1681 респондентів, 918 дівчат і 763 хлопчиків, віком від 12 до 17 років.

Дітям було запропоновано відповісти на ряд питань, пов’язаних із їх досвідом взаємодії з кіберризиками і пропонувалися 3 варіанти відповідей: «так», «ні», «мені важко відповісти». В опитуванні використовувалася найпримітивніша шкала відповідей, щоб полегшити процедуру та розуміння дітьми питань.

*Таблиця 1. Кіберризики 2018*

| *«З якими небезпеками під час використання Інтернету Вам доводилося стикатися особисто?» (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 цих досліджень, у 2018 році українські школярі найчастіше стикаються з такими кіберризиками як СПАМ або контекстна реклама, коли користувачам нав'язують непотрібну інформацію (майже 60%), найменше (майже 6%) діти стикаються з такими кіберризиками, як підбурювання до самоушкодження (див. Таблицю 1. Кіберризики).

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 непотрібних товарів і послуг, які можуть бути зовсім не потрібні споживачу і які, інколи, можуть зовсім не відповідати віку, тих, хто отримує цю інформацію. Наприклад, це може бути інформація сексуального чи релігійного характеру, можуть бути листи, основна ціль яких когось "очернити" чи "побулити". По-третє, через нав'язливу інформацію діти можуть потрапляти на гачки кіберзлочинців. Наприклад, це може бути інформація про те, що користувач може одержати якимось чином велику суму грошей, яка перейде за посиланням. В-четвертих, досить часто такі повідомлення супроводжуються шкідливими програмами, вірусами. Власне, кіберризик пов'язаний із втручання у роботу обчислювальних пристроїв та зараження техніки різними віруси – майже так само добре знайомий дітям, як і нав'язлива інформація.

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

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

Окремо хочемо виділити такий Інтернет-ризик як кібербулінг, оскільки досить часто українські медіаосвітяни піднімають дану тему на щорічних стратегічних нарадах. У 2019 року в Кодексі про адміністративні правопорушення з'явилася нова стаття 173-4 "Булінг (цькування), що обумовлено збільшенням числа подібних випадків в українських школах. При умовній екстраполяції отриманих у 2018 році даних на всю генеральну сукупність, ми отримуємо орієнтовну кількість підлітків, які знаходяться під впливом надзвичайно небезпечних і деструктивних видів кібербулінгу. Так, щодо переслідування, якого зазнають 7,1%, до групи ризику входить більше 77 тисяч підлітків, 6,1% школярів, яких кіберпростір спонукає до насильства – це більше 66 тисяч, а 5,8% учнів, яких підштовхують через інтернет до самоушкоджень, загалом по всій Україні кількісно складає більше 63 тисяч осіб групи ризику (Найдьонова, Дятел, Вознесенська та ін., 2018). Наразі в Україні за таке правопорушення 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 (Стаття 173-4. Булінг (цькування), 2018).

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

Булінг може приймати різні види та форми і носити психологічний, фізичний або економічний характер. Кожен учасник булінгової ситуації потребує кваліфікованої психологічної допомоги – не тільки жертва, але й агресор та спостерігачі (яким ця ситуація також може завдати глибинної психотравми).

Третю групу Інтернет-ризиків *маніпуляційного впливу* складають три найбільш небезпечні форми: *спілкування з незнайомими людьми* з небажаними наслідками, (наприклад, прохання надіслати фото інтимного характеру або небезпечні зустрічі з незнайомцями в реальності) (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 існуючих загроз.

При цьому 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 з жодними небезпеками під час користування Інтернетом.

В опитуванні 2020 року ми можемо спостерігати трішки іншу картину.

Частота зіткнень з деякими кіберризиками, які отримали низькі оцінки у 2018 році, зросла майже вдвічі, а найпоширеніші кіберризики у 2018 році трохи "втратили" свої позиції (див. Табл. 2).

*Таблиця 2. Кіберризики 2020*

| *«З якими небезпеками під час використання Інтернету Вам доводилося стикатися особисто?» (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 обох років, керівник Всеукраїнського експерименту з упровадження медіаосвіти в загальноосвітні навчальні заклади України Найдьонова Любов Антонівна звернула увагу, що Спонукання до насильства, агресії, підбурювання нетерпимого ставлення до інших зросло в два рази, складає 11 %. Підштовхування до самоушкодження (суїцидальні ігри та челенджі) наразі складає 8,9 % (Найдьонова, 2021, 8 квітня). У зв'язку з чим група вчених в Інститут соціальної та політичної психології у 2021 році розробляла окремих проект превенція і поственція суїцидальної поведінки (Чуніхіна, Умеренкова, 2022)

Але найбільше занепокоєння, на нашу думку, викликає зростання кількості епізодів, пов'язаних з кібербулінгом із 14 % до 23 %. Це дуже небезпечна тенденція, на яку обов'язково потрібно звернути увагу в роботі, насамперед - з батьками (Найдьонова, 2019).

Як же мають діяти батьки у ситуації , коли їх дитина стала жертвою шкільного булінгу?

1. Перш за все, поставтеся з розумінням і співпереживанням до ситуації. Не потрібно давати на дитину, кричати або сварити за зниклі речі. Спробуйте завести з дитиною відверту розмову і наполягати на тому, що ви завжди на боці свої дитини, що ви її опора, допомога і захист у складних ситуаціях.
2. Уважно вислухайте, не перебивайте, не задавайте багато уточнюючих питань. Не намагайтеся одразу стати "караючим оком", оскільки одним із багатьох страхів дитини, пов'язаних із ситуацію булінгу, є те, що у школу прийде мама/тато і влаштують там скандал і після цього дитину будуть ще гнобити за це. Тому спочатку запитайте у дитини, якої лінії поведінки вона притримується із кривдниками, чому нею була обрана саме така стратегія, які у цієї стратегії сильні і слабкі сторони.
3. В процесі обговорення дитячої поведінки постарайтеся максимально детально дізнатися про всі інциденти булінгу, які зазнавала дитина. Запитайте чи існують матеріальні докази – переписки, пости у соціальних мережах, відео тощо. Спробуйте отримати доступ до цих доказів.
4. Далі можуть бути два шляхи вирішення ситуації. Перший, ви зі своєю дитиною разом, в обговоренні придумуєте як вона може поводитися, щоб "перемогти" своїх кривдників. Розробляєте стратегію, навчаєте дитину різним психологічним прийомам і методам антибулінгу (Чаплінська, 2020). Спробуйте підтримати свою дитину на шляху до подолання цієї небезпеки, навчаючи справлятися самостійно, але мають за спиною підтримку батьків. Такий шлях доцільно використовувати, якщо булінг має здебільшого психологічних характер. У разі фізичного чи економічного булінгу, варто піти другим шляхом і залучити адміністрацію школи до вирішення

проблеми.  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. Подібного роду конфлікти мають вирішуватися або на рівні “дитина-дитина”, або на рівні “дорослі-дорослі”, і точно не на рівні “дорослі-діти”.

Варто зазначити, що так само як і в 2018 році, існує група дітей, які вважають, що Інтернет для них є абсолютно безпечним місцем – 7,75% дітей, а 6,08% запевняють, що вони особисто не стикалися з жодними небезпеками під час користування Інтернетом. Це група опитуваних особливо вразлива, оскільки ще не мала досвіду взаємодії із кіберзагрозам, що чатують на них в Інтернеті, саме тому критичність їх мислення щодо такого роду небезпек може бути знижена.

Також у дослідженні 2020 році дітям були поставленні додаткові запитання щодо окремих видів кіберзагроз (див. табл. 3) для того, щоб сформувати більш чітку картину.

*Таблиця 3. Додаткові питання для виявлення дитячих кіберризиків*

| *Уточнюючі запитання* | *%* |
|---|---|
| Ви стали мішенню для ТРОЛІНГУ в соціальних мережах (для розваги інших людей) | 33.1 |
| Чи стали ми жертвою ШОКТРОЛУ – маси образливих постів з метою викликати ваш гнів, розчарування чи приниження | 22.7 |
| Ви сварилися в соцмережах (ФЛЕЙМІНГ), коли в запалі суперечки ви говорили те, що не сказали б у 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, що ви не хотіли робити через онлайн-погрози та шантаж? | 55.4 |
| Чи були ви коли-небудь у ситуації 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 неіснуючих людей)? | 37.0 |
| Чи були ви в ситуації СЛЕММІНГУ – підбурювання спостерігачів до кібербулінгу, де спостерігачі не були ініціаторами бійки? | 23.9 |
| 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, яких ви зустрічали | 31.1 |

| | |
|---|---|
| лише в Інтернеті? | |
| Чи стикалися ви з SEXTING – текстовими повідомленнями чи коментарями на вашу адресу, які мали сексуальний характер? | 50.2 |
| Чи зустрічали ви в Інтернеті небажані зображення, які супроводжують сексуальну поведінку? | 50.4 |
| Ви стикалися з кібергрумінгом (CYBERGrooming) – коли незнайомі люди в мережі намагалися залучити вас і запросили на зустріч офлайн? | 39.4 |

Як ми бачимо, рівень зіткнень дітей з різними видами кібернебезпек насправді дуже високий. Хоча молодь може 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 у лютому 2022 року, повноцінні моніторинги та опитування щодо кіберзагроз дітей в Інтернеті не проводилися, хоча ми можемо спрогнозувати, що загальна картина і окремі тенденції зміняться. Українські школярі в умовах воєнного часу можуть зіткнутися із значною кількістю фейкової інформації, вірусними кібреатаками, злами персональних акаунтів та крадіжка 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 та пошкодженням комп'ютерних даних або електронні листи з назвою «Військові злочинці РФ.htm», відкриття яких призводило до того, що зловмисники отримували віддалений доступ до комп'ютера жертви), реттінг (за якого діти впевнені, що ведуть переписку із 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.

Подібно до того, як дорослі застерігають дітей від загрози 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 цим контроль. І вона вже ніяк не вплине на те, чи буде таке фото показано 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, осміянням, булінгом і покаранням може штовхати дитину на крайні міри у бажанні уникнути цього – на суїцид.

Саме тому ми вважаємо необхідним ввести до шкільної програми такий предмет як кібербезпека. Підготувати дітей до зустрічі з кіберризиками в дорослому віці. Під час таких занять, дитина має отримати не тільки загальні знання про можливі Інтернет загрози, вона також має розуміти особливості схем та прийомів кіберзлочинців, виробити особисті правила безпеки і неуклінно їх дотримуватися, сформувати психологічні стійкість і бути готовою справлятися зі наслідками кіберзагроз.

В цих рамках, ми можемо визначити *кібербезпеку* як набір знань користувача Інтернет-мережі для захисту власних життєво важливих інтересів при використанні кіберпростору, а також вміння нівелювати наслідки кіберзагроз.

Варто зазначити, що технічні аспекти кібербезпеки часто розглядаються в науковій літературі. Але підходів, які б описували психологічну складову, бракує. Оскільки дитину необхідно навчати не тільки технічні особливостям кібербезпеки, але й правильно пояснювати ризики. Наприклад, дорослий говорить дитині: «В Інтернеті не можна переходити за сумнівними посиланнями, тому що онлайн-ігри та програми можуть містити «віруси» або фішинг, тому для завантаження потрібних файлів потрібно 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.

Кібербезпеку потрібно пояснювати дітям на конкретних прикладах. Необхідно скласти з дітьми плани дій на випадок, якщо вони зіткнуться з кібернебезпекою (чітко пояснити послідовність їх дій у ситуаціях зустрічі з кіберзагрозами в Інтернеті). Дітям потрібно розповісти, до кого вони можуть звернутися за допомогою. Іноді буває, що діти не хочуть або соромляться звертатися за допомогою до батьків, тому це може бути будь-який дорослий, якому дитина довіряє (брат, сестра, дідусь, бабуся, тітка, дядько, шкільний вчитель, психолог тощо). Також дітям потрібно розповісти про кіберполіцію та закони, пов'язані з кіберзлочинами та покаранням за них.

Даний практичний посібник направлений на підготовку вчителів для роботи за темою кібербезпеки як у мирний, так і воєнний час. Використання матеріалів даного посібник для підготовки занять для дітей із означеної теми дозволить:

●формувати у дітей загального уявлення про кіберризик і кібернебезпеки як мирного, так і воєнного життя

●зрозуміти різницю між кіберризиком, кіберзлочином, кібертероризмом та кібервійною;

●дізнатися особливості юридичної системи України в контексті кібербезпеки;

●надасть можливість психологічної підготовки дітей до протистояння кіберризикам.

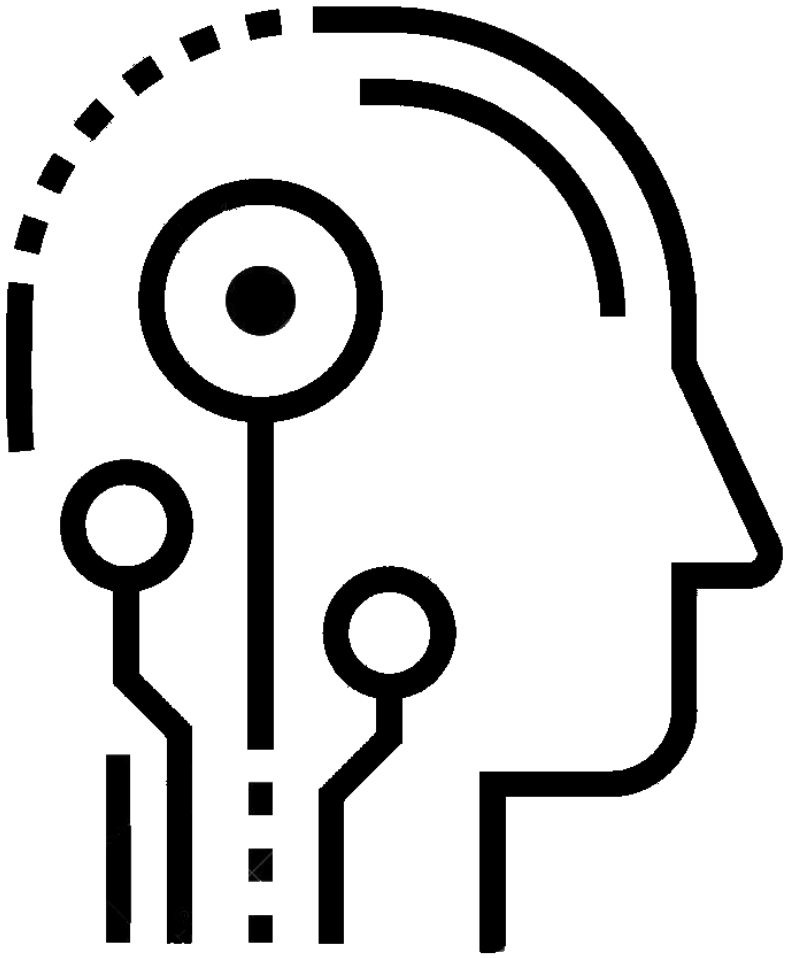
Посібник складається із вступу, теоретичної частини та п'яти психологічних практикумів, додатків, списку використаної літератури.

В теоретичній частині представлено два підрозділи. В першому розкривається понятійний апарат кіберзагроз і детально розглядаються такі поняття як поняття кіберризики, їх види та наслідки; кібератаки та кіберінцеденти; кіберзлочини та їх відмінність від звичайних злочинів; кібертероризм, його видові особливості та проявів, а також кібервійна та її відмінностей від інформаційної війни. Другий підрозділ акцентує увагу на кібербезпеці в цілому (індивідуальний, організаційний/груповий та державний рівні) та її юридичних аспектах в принципі. Представлено поняття воєнної кібербезпеки та її ключових моментах (безпека мобільних пристроїв, двоетапна аутентифікація, програмне забезпечення, безпека соціальних мереж, неправдиві повідомлення або фейки, ненадійні сайти та посилання), а також розписано важливість сімейних правил кібербезпеки. Окремо зосереджено увагу на діяльності кіберполіції в Україні, як і воєнний, так і у мирний час. Надається опис нормативних документи які регулюють кібербезпеку, як в Україні. Також у другому підрозділі розписано алгоритм дій у випадку, якщо ви стали жертвою кіберзлочинця з використанням психологічних технік та авторську техніку "Наслідки кіберзлочину і Я".

Друга частина Психологічного практикуму складається із п'яти практичних занять, направлених на закріплення матеріалу, представленого у теоретичній частині. Перший практикум, основується 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 військовий час). Другий практикум представляється у форматі дискусійного клубу або дебатів і має на меті допомогти учням розвинути навички логічної та послідовної аргументації у публічних виступах, вміння слухати та відстоювати власну позиції у взаємодії з іншими людьми, а також поглибити знання у психологічних особливостях кіберсоціалізації особистості або у особливостях воєнної кібербезпеки (на вибір). Третій практикум ґрунтується на авторській методиці “Тотемний кіберїжак” і покликаний допомогти у формуванні сімейних правил кібербезпеки та алгоритмів дії для всіх членів сім’ї (або трудового колективу) у небезпечних ситуаціях. Темою четвертого практикуму є розвінчання фейків (що є особливо актуальною у воєнний час). Основна його мета ознайомлення дітей із схемою створення фейкових повідомлень та новин під час війни та навчити їх розпізнавати дезінформацію за ключовими показниками. П’ятий практикум, а саме судові кейси, правлений на ознайомлення дітей з юридичним компонентом кібербезпеки. Завдяки даному практикуму діти навчаться співвідносити статті українських законів із реально вчиненими кіберзлочинами та зрозуміють, які наслідки та варіанти покарання за різні види правопорушень можуть очікувати кібезлочинців.

# ЧАСТИНА І



## 1.2. ВІД КІБЕРРИЗИКУ ДО КІБЕРВІЙНИ

### *КІБЕРРИЗИК*

**Що таке кіберризики?**

Кіберризик – можна розглядати в першу чергу як загрозу, пов'язану з інтернет-активністю користувачів, як з технологічними, так і психологічними її сторонами, а також зберіганням персональних даних. З точки зору інформаційної безпеки кіберризик – це втрати, що може понесе користувач Інтернет-мережі через порушення конфіденційності, цілісності або доступності інформаційних ресурсів чи персональних даних. У подальшому поняття кіберризику та кіберзагрози ми будемо використовуватися як синонімічні.

Одним із інструментів реалізації кіберризику є *кібератака*. Під даним поняттям потрібно розглядати дії кіберзловмисників (хакерів) або шкідливих програм, які спрямовані 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 *кіберінцеденти*. Під даним терміном потрібно розглядати подію або ряд несприятливих подій навмисного характеру, що мають ознаки кібератаки, та становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів (Про основні засади забезпечення кібербезпеки України, 2017).

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

**Які існують види кіберризиків?**

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

*Нецільові атаки* – коли кіберзлочинці працюють в рамках розробленої злочинної схеми, використовуючи підготовлені скрипти, які використовують у взаємодії із всім жертвами. Передбачає не персоналізований підхід (фішинг, кардінг, смсшахрайство)

*Атаки внутрішні* – коли кіберзлочинці 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).

*Атаки зовнішні* – коли кіберзлочинці готуються до скоєння кіберзлочину, збирають інформацію, але є не частиною організації, на яку влаштовують кібератаку і не мають підтримки її співробітників.

**Якими можуть бути наслідки?**

*фінансові втрати* (наприклад, в результаті фішінгової атаки, коли зловмисники отримали доступи і паролі до вашої банківської картки);

*часові витрати* (наприклад, якщо через вірусне блокування комп'ютера ви не зможете зробити необхідну роботу);

*репутаційні втрати* (наприклад, через викрадення та розповсюдження 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 на даному етапі розвитку нашого світу будь-який політичний або військовий конфлікт завжди супроводжується організованим противоборством в мережі Інтернет. Наприклад, у 2005 році в Японії пройшла хвиля кібератак, каталізатором якої був випуск шкільного підручника з історії. В даному підручнику спотворювалися історичні події, що відбувалися в Китаї в 1930-1940 роках XX ст., зокрема в ньому замовчувалися військові злочини японських військ під час інтервенції. У списку сайтів, що піддавалася хакерським атакам, були Японські Міністерства та Відомості, сайти найбільших японських корпорацій та сайті, що були присвячені Другій Світовій війні. При цьому китайські хакери продемонструвати високий рівень організованості та синхронності при масовій атаці. З огляду на наявність державного контролю в Китаї за мережею Інтернет, можна припустити, що дана атака була санкціонована державою (Дзюндзюк, Дзюндзюк, 2013).

## *КІБЕРЗЛОЧИН*

Розповсюдження нових інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та засобів комунікацій, сформувало єдиний світовий інформаційний простір, де кожен може отримати доступ до будь-якої інформації з різних точок планети, дистанційно керувати бізнесом, здійснювати управління власними активами, укладати угоди без необхідності особистого контакту тощо.

Разом з цим, інформаційний простір став місцем та в той же час й безпосередньо інструментом злочину. Відтепер злочинцю не потребує попередньої «обробляти клієнта» та 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 отримується 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 з метою створення збитків компаніям, DDoS атаки на Інтернет-ресурси – це далеко не повний перелік подібних загроз, які несе з собою бурхливий розвиток сучасних інформаційних технологій, та, 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 у 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 та 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) була прийнято *Конвенції Ради Європи про злочинність у кіберпросторі* (далі – *Будапештська конвенція*). Дана конвенція є фундаментом для розробки законодавства у боротьбі з кіберзлочинами як для кожної країни окремо, так і для загальносвітового законодавства. Вона також класифікує кіберзлочини. Оскільки існує багато різних різновидів, їх для зручності можна поділити на групи.

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

У *другу групу* входять злочини, пов`язані з використанням комп`ютера як засобу скоєння злочинів, а саме як засобу маніпуляцій з інформацією. У цю групу входять комп`ютерне шахрайство та комп`ютерне підроблення.

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

У *четверту групу* увійшли злочини, пов`язані з порушенням авторського права і суміжних прав.

*П`ята група* злочинів зафіксована в окремому протоколі, зокрема це акти расизму та ксенофобії, вчинені за допомогою комп`ютерних мереж.

Ще одна категорія злочинів, не включена окремо до Конвенції Ради Європи (і набула поширення вже після ухвалення Конвенції) – identity theft, крадіжка, передача та використання персональних даних з метою скоєння злочинів (Номоконов, Тропина, 2013).

За об`єктом посягання виділяються наступні 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 існує велика кількість кіберзлочинів, що зазіхають на декілька об’єктів.

**Чим кіберзлочин відрізняється від звичайного?**

По-перше, здійснення кіберзлочину вимагає від злочинців наявності спеціальних технічних знань. Крім того хакерська субкультура, в якій зростає більшість кіберзлочинців, стимулює інтелектуальний розвиток. Але на відміну від інших інтелектуальних кримінальних правопорушень, кіберзлочини доступні людям невисоких соціальних та вікових можливостей, досить мати доступ в Інтернет та комп’ютер.

По-друге, більшість кіберзлочинів анонімні і неперсоніфіковані – механізми ідентифікації глобальної мережі дозволяють злочинцю 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 та суб'єкта злочину в момент вчинення такого.

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

У зв'язку з анонімність, широтою покриття та латентністю, шансів бути виявленим у кіберзлочинця набагато менше, ніж у грабіжника банку. І навіть при затриманні в нього менше шансів бути притягнутим до кримінальної відповідальності, оскільки законодавство щодо кіберзлочинців все ще є недосконалим.

## *КІБЕРТЕРОРИЗМ*

**Що таке кібертероризм?**

Під *кібертероризмом* (комп'ютерним тероризмом) слід розуміти 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 були скоєні з метою порушення суспільної безпеки, залякування населення, провокації військового конфлікту (Пилипчук, Дзьобань, 2011).

Цілі здійснення кібертероризму збігаються з цілями і мотивами здійснення всіх відомих видів терористичних дій, а саме: порушення суспільної і державної безпеки; залякування населення; провокація військового конфлікту; ускладнення міжнародних відносин; вплив на прийняття 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 воєнними мережами й медичними закладами, банківські та інші фінансові мережі, засоби передачі даних за допомогою комп'ютерних мереж. Він може здійснюватися з метою саботажу (урядових установ), заподіяння економічного збитку (великим виробничим корпораціям), дезорганізації праці з потенційною можливістю смертей. Інформаційна атака на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури, що здійснюється терористичними угрупованнями або окремими особами є основною кібертероризму. Така атака дозволяє проникати у систему, перехоплювати управління або пригнічувати засоби інформаційного обміну в мережі, чинити інші деструктивні впливи (Бутузов, Тітуніна, 2007).

**Яких форм може набувати кібертероризм?**

Дослідник з проблем тероризму В.П. Журавльова вважає, що кібертероризм проявляється у двох формах: по-перше, комп'ютерні економічні злочини, які вчиняються за допомогою спеціалістів хакерів, серед яких:

- 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 вірусами, що порушують функціонування державних органів та інших установ);

●незаконне користування комп'ютерними послугами (програмами, покупки за рахунок інших тощо);

по-друге, розголошення таємниці – отримання комерційної та конфіденційної інформації (що нерозривно пов'язане з першим видом), серед чого:

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

●незаконний збір та переховування інформації;

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

**Чим кібертероризм відрізняється від звичайного тероризму?**

Тактика і прийоми, що використовуються при вчиненні цього злочину, відрізняються від тактики і прийомів вчинення класичних комп'ютерних злочинів тим, що комп'ютерний терористичний акт повинен мати небезпечні наслідки, стати широко відомим населенню й одержати великий суспільний резонанс. Від комп'ютерних злочинів кібертероризм відрізняється насамперед своїми цілями, що властиві тероризму в цілому: дії завжди мають публічний характер і спрямовані на вплив, що здійснюється відносно окремих осіб, суспільства чи влади. Від традиційного тероризму (політики залякуванням, пригнічення супротивників здійсненням актів насильства) він відрізняється засобами здійснення, а також своєю анонімністю та знеособленістю.

Збитки від терористичної операції суттєво збільшуються при підключенні засобів масової інформації (варіант, що вже практикується в глобальному інформаційному суспільстві). Роль ЗМІ у такому випадку може виконувати телебачення та Інтернет. У результаті рівень впливу терористичної операції суттєво зростає. Таким чином, у терористів з'являється потенційна можливість впливати на зміст інформації про теракт, використовуючи контрольовані джерела інформації, підключені до ЗМІ. Їх роль можуть виконувати розроблені в мережі Інтернет сайти (з метою легалізації інформації офіційні ЗМІ посилаються на такі сайти). Завдяки цьому негативні наслідки від терористичної операції у відношенні системи, на яку здійснюється атака, значно зростають (Бутузов, Тітуніна, 2007).

## *КІБЕРВІЙНА*

**Що таке кібервійна?**

Річард А. Кларк, в книзі «Кібервійна» (англ. *CyberWarfare*) визначив дане поняття як "дії однієї національної держави з проникнення в комп'ютери або мережі іншої національної держави для досягнення цілей нанесення збитку або руйнування" (Clarke, Knake, 2011).

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

●високий рівень анонімності;

●невизначеність часу початку;

●певна відсутність слідів;

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

●відсутність будь-століття почалось з революційних змін, які якого правового міжнародного регулювання.

Зараз глобальна мережа Інтернет має загальне управління з боку ICANN (Internet Corporation for Assigned Names and Numbers). Регулювання відбувається за парадигмою “один світ – один Інтернет”. При такому підході неможливими стають будь-століття почалось з революційних змін, які звичні у військовому праві міжнародні угоди. ICANN заперечує право держав регулювати і нести відповідальність за певний сегмент Інтернет. Де факто Інтернет та інші мережі мають наднаціональний характер, а бойові дії в кіберпросторі направлено на певні національні держави та їх структури. Наявна ситуація, коли ніякі юридичні і будь-століття почалось з революційних змін, які погоджувальні механізми профілактики та запобігання кібервійнам не можуть діяти. Характерні риси кібервоєн вказують, що вони є особливо небезпечними, тому що легко розв’язуються і практично не регулюються (Горбенко, 2021 а).

Кібервійни напряму пов’язані із кібершпіонажем, кіберзлочинністю та кібертероризмом.

Існує також поняття інформаційної війни, що не є тотожним до кібервійни.

**Що таке інформаційна війна?**

*Інформаційна війна* – це міждержавне протиборство в інформаційному просторі з метою нанесення збитку інформаційним системам, підриву політичної та соціальної системи, а також масованої психологічної обробки населення для дестабілізації суспільства та держави. Для інформаційної війни на першому місці знаходяться: психологічний вплив, дезінформація, PR-століття почалось з революційних змін, які компанії та спеціальні інформаційні операції (Горбенко, 2021 а).

Більш чіткий поділ між інформаційними війнам та кібервійнами почався приблизно 15 років тому з революційних змін в кібертехнологіях.

**У чому різниця між інформаційною та кібервійною?**

Інформаційні та кібервійни відрізняються за об’єктами та засобами дії. Інформаційні війни є контентними війнами, що мають за мету зміну масової, групової та індивідуальної свідомості, нав’язування власної волі противнику та перепрограмування його поведінки. Під час інформаційної війни іде боротьба за свідомість, цінності, переконання, шаблони поведінки тощо. Виникли тисячоліття тому, а Інтернет дав їм новий рівень інтенсивності, масштабності та ефективності.

Об’єктами впливу інформаційних війн є різноманітні суб’єкти – від невеликих груп до певних народів та націй, населення держав.

Засобом впливу є спеціальні підготовлені семантичні повідомлення у вигляді текстів, відео та аудіо матеріалів.

Кібервійни є цілеспрямованим деструктивним впливом інформаційних потоків у вигляді програмних кодів на матеріальні об’єкти та їх системи, їх руйнування, порушення функціонування або перехоплення керування ними.

Об’єктами впливу кібервійни є виробничі структури, інфраструктури соціального, воєнного та фінансового призначення, роботизовані та високоавтоматизовані виробничі та технологічні лінії.

Основним типом засобів бойового впливу у кібервійнах є певний програмний код, який порушує роботу, виводить з робочого стану, або забезпечує перехоплення керування різного роду матеріальними об’єктами та мережами, що мають у оснастці електронні системи керування.

Інформаційні війни та кібервійни є двома різновидами війн, які у більшій своїй частині ведуться через комп'ютерні мережі – глобальну мережу Інтернет, закриті державні, військові, корпоративні та приватні мережі. Для кожного із цих двох типів війн наявні власні інструментарії, методи, стратегії та тактики ведення, закономірності ескалації, можливості попередження, тощо (Горбенко, 2021 b; Ranger, 2017).

## 1.2. КІБЕРБЕЗПЕКА ТА КІБЕРКУЛЬТУРА

Один із ключових аспектів життя людини в інформаційну добу є кібербезпека. Оскільки смартфони, соціальні мережі й інші онлайн-сервіси містять в собі "інформаційні відбитки" користувачів і, відповідно, багато особистої інформації. Інколи навіть більше, ніж люди гадають. При цьому, облікові записи на онлайн серверах можуть бути значно вразливішими для атак зловмисників, ніж людина в реальному житті. Тому уся електронна інформація, сервіси і пристрої потребують захисту і дотримання певних правил безпеки (Баранова, 2014).

*Кібербезпеку* в загальному сенсі можна визначити як захищеність життєво важливих інтересів людини й громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз державній безпеці в кіберпросторі (Закон України "Про основні засади забезпечення кібербезпеки України" (Газізова, 2022).

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

### *ІНДИВІДУАЛЬНА БЕЗПЕКА*

Для забезпечення індивідуальну безпеки у 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. У зв'язку з чим, ми радимо обговорити з дітьми правила загальної безпеки та виробити щонайменше 5 голодних, які мають діяти в будь-яких ситуаціях, незважаючи на обставини.

Дорослі мають пам'ятати, що про кібербезпеку потрібно почати говорити з дитиною з того віку, коли вона має доступ до гаджетів. У когось дитина вже у 2 роки активно користується планшетом чи батьківським смартфоном, а для когось дорога в світ безмежного інтернету розпочинається у 7 років, коли дитина йде до школи і батьки бажаючи бути з нею на зв'язку, дарують гаджет.

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

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

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

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

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

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

Для більш дорослих дітей, правила можуть бути дещо розширеними і у більш схематичному вигляді. Наприклад:

●Не повідомляй нікому (особливо незнайомцям в Інтернеті) особисту інформацію: домашню адресу, номер домашнього телефону, робочу адресу батьків, їхній номер телефону, назву та адресу школи. Також подібну інформацію краще постити в соціальних мережах, оскільки нею можуть використати кіберзлочинці. за потреби ти можеш запитати у батьків дозвіл на розголошення подібної інформації.

●Якщо в Інтернеті ти зіткнетеся із будь-якою інформацію, яка тебе збентежить чи/або викличе внутрішнє занепокоєння, підозру – поговори про це з дорослими, яким довіряєш.

●Ніколи не погоджуйтеся на зустріч з кимось, з ким ти познайомився (лась) в Інтернеті без додаткового страхування у вигляді дорослого поряд. Краще на подібні зустрічі спочатку запитати дозвіл у батьків. Перша зустріч з інтернет-другом має відбутися в людному місці, в денний час та в присутності когось із знайомих дорослих . Не обов'язково, щоб дорослі тримав тебе за руку, просто щоб був десь поруч і міг переконатися, що в тебе все добре і на зустріч дійсно 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 дане правило стосується інтимних (або напівоголених, наприклад, у купальнику) фотографій. Також ніколи, за жодних обставин, вмовлянь чи тиску з боку іншої людини не оголяйте свого тіла або її частину на веб-камеру.

●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 "0". Якщо ти отримуєте СПАМ-листи чи листи з погрозами, то обов'язково зверніться до дорослих, разом ви можете звернутися до компанії, яка надає послуги Інтернету, щоб заблокувати отримання подібних листів або до кіберполіції, для юридичного врегулювання даної проблеми.

●Не довіряй свої паролі нікому, навіть найближчим друзям. Пам'ятай, що електронні пристрої зберігають значну кількість персональної інформації. Ця інформація має бути захищеною. Використовуйте складні паролі для захисту телефону, планшету чи ноутбуків. І можеш прямо прости інших людей відвернутися, коли вводиш пароль. Відстоюй своє право на конфіденційність.

●Не роби незаконних дій в Інтернеті, оскільки навіть для неповнолітніх злочинців, існують різні варіанти покарань.

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

Подібні сімейні правила виховують в дитині кіберкультуру, привчають як саме можна себе поводити в мережі Інтернет, а чого робити не варто. Так само як в сімейному колі потрібно приділяти час питанням культури та правилам, так само дані аспекти життя мають підкріплюватися і в закладах освіти.

## *ГРУПОВА/ОРГАНІЗАЦІЙНА БЕЗПЕКА*

(Кібербезпека в закладах освіти)

Організаційна безпека або безпека у трудових чи у нашому освітніх колективах, важлива і складна річ, оскільки вона має централізовано створити та впровадити загальні для всіх учасників процесу правила кібербезпеки. А також слідкувати за їх виконанням та певним чином розбиратися із наслідками їх недотримання.

У складні для України часи вважаємо за вкрай необхідним приділяти особливу увагу заходам кібербезпеки у навчальних закладах. Учасники освітнього процесу мають бути попереджені про небезпеки з якими можуть зіткнутися в мережі Інтернет не тільки про ті, що бути розповсюджені у мирний час, але й про такі, що виникли з військовою агресію з боку Російської Федерації. Ми можемо говорити про те, що воєнні кіберзагрози трансформувати форми, наприклад, кібершахрайства, і змінили свою інтенсивність.

Валерій Биков з колегами визначили певні правила для захисту суб’єктів навчання. Так, науковці наполягають, що в навчальному закладі повинні бути інструкції про те, як і на які теми можна спілкуватися із сторонніми особами стосовно персональних особливостей, яку інформацію можна надавати для служби технічної підтримки, як і яку інформацію може повідомити учасник навчального процесу стороннім особам і працівникам мас-медіа.

1. *Призначені для користувача облікові дані є власністю навчального закладу.* Всім співробітникам в день прийому на роботу має бути роз'яснено те, що ті логіни і паролі, які їм видали (якщо це має місце), не можна використовувати в інших цілях (на webсайтах, для особистої пошти тощо), передавати третім особам або іншим співробітникам, які не мають на це права.
2. *Необхідно проводити вступні та регулярні навчання* співробітників і учнів, *спрямовані на підвищення знань з інформаційної безпеки*.
3. *Обов'язковою є наявність регламентів з безпеки, а також інструкцій,* до яких користувач повинен завжди мати доступ. В інструкціях повинні бути описані дії учасників освітнього процесу при виникненні тієї чи іншої ситуації.
4. На комп'ютерах користувачів *завжди має бути актуальне антивірусне програмне забезпечення*.
5. У корпоративної мережі навчального закладу або об'єднання закладів *необхідно використовувати системи виявлення та запобігання атак*. Необхідно також використовувати системи запобігання витоку конфіденційної інформації. Усе це дозволить знизити ризик виникнення фішингових атак.
6. *Необхідно бути пильним щодо джерела, яке 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).

За останні кілька років в Україні тема безпеки дітей в Інтернеті набула неабиякої популярності, що в свою чергу створює попит на якісні ресурси для навчання і отримання додаткових знань з теми кібербезпеки. Наприклад, Онлайн-курс “Основи кібербезпеки для школярів”, створений CRDF Global в Україні у співпраці з ГО “Смарт Освіта” та Technomatix; сайт “Онляндія: моя безпечна веб-країна” 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. Незважаючи на наявність матеріалів у відкритому доступі, на нашу думку, навчальні заклади приділяють все ще мало уваги тематиці кіберзагроз та кібербезпеки. Існує потреба у не просто гуртках чи факультативних заняттях, а якісній навчальній програми для середньої та старшої школи з теми “Кібербезпеки”.

## *ДЕРЖАВНА БЕЗПЕКА*

Людство нині живе в епоху інформаційного суспільства, коли інформаційні технології та телекомунікаційні системи охоплюють усі сфери життєдіяльності людини, держави. Але таке повсюдне проростання телекомунікації і глобальної комп’ютеризації у людське життя може привести к серйозним наслідками. Зараз жертвами хакерів та кіберзлочинців можуть стати не лише люди, але й цілі держави.

У 2014 році Російська Федерація розв’язала проти України *гібридну війну*, яка передбачає, що країна-агресор може залишатися публічно непричетною до такого конфлікту та 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 водночас простої, але широкомасштабної розвідувальної кібероперації, спрямованої на приватний сектор, є BugDrop. Вона була зосереджена на отриманні 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, в яких закликали відкрити файл Microsoft Word, що містив шкідливий макрос. Так, одним натиском клавіші людина може поставити під небезпеку не лише свої дані, але й дані, які, в разі втрати, несуть велику небезпеку для держави в цілому (Міністерство оборони України, 2018).

А у лютому 2022 року Російська Федерація нанесла відкритого удару по території України, що в свою чергу перевело збройний конфлікти у нову фазу. Але при цьому методи злочинних кіберопреацій трансформувалися і набули неймовірних масштабів. Перш за все, це стосується розсилки за електронними адресами і через соціальні мережі інформації пропагандистського характеру, фейкових новин для просування вигідної точки зору та дезорієнтації населення. Також це може бути хакерський злом приватних сторінок або серверів баз даних для збору цінної інформації та її заміни на інформацію, корисну супротивнику стороні. У цьому випадку дезінформація та викрадення даних, наприклад, відомостей щодо об’єктів критичної інфраструктури чи пересування українських військових у районах ведення бойових дій, неминуче

призведе до людських втрат. Кібератаки на об'єкти критичної інфраструктури — атаки на комп'ютери та системи, що забезпечують життєдіяльність міст, а саме: системи водопостачання, електроенергії, транспорту тощо. Коли такі кібератаки були відбиті українськими спеціалістами з кібербезпеки, супротивних почав цілеспрямоване бомбардування. Також це можуть бути цілеспрямовані атаки на бази даних чи сервери або втручання в роботу обладнання, що забезпечує, наприклад, роботу комунікаційних військових систем. У також 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 користуватися будь-якою можливістю для отримання інформації та нанесення шкоди. Тому *воєнну кібербезпеку* можна звести до відповідального ставлення кожного громадянина країни і зберіганні у таємниці від ворогів, тобто нерозповсюджені у соціальних мережах, форумах, чатах, спеціальних додатках і каналах, інформації пов'язаної з військовими об'єктами, об'єктами критичної інфраструктури, пересуванням і дислокацією військ, персональними даними солдат та їх сімей, пильне зберігання особистої інформації, якщо вона може становити загрозу національній безпеці, а також миттєвому реагуванні та повідомленні у відповідні державні органи про підозрілі активності, особистості, підготовку диверсій та спроб хакерських атак.

Зосередити увагу на кількох ключових моментах військової 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 всього, ще й новинний портал, зв'язок із близькими. І він потребує захисту не менше ніж офіційні документи. Оскільки солдати армії Російської Федерації (РФ) можуть використовувати приватну інформацію українських громадян проти них самих. Наприклад, солдати РФ 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 у Telegram-каналах, також можуть читати переписку з близькими та друзями у надії знайти докази проти російської позиції.

Іншою загрозою можуть бути фейкових додатків, які розповсюджуються через реклами в іграх та на сумнівних сайтах, мета яких – викрадення ваших особистих даних. Надалі персональні дані українських громадян можуть бути використані для спуфінгу (*spoofing* – це ситуація, в якій одна людина чи програма успішно маскується під іншою шляхом фальсифікації даних), переписок з близькими та друзями, отримання від них інформації про ключові об'єкти інфраструктури їх рідних міст, фотографій, дислокацій українських військ чи будь-якої інформації, яка необхідна ворогу.

*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 та де прийдеться вставляємо пам'ятну дату та символ – !192b0n2b91 або 2b0n2b1991!

Для складного пароля можна також використати дати народження та ФІО ваших друзів (але не близьких родичів!). Наприклад, наші друзі:

Павленко Іван Романович 1964

Гуцул Петро Юрійович 1975

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

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

●завантажуйте додатки тільки перевірених та відомих розробників;

●уникайте підключення до невідомих мереж Wi-Fi;

●не переходьте за сумнівними посиланнями навіть зі смартфону;

●надійність жодного з месенджерів не доведена. Більш-менш надійними вважається Telegram та 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).

*Двоетапна аутентифікація.*

Двоетапна аутентифікація важлива не лише у військовий, а й у мирний час, оскільки завдяки даній процедурі, користувачі різних видів послуг можуть убезпечити себе від кіберзлочинності. Отже, двоетапна аутентифікація – це підтвердження входу в Інтернет-банкінг, різноманітні акаунт, особисті кабінети за допомогою телефону (додаткового дзвінка на ваш номер або СМС із кодом-підтвердженням). Якщо дана функція увімкнена, то це серйозно ускладнює кібезлочинцям, а інколи і унеможливлює, отримання доступу до персональних даних користувача. Оскільки для входу потрібне додаткове підтвердження через доступ до телефонного номера користувача. Більшість банків без даної функції взагалі не працюють. Двоетапну аутентифікацію НЕОБХІДНО увімкнути і у Google акаунтах. Якщо ви використовуєте телефон на системі Android, то Google акаунт – це і є ваш телефон з усіма даними на ньому.

Увімкнути двофакторну аутентифікацію легко:

Необхідно відкрити сторінку google account. На панелі навігації обирати вкладку “Безпека”. В розділі “Вхід в акаунт Google” обирати “Двухетапна аутентифікація” > Почати. Далі покроково виконати запропоновану програмою інструкцію.

Те ж саме необхідно зробити і з акаунтом FaceBook чи іншої соціальної мережі, якою ви користуєтесь. Розглянемо приклад FaceBook двоетапної аутентифікації.

Потрібно перейти на сторінку https://www.facebook.com/settings/. Натиснути розділ “Безпека й авторизація” > двоетапна перевірка > редагувати. Обирати 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 вибагливими, не користуйтесь піратськими безкоштовними версіями, використовуйте лише ліцензійні програми. Це допомагає розробникам удосконалювати програмне забезпечення, дає можливість користуватись технічною підтримкою та оновлювати свої продукти, робити їх зручнішими та безпечнішими.

Не використовуйте антивіруси, програми, соцмережі, бухгалтерськими програмами, системи управління бізнесом чи процесами, які розроблені в Російській Федерації! Оскільки Федеральну 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 та на інформаційному воєнному фронті.

Використовуючи програмне забезпечення противника, розроблено в Російській Федерації ви:

●ризикуєте конфіденційністю власної інформації;

●підтримуєте загарбника.

Існує безліч більш надійного програмного забезпечення, ніж програмне забезпечення агресора!

*Безпека соціальних мереж.*

Соціальні мережі у XXI столітті – це безмежне джерело інформації про користувачів. Починаючи від місця роботи і закінчуючи особистим життям. окрім того, це приватні чи робочі переписки, які користувачі необережно ведуть, інколи розкриваючи, самі на те незважаючи, корпоративні таємниці.

У 2013 році Паша Дуров (творець та засновник соцмережі ВКонтакте) відмовився видавати Федеральній службі безпеки Російської Федерації особисті дані користувачів соціальної мережі "ВКонтакті" і тому був звільнений із власної компанії, піддавався тиску та гонінні з боку силових структур та вимушений був емігрувати. Це приклад того, що через отримання доступу до особистих даних користувачі, силові структури можуть слідкувати за людьми, збирати на них досьє та докази, наприклад, антиросійської позиції, які потім будуть представлені у суді. також даних приклад дає розуміння, що інші соцмережі та розробники програмного забезпечення могли і не відмовитися співпрацювати з силовими структурами РФ. У зв'язку з чим постає питання про безпеку соціальних мереж та того контенту, що користувачі постать. Особливо це важливо у військових час!

*Що не можна постати у соціальних мережах?*

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

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

●точні адреси та координати місць бойових дій;

●відео та фото з розпізнавальними знаками: таблички з назвами вулиць, станціями метро, автобусними зупинками, магазинами та супермаркетами, заводами й підприємствами, номери авто;

●роботу української ПВО;

●відео та 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 та не є з офіційних джерел;

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

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

●інформацію про об'єкти критичної інфраструктури українських міст, жодної інформації про такі підприємства.

Окрім того, ворог намагається поширювати фейки, щоб деморалізувати українців, а також розвідати інформацію для корегування вогню. Саме тому надзвичайно важливо перевіряти інформацію, яка до вас надходить, користуйтеся і постити лише інформацією з офіційних джерел, за можливістю розвінчати фейки.

Також можна робити пости в соціальних мережах, висвітлюючи військові 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!). Всі знімки місцевості мають бути

крупним планом, аби ворог не зміг визначити локацію (Інформаційна безпека українців, 2022).

У випадку, якщо це не буде загрожувати життю українських громадян, можна надати інформація про місцеперебування окупантів, ДРГ чи дислокацію ворожої техніки за допомогою чат-боту у *Telegram@evorog_bot*.

І найважливіше – фільтруйте друзів у соцмережах. Не додавайте тих людей, з якими ви не знайомі особисто. Перегляньте список уже наявних друзів і "вичистіть 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 чаїтися ворожий чат-бот або спуфінговий чи зламаний акаунт.

*Неправдиві повідомлення або фейки.*

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

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

Читаючи емоційні заголовки на новинних сайтах або поста, потрібно перш за все перевірити посилання на джерело інформації, якщо воно є, переглянути домен сайту, щоб він точно 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 у паніку та відчай.

●Не ліниться перевіряти інформацію, що надходить.

●Не показувати іншим неперевірену інформацію, не розповсюджуйте чутки.

*Ненадійні сайти та посилання.*

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

Ненадійні посилання – це основна зброя ворога в інформаційному полі. Їх створюють задля крадіжки паролів, доступів, викривлення інформації, знищення інформації та пристроїв. На такі посилання можна натрапити усюди – в мессенджерах, соціальних мережах, на електронній пошті чи у смс-повідомленнях.

*Що робити?*

Будьте максимально пильні та уважні до кожної дрібниці:

●дуже уважно вдивляйтеся в кожне посилання;

●перевіряти автентичність сайтів, відстежувати правильність URL-адрес ресурсів в Інтернеті, особливо сервісів банківських установ, адже через неточності можна потрапити на фейковий ресурс;

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

●обмірковуйте отриману інформацію та довіряйте власним сумнівам! Якщо такі сумніви виникають – не користуйтесь цим ресурсом;

●в Інтернеті не переходити за сумнівними посиланнями, адже в рекламі онлайн-ігор та додатків можуть бути "віруси" або фішинг, тому для завантаження необхідних файлів потрібно використовувати лише перевірені офіційні ресурси;

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

Окрім того, варто знати, що в Україні функціонує спеціальних державний орган, який на державному рівні забезпечує профілактику, контроль та розкриття злочинів в кіберпросторі – *Кіберполіція*. І незважаючи на те, що кіберполіція має не таку довгу історію в Україні, у часи воєнного конфлікту з Росією, вона займає одне з провідних місць у протидії Російській агресії. У перші дні війни Кіберполіція офіційно звернулася до найбільших світових ІТ-компаній, VPN-сервісів, компаній із розробки програмного забезпечення, антивірусів, компаній із надання послуг електронної комерції із закликом припинити співпрацю із РФ. Зокрема було надіслано понад 350 звернень, у підсумку близько 20 % компаній відреагували шляхом повного або часткового обмеження своєї діяльності на території Російської Федерації (Кіберполіція закликала 30 міжнародних VPN-сервісів припинити співпрацю з РФ, 2022).

Фундамент на якому було побудовано сучасну Кіберполіцію було закладено *27 липня 2009 року* при заснуванні **відділу 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 було створено самостійний структурний підрозділ – Управління боротьби з кіберзлочинністю. А 13 жовтня 2015 року була створена нова Кіберполіція, як структурний підрозділ Національної поліції.

Мета існування Кіберполіції в Україні є використання висококваліфікованих фахівців у протидії кіберзлочинності, залучення їх в експертних, оперативних та слідчих підрозділах поліції, задля розкриття злочинів з використанням новітніх технології.

Основними завдання Кіберполіції є:

1. реалізація державної політики у сфері протидії кіберзлочинності;
2. завчасне інформування населення про появу новітніх кіберзлочинів;
3. впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини;
4. реагування на запити закордонних партнерів, що надходитимуть 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 військове вторгнення Росії 24 лютого 2022 року з'явилися нові напрямки роботи:

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

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

●виявлення та реагування на антиукраїнську пропаганду в мережі інтернет, що координувалася підконтрольними Росії ЗМІ, а також ботами у соціальних мережах.

●пошук та ідентифікація колаборантів та інших злочинців з боку військових чи інших осіб, які підтримують війну (Кіберполіція викрила киянина на підтримці «руського міра», 2022);

●розробка систем та механізмів для швидкого та повного збору інформації з відкритих джерел про військових чи інших найманців з незаконних збройних формувань.

●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 медіа роботу проти України;

●здійснено розробку телеграм-боту "Народний месник" (@ukraine_avanger_bot, який був архівовано 1 червня 2022 у Wayback Machine), що збирав повідомлення про "ворожі мітки", "рух техніки/живих сил", "нерозірвані снаряди", "мародерів";

●розроблено сервіс "Russian black book" (https://t.me/BlackBookRussians, був архівовано 1 червня 2022 у Wayback Machine) для додавання та накопичення інформації про військових та правоохоронців Російської Федерації, враховуючи їх особисту участь у війні на території України, а також публічну підтримку війни вказаних осіб. Даний сервіс наповнювали інформацією волонтери;

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

●розроблено вебресурс DefenseUa (https://www.defenseua.com/) для російських солдат, на який звернулось більш ніж 460 осіб, які хочуть перейти на сторону України у війні або вступити до лав ЗСУ;

●розроблена платформа для документації воєнних злочинів солдат Російської Федерації в Україні (https://warcrimes.gov.ua/) тощо.

Також фахівці кіберполіції працюють над ідентифікацією та збереженням цифрових доказів, що отримані під час дослідження технічних комп'ютерних та мобільних пристроїв (мобільні телефони, смартфони, носії інформації, комп'ютери, планшети тощо), які тим чи іншим чином використовувалися для здійснення злочинів, пов'язаних із війною, або були у володінні російських окупантів. Проводиться їх детальний технічний аналіз і аналіз наявного та видаленого контенту: фото-, відеозображень і метаданих до них, контактів і зв'язків тощо, що у свою чергу дозволяє виявити сліди оперативно-значущої інформації для подальшого долучення її до матеріалів кримінальних проваджень, розпочатих проти військовослужбовців РФ.

Така інформація є основою для проведення пошуку у витоках і базах (банках) даних, наявних у відкритому та Darknet-сегменті мережі Інтернет та збагачення додатковими пов'язаними даними, як, наприклад, звання та посади військовослужбовців РФ, облікові дані військових квитків, приналежність до тих чи інших військових частин тощо.

За підтримки іноземних партнерів застосовується технологія *Clearview AI* від Нью-Йоркського постачальника (Clearview AI, 2022), з допомогою якої на основі нейромереж здійснюється розпізнавання облич російських загарбників. Програмне забезпечення здатне знаходити в мережі "Інтернет" зображення із заданими обличчями, що у свою чергу також дозволяє проводити заходи щодо ідентифікації військовослужбовців РФ і виявлення їх злочинів на території України.

Важливим напрямком роботи також є дослідження супутникових знімків, що разом із переліченими вище заходами дозволяють додатково виявляти та фіксувати

унікальні підтверджуючі факти злочинної діяльності загарбників із прив'язкою до геокоординат місць вчинення злочинів.

Також кіберполіція в рамках своїх можливостей і спільних військових директив здійснює інформаційний супротив, волонтерську діяльність, технічний супровід відновлення тимчасово окупованих територій, а також забезпечує безпеку та 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, гарно діють ви вигляді профілактичних мір, але, що робити, якщо кібербезпека вже порушена і користувач стикається із кіберзлочинністю face-to-face?

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

*У разі якщо ви стали жертвою кіберзлочинця,* перш за все, не піддавайтеся паніці. Оскільки у подібній ситуації досить часто зашкалюють негативні емоції, тому перше, що має зробити жертва кіберзлочину, це заспокоїтися, "взяти себе до рук". Для того, щоб це зробити, можна використати одну із наведених нижче техніки.

*"Дихання 4-7-8"*

Помістіть язик на піднебіння, прямо за передніми зубами (потрібно тримати його тут протягом усієї вправи). Вдихайте через ніс протягом 4 секунд. Затримайте дихання на 7 секунд. Видихайте через рот протягом 8 секунд, дозволяючи видиху видавати природний звук, ніби ви задуваєте свічку. Зосереджувати увагу на підрахунку і своєму диханні. Повторити від 5 до 10 разів, поки не відчуєте внутрішній спокій.

*"Дихання по квадрату"*

Намалюйте на листочку паперу великий квадрат. Далі потрібно дихати, плинучи поглядом по кожній його стороні: на 4 рахунки вдихнути (1 сторона), на 4 рахунки видихнути (2 сторона), на 4 рахунки видихнути (3 сторона), на 4 рахунки затримати (4 сторона). Також можна використовувати картинку нижче для цієї вправи. Обов'язковою умовою виконання цієї вправи є зосередження уваги на підрахунку і диханні. Повторити від 5 до 10 разів, поки не відчуєте внутрішній спокій.

*"М'язова напруга/релаксація"*

У стресовій ситуації тіло часто надмірно напружуються, а м'язи затискаються. Для того, щоб повернути собі емоційну рівновагу, також можна 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 у стані спокою на 5 секунд і сильно напружити кулачки. Порахувати до 5 і знову розслабити тіло. Далі необхідно напружувати сідниці, порахувати до 5, а далі – розслабити тіло. Повторити процедуру зі стопами і пальцями на ногах.

Після того, як буде знятий перший емоційний запал, потрібно скласти відповідний план дій. Для цього можна використати питання, із наведеною нижче авторською техніки *"Наслідки кіберзлочину і Я"*:

1. З якою проблемою я стикнувся (описати детально)?
2. Якими можуть бути для мене негативні наслідки цієї проблеми (перераховувати не менше 5)?
3. Який із негативних наслідків проблеми лякає мене найбільше і чому?

4. Які конкретно кроки я можу зробити, щоб уникнути негативних наслідків від цієї проблеми?

5. Які з цих кроків потрібно зробити терміново, а які можуть почекати? Проранжуйте їх (від найбільш важливих і термінових до не таких важливих і термінових).

6. Які ресурси я для цього можу залучити (людські, адміністративні, технічні тощо)?

7. Якщо в моє життя прийде один або кілька негативних наслідків від означеної проблеми, що я буду робити для того, щоб мінімізувати (нівелювати) деструктивний для мене вплив?

8. Хто або що може мені в цьому допомогти?

9. Якщо зі мною трапиться негативний наслідок означеної проблеми, якого я боюся більше за все, то…

… що я відчую в цей момент?

… що я буду робити?

… які 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 3)

11. Чому саме мене має навчити вся ця ситуація (перерахувати не менше 5 життєвих уроків).

Також для розв'язання проблеми можна використати *Квадрат Декарта* (TQM systems, 2020). Рене Декарт – французький філософ, фізик, математик, який розробив універсальну систему для прийняття рішень. Для проведення цієї методики потрібно розкреслити аркуш паперу на 4 частини, в кожній з яких будуть міститися відповіді на 4 питання.

- "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 Рис.1. представлена схема роботи з даною методику і приклад.

У кожен з 4-х квадратів ми вписуємо певні факти, які відбудуться чи ні, як і передбачає методологія Декарта. Тому дану методику доцільно використовувати для аналізу наслідків з якими жертва кіберзлочину може стикнутися. Також отриманий список можна використати для емоційного аналізу ставлення жертви до ситуації і втратам, які ця ситуація принесе. Можна обрати три різні кольори, наприклад, синій, чорний і помаранчевий, де чорний – означити як найбільш емоційно значну втрату (де поки що складно уявити, як пережити наслідки втрати), синій – втрати середньої тяжкості, наслідки якої складно, але пережити можна (є варіанти вирішення проблеми), помаранчева – втрата, наслідки якої будуть особливо не відчутними.


Рис.1. Квадрат Декарта з прикладом

Також, важливо пам’ятати, наступні постулати, якщо ви стали жертвою кіберзлочину.

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

У випадку 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 з ситуацією кіберзлочину самостійно буває досить складно і краще звернутися за допомогою (батьків, вчителів, адміністрації школи, психологу, кіберполіції). Часто підлітки просять поради і допомоги у своїх однолітків, але забувають, що підлітки дуже часто обмежені у своєму життєвому досвіді та можливостях вирішення проблеми у правовому полі. Тому краще просити про допомогу у дорослих, яким ви довіряєте.

У випадку кібербулінгу і розповсюджені контенту, який шкодить репутації та людській гідності жертви булінгу, у соціальних мережах чи на певних веб сайтах, потрібно звернутися до модератора чи адміністратора соціальної мережі або веб сайту. Потрібно написати скаргу з поясненням ситуації і проханням видалили або заблокувати відповідний контент.

Якщо ви стали жертвою кіберзлочинців, перше, що вам необхідно 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 є можливість подати електронне звернення. В даній формі слід вказати своє ПІБ, дату народження, паспортні дані, контактний номер телефону, e-mail, адресу проживання, а далі викладається суть події, а саме де (на якому інтернет майданчику), в який час, в який спосіб було скоєно злочин, який збиток від скоєного і чим підтверджується. Після описової частини, необхідно викласти прохальну, де потрібно попросити внести вашу заявку в ЄРДР (єдиний реєстр досудових розслідувань) і почати досудове розслідування, крім того визнати вас потерпілою стороною у даній справі.

Також держава гарантує кожному громадянину право на отримання безоплатної правової допомоги. Для цього необхідно телефонувати за номером Єдиного контакт-центру 0-800-213-103 (цілодобово та безкоштовно у межах України зі стаціонарних та 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 досить високому рівні і, відповідно, мало хто знає законодавчі аспекти, пов’язаних з кіберзлочинами. На нашу думку, надзвичайно важливим бути обізнаним і в даній області. На сьогодні правове підґрунтя інформаційної безпеки України створюють:

1) Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згоду на обов'язковість яких надала 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 та Стратегія кібербезпеки України

4) Кримінальний кодекс України

У Кримінальному кодексі України злочини, які здійснюються у кіберпросторі, зазвичай, розглядаються у розділі 16 “Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку” і представлено 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;

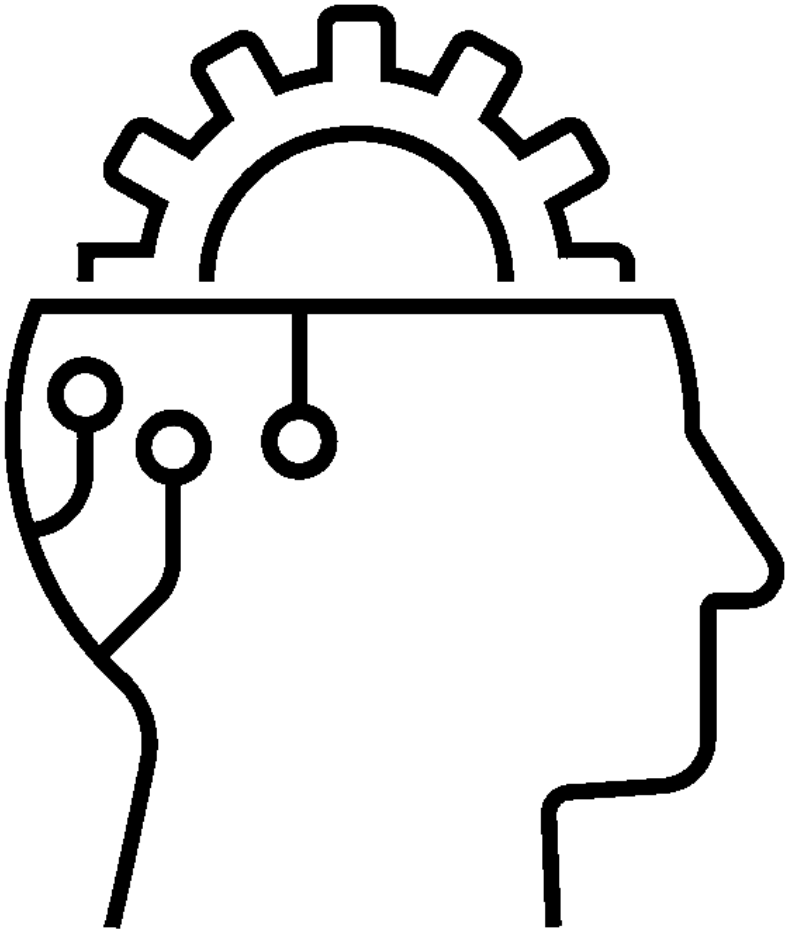
*ст. 362* – несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї;

*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 оброблюється;

*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 зарахувати *ст. 176* (порушення авторського права і суміжних прав) і *ст. 190* (шахрайство) та *ст. 209* (легалізація (відмивання) майна, одержаного злочинним шляхом).

# ЧАСТИНА ІІ



## ПРАКТИКУМ № 1.
## *Методика "ЛАНДШАФТНА МАПА ПОТЕНЦІЙНИХ КІБЕРЗАГРОЗ"*

Для того, щоб створити у дітей навички протистояння кіберзагрозам, спочатку потрібно "м'яко" увести їх в тему, створити підґрунтя на якому побудується фортеця вмінь та навичок протистояння кіберризикам. Сучасні діти ліпше запам'ятовують інформацію, що представлена у вигляді візуальних образів, особливо образів, які вони створили самі, в які вклали власну логіку, уявлення та символи. У зв'язку з чим ми пропонуємо розпочати знайомство дітей з даним курсом через авторську методику "Ландшафтна мапу потенційних кіберзагроз". Ця методика базується на принципах арт-терапії.

Дана методика може використовуватися як для індивідуальної, так і для групової роботи. Але в даному посібнику вона буде представлена у груповій версії. Також зважаючи на вимоги часу ми представимо методику для проведення в онлайн та офлайн форматах.

**Основною метою** даної методики є створення у свідомості дітей цілісного образу кіберзагроз з якими вони можуть зіткнутися в інтернет просторі.

**Завдання:**

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

Ми рекомендуємо розбити методику на три смислові блоки і проводити їх у різні дні. Оскільки емоційне навантаження на дітей, якщо проводити всі три блоки підряд, може бути значним. Що в свою чергу знизить їх рівень сприйняття інформації і залученості у процес.

**Тривалість** блоків має різний часовий інтервал.

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

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

Блок 3. Кіберзагрози військового часу. Орієнтовний час – 1,30 хв.

*Блок 1. Створення ландшафтної мапи потенційних кіберзагроз*

| Онлайн | Офлайн |
|---|---|
| **Інструментарій** (що необхідно для проведення блоку): ватман, кольорові маркери, кольоровий папір, клей, ножиці, степлер, листочки формату А4 та інші матеріали за допомогою яких діти можуть проявити свою креативність (старі кольорові журнали, ґудзики, пластилін, штучні квіти, бусинки). | **Інструментарій** (що необхідно для проведення блоку): одна із програм за допомогою яких можна створити Mind map.<br>Ми рекомендуємо:<br>**Coggle** – це онлайн додаток для створення Mind map (передбачено безкоштовний тарифний план). Сервіс працює у браузері. У роботі можна використовувати зображення, індивідуальні колірні схеми, а створенні мапи можуть експортуватися в форматі PNG або PDF. Додаток підтримує спільну |

роботу разом із командою над проектами (Coggle YouTube Channel, 2016), тому його можна використовувати для групової роботи.

Програма **iMindMap** – сервіс від самого славнозвісного **Тоні Бьюзена**, родоначальника, автора методики побудови ментальних карт (передбачено пробний термін безкоштовного використання протягом 30 днів). Програма пропонує 4 режими: фіксація ідей і думок, мозковий штурм, створення інтелект-карт, Конвертація даних в презентації 2D і 3D, ПДФ-файли, таблиці і інші формати (Coggle YouTube Channel, 2016). Дана програма використовується для індивідуальної роботи.

Ви також можете використовувати будь-які інші програми.

**Хід роботи:**

1. Вступ – 20 хв
2. Створення арт-продукту (мапи) – 45 хв
3. Обговорення – 25 хв
4. Завершення –в 10 хв

Вступ

Слово модератора:

*“Кожен із вас так чи інакше стикався із загрозами, які в собі таїть Інтернет-середовище… Можливо, хтось втрачав гроші на кібершахрайстві, у когось зламували чи крали акаунти в соціальних мережах, хтось ставав жертвою кібербулінгу, а у когось під виглядом дружнього спілкування видурювали конфіденційну інформацію. Не обов’язково, що так чи інша історія трапилася саме з вами, але можливо із вашими знайомим чи друзями, ви могли про щось таке чути від батьків, читати в інтернеті або дивилися до телевізору.*

*Можете розказати, що ви знаєте про загрози в інтернеті?”*

Далі модератор дає можливість дітям висказатися, розказати свої чи чужі історії. записувати його на дошці, щоб всі бачили.

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

У випадку, якщо діти не бажають говорити, можна використати спеціальну підготовлений список про можливі загрози в інтернеті для обговорення даної теми (Див. Додаток 1)

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

Після кожної історії, потрібно давати назву кіберризику. Обов’язково потрібно назву візуалізувати, у зв’язку з чим ми пропонуємо назначити когось відповідальним за цей шматок роботи:

записувати назви у себе на комп’ютері і демонструвати екран, щоб всі бачили загальну картину.

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

Під кінець розповідей на дошці точно мають бути зазначені такі основні кіберризики:

- Фішинг або Кетфішинг
- Спуфінг
- Тролінг або Флеймінг
- Сталкінг
- Кібербулінг
- Кібербойкот
- Секстінг
- Кібергрумінг
- Реттінг

Створення арт-продукту

Слова модератора:

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

Слова модератора:

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

*Ви можете створити мапу потенційних кіберризиків будь-якою, але… Є кілька умов:*

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

*2. Якщо ви будете використовувати якісь умовні позначки, їх розшифровка обов’язково має зазначатися у мапі.*

*3. Ваша мапа має вміщувати в собі всі загрози про які ми говорили і, можливо, ще якісь, які ви згадаєте під час роботи над цим завдання.*

*4. Розміщення на даній мапі елементів, їх форма та розмір і навіть кольоровий супровід - має бути погоджено усіма членами групи одноголосно. Це важлива умова! Якщо хтось має своє бачення розміщення елементів - вам потрібно буде вступити у переговори і домовитися тим чи іншим способом. І пам’ятайте, що ви роботи спільну справу, а не відстоюєте індивідуальні переконання!*

*Також на останок дам вам одну пораду, до того, як почнете фізично створювати мапу, обговоріть і погодьте композицію. Що де знаходиться? За яким принципом? Тобто чому саме цей елемент знаходиться тут? Що з чим елементом пов'язано? Якими будуть межі між елементами і т.д.*

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

Обговорення

Слова модератора:

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

Необхідно дати дітям час на презентацію своєї роботи.

Далі за допомогою відкритих питань обговорити результати їх роботи. Питання від модератора допоможуть дітям краще зрозуміти свою роботу і відрефлексувати моменти на які вони в процесу роботи, можливо, не акцентували увагу.

На що потрібно звернути увагу при обговоренні мапи потенціальних кіберризиків з дітьми:

1) на принцип за яким діти розташовували елементи на мапі. Тобто чи є логіка побудови, чи, можливо, елементи знаходяться у довільному. Принцип побудови можна дізнатися під час презентації мапи.
   Може бути кілька принципів у побудові мапи потенційних кіберризиків. Наприклад, від найчастішої загрози до найменш зустріненої 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 кіберзагрозу - двоє або група.
2) на центральну фігуру на колажі. В центрі може бути розміщення одна зі загроз або це може бути перетин кількох кіберзагроз.
   Для аналізу розміщення елементів на ландшафтній мапі потенційних кіберзагроз можна використовувати принципи побудови колажів у арт-терапевтичному підході.
3) наявність чітких меж у кожної із кіберзагроз або їх відсутність. Якщо межі відсутні потрібно уточнити, чому це саме так. І зазначити, в яких елементах ці межі відсутні.
   При індивідуальній роботі, це може вказувати на факт попереднього досвіду взаємодії діти з цією кіберзагрозою.
4) на розмір областей, кожної із кіберзагроз. Яка з загроз найменша, а яка найбільша. Потрібно уточнити, чому діти обрали саме такий розмір для кожної із загроз.
5) на кольори, якими заповнені області кожної із кіберзагроз. Уточнити, що для дітей означає той чи інший колір, який сенс вони у це вкладають.
   Для аналізу кольорів мапи потенційних кіберзагроз можна використовувати кольорову символіку тесту Люшера.
6) наявність символів або певних втілень для тієї чи іншої кіберзагрози. Уточнити у дітей асоціації і попросити пояснення символу. Потрібно уточнити, що діти у цей символ вкладали.

Завершення

Слово модератора:

“*Сьогодні ми працювали над темою кіберзагроз поділіться своїми враженнями. Що для вас було цікавим? Що нового ви для себе відкрили? Можливо було щось, що не сподобалось?”*

*Я пропоную вам обрати місце у 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 та кіберзагрози. Емоційна рефлексія*

Онлайн

**Інструментарій** (що необхідно 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 проявити свою креативність (старі кольорові журнали, ґудзики, пластилін, штучні квіти, бусинки), мапа потенційних кіберзагроз.

Офлайн

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

**Хід роботи:**

1. Вступ - 10 хв
2. Створення арт-продукту (фішок) - 15 хв
3. Обговорення - 25 хв
4. Завершення - 10 хв

Вступ

Слово модератора:

*“Сьогодні ми продовжуємо вивчення теми кіберзагроз. Чи міркували ви про потенційні кіберризики та мапу, яка була створена? Можливо, у вас з’явилися якісь цікаві думки чи свіжі ідеї? Може, ви стикнулися з якимись історіями, що пов’язані з цією темою? Якщо хтось хоче поділитися, то, будь ласка…”*

Модератор має дати учасникам можливість проговорити свої думки, емоції та почуття, якщо вони у когось виникли щодо теми їх роботи на минулому занятті.

Слово модератора:

*“Давайте повернемося до мапи, яку ви створили на минулому занятті… Скажіть, коли ви зараз дивитесь на неї чи є у вас бажання щось змінити в ній? Можливо, щось додати?”*

Якщо у учасників є бажання щось додати до мапи, модератор має дати їм таку можливість.

Створення арт-продукту (фішок)

Слово модератора:

*“І сьогодні ми будемо з вами досліджувати наскільки ви готові чи не готові стикнутися у реальному житті з тими кіберризиками, які ми з вами розбирали на минулому занятті.*

*Але перед початком, я хочу запропонувати вам створити фішку, яка б на символічному рівні уособлювала б вас. Цю фішку ми будемо використовувати далі у роботі.*

*У вас вже є підготовлені заготовки у формі кулі. Для наданням їх 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 хвилин. “*

Слово модератора:

*“І сьогодні ми будемо з вами досліджувати наскільки ви готові чи не готові стикнутися у реальному житті з тими кіберризиками, які ми з вами розбирали на минулому занятті.*

*Але перед початком, я хочу запропонувати вам створити фішку, яка б на символічному рівні уособлювала б вас. Цю фішку ми будемо використовувати далі у роботі.*

*Кожен з вас зараз створіть новий елемент на мапи. 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 самостійний, незалежним і легко пересуватися по карті.*

*Для створення фішки у вас є до 5 хвилин”*

Обговорення

Слово модератора:

*“Будь ласка, подивіться на мапу.*

*1) Подумайте, яка із представлених кіберзагроз лякає вас найменше”*

Модератор дає кілька хвилин на “подумати” і виконати завдання.

*“Чому ви обрали саме цю кіберзагрозу? Ви знаєте як впоратися у ситуації, коли зіткнетеся face to face зі такою загрозою?”*

Модератор дає кожному учаснику час дати відповідь на це запитання. Можливо поділитися власним досвідом врегулювання проблемної ситуації, що була пов’язана з даним кіберризиком.

*2) “А тепер подумайте, яка із 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 це можливо для вас, то поділіться власним досвідом”*

Модератор дає кожному учаснику час дати відповідь на це запитання.

*3) Чи є із представлених кіберризиків такі, з якими ви вже стикалися у житті і точно знаєте, що робити у такі ситуації? Кому дзвонити, як діяти і т.д.? Якщо таких варіантів кілька, поставте свою фішку на одному з них, а інші просто проговорить у голос.*

*4) Чи вважаєте ви щось із представленого на карті 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 із представленого на карті різноманіття, що ви засуджуєте найбільше? Те, що вважаєте абсолютно несприятливими?*
*Щось одне. Чому?*

*6) Чи є щось із представленого на карті різноманіття тим, з чим би ви хотіли зіткнетеся face to face, щоб випробувати власні сили? те, що ви сприймаєте 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 дітям, що жертвою кіберзагроз може стати кожен. Не існує імунітету. Потрібно розвивати пильність та критичне мислення.

*7) Зараз візьміть листок паперу і ручку, на ньому напишіть список визначених кіберризиків. Написали? А тепер навпроти кожного із них напишіть ті емоції і почуття, які конкретно цей ризик вас визиває.*

*8) А тепер сильно не задумуючись, напишіть навпроти кожного ризику ім'я людини до якої б ви звернулися по допомогу, який щось подібне 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

Слово модератора:

"*Сьогодні ми продовжили працювати над темою кіберзагроз, досліджували ваше ставлення, знання, почуття та емоції щодо них. Поділіться, будь ласка, своїми враженнями після заняття. Що нового ви про себе дізналися? Що для вас стало незвичайним? Можливо, якимось відкриттям?"*

*Блок 3. Кіберзагрози військового часу*

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

**Хід роботи:**

1. Вступ - 20 хв
2. Доповнення арт-продукту - 30 хв
3. Обговорення - 20 хв
4. Завершення - 10 хв

Вступ

Слово модератора:

*"Сьогодні ми з вами завершуємо нашу роботу над мапою потенційних кіберзагроз. І піднімемо складне питання про військові кіберзагрози.*

*Як ви вважаєте чи відрізняються кіберризики у мирний час від військового? Якщо так, то чим саме?*

*Які ви можете назвати потенційні військові кіберризики?*

Записуємо обов'язково назви кіберризиків у військовий час і їх основні (короткі) характеристики.

Створення арт-продукту

Слова модератора:

*“Тепер, коли ми проговорили військові кіберзагрози, я пропоную вам доповнити вашу ландшафтну мапу потенційних кіберризиків.*

Обговорення

Слова модератора:

*“Ви доповнили свою мапу потенційних кіберзагроз.*

*Які почуття у вас мапа викликає зараз?*

*Яка із представлених на ній кіберзагроз, здається вам найстрашнішою (викликає найбільший страх)? Чому?*

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

Завершення

Слова модератора:

*“Сьогодні ми завершили працювати над мапою потенційних кіберзагроз.*

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

*А що для себе ви зрозуміли внаслідок усієї роботи над мапою потенційних кіберзагроз?*

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

*Що ресурсного ви для себе взяли після роботи з темою 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. У зв'язку з чим ми пропонуємо використовувати формат дебатів або дискусійного клубу.

Дебати – це спеціально організований публічний обмін думками між двома сторонами на задану тему. Це поняття має довгу історію, починаючи від філософських і політичних дебатів Стародавньої Греції, крізь заснованих в епоху просвітництва дискусійних товариств та представленому нині, всесвітньовідомому навчальному методі.

У класичному варіанті дебатів питання для обговорення вносить голова або модератор, який переходить до регулювання дискусії між двома або більше учасниками публічних дебатів. Спікерам надається певна кількість часу, щоб аргументувати свою точку зору. Спікерам не дозволялося лихослів'я чи образи стосовно інших ораторів, або відхилятися від теми, що розглядається. Учасники дебатів мають переконати в 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: 60).

Дебати можуть стати платформою не тільки для критики, але й розвитку нових ідей та покращення 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.

Дані форми безпечного вираження думок можуть використовуватися для обговорення будь-яких тем і позицій, але з урахуванням специфіки даного посібника, ми пропонуємо два варіанти: "Ризики кіберсоціалізації" або "Особливостях воєнної кібербезпеки".

### *Варіант 1. РИЗИКИ КІБЕРСОЦІАЛІЗАЦІЇ*

Як ми вже зазначали, сучасні люди живуть у світі технологій, які невпинно розвиваються. Вже не можна уявити своє життя без комп'ютерів, смартфонів, планшетів та соціальних мереж. Комунальні платежі здійснюються через спеціальні сайти, оплата проїзду у 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, без сумнівних переваг, вони кіберсоціалізувалися.

*Кіберсоціалізації* (від грец. Kybernetike – "мистецтво управління", від грец. kybernao – "правлю кермом, управляю", від грец. Κυβερνήτης – "керманич" та англ. socialization – "соціалізація") є процесом опанування навичками користування інтернетом, різноманітними програмними продуктами віртуальної мережі, наслідком чого є специфічна соціалізація особистості.

Але у кіберсоціалізації, як і будь-якого процесу, існують свої власні ризики. Інколи – об'єктивні, інколи – потенційні, інколи – вигадані, а інколи – неминучі. У даній книжці підготовлений перелік тем, щодо проблем, з якими може стикнутися людство із розвитком технології. Дані теми можна використовувати для роздумів чи

дискусій на тему кіберсоціалізації *(див. Додаток 2)*. Більшість тем мають психологічне спрямування та моральну дилему. Вони представлені у вигляді карток. З одного боку картки – назва кіберризику, з іншої – короткий опис проблеми.

**Основною метою** даної гри є допомогти учням розвинути навички логічної та послідовної аргументації у публічних виступах, вміння слухати та відстоювати власну позиції у взаємодії з іншими людьми, а також поглибити знання у психологічних особливостях кіберсоціалізації особистості.

**Завдання:**

● Порівняти особливості життя людей до Інтернет-епохи та під час неї, а також спрогнозувати як зміниться людське життя у недалекому майбутньому.

●Навчити сформувати логічну та продумати аргументацію для захисту власної думки та позиції.

●Сформувати навички виступати публічно.

●Надати впевненість у собі під час відповідати на запитання аудиторії.

**Особливості та правила проведення дискусійного клубу:**

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

Кожна команда може мати два-три конструктивних (стверджувальних виступи) виступи і два-три виступи-заперечення. Але не більше. Перша команда дає стверджувальну промову, після якої друга команда спочатку дає заперечувальну проводу (спростування) на ту аргументацію, що приводила перша команда, після чого висловлює свою стверджувальну промову. Після цього перша команда дає заперечувальну промову, а далі – свою стверджувальну.

Тобто план такий:

| | |
|---|---|
| Раунд № 1 | Команда № 1. Стверджувальна промова |
| | Команда № 2. Заперечна промова |
| Суддівське рішення | |
| Раунд № 2 | Команда № 2. Стверджувальна промова |
| | Команда № 1. Заперечна промова |
| Суддівське рішення | |
| Раунд № 3 | Команда № 1. Стверджувальна промова |
| | Команда № 2. Заперечна промова |
| Суддівське рішення | |

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

Команда, яка висловився стверджувальну промову, має привести аргументи та докази, що будуть відстоювати визначену позицію. У промові має бути присутня логіка, щоб переконати розумну, але раніше необізнану особу, що розумніше вірити цьому твердженню, ніж не вірити йому. Факти мають бути точними. Дозволено використання візуальних матеріалів, але після їх оприлюднення, вони також стають доступними для аргументації іншою командою за їх бажанням.

Кожному оратору, як тільки він завершує свій конструктивний виступ, ставлять запитання. Оратор повинен відповідати на запитання без консультації з членами команди. Питання можуть ставити як члени опозиційної команди, так і глядачі. Запитання має бути чітко сформульоване і мати прямий стосунок до теми.

У період заперечувальної 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. Суді повинені базувати своє рішення виключно на представлених під час дискусії аргументах та матеріалах, не беручи до уваги іншу інформацію, якою вони можуть володіти або власну суб'єктивну позицію.

**Тривалість дискусій.**

Для письмової форми роботи тривалість триватиме від 60 хвилин до 1,30 хвилин. В залежності від індивідуальних особливостей роботи групи.

Для дебатів тривалість буде залежати від кількості раундів. На кожен раунд (стверджувальний виступ – виступ-заперечення та час присвячений відповідям на запитання) відводиться 60 хвилин. На кожен виступ дається до 10 хвилин + до 10 хвилин на час "питання-відповіді" до оратора. І до 10 хвилин на прийняття рішення судівською комісією, хто переміг у цьому раунді.

Ми рекомендуємо проводити дана завдання у два смислові блоки, спочатку з індивідуальному форматі роботи, а потім у груповому. Але в залежності від обставин, описані нами блоки можна проводити незалежно один від одного.

**Інструментарій:** підготовлені картки для дискусійного клубу, білі листки паперу формату А4, ручки, ноутбук або комп'ютер для кожної групи учасників із доступом до Інтернету, програма Power Point (за потреби), проектор.

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 у письмовому вигляді*
(індивідуальний формат роботи)

На початку заняття модератор має запропонувати дітям подумати і описати як жили люди до появи Інтернету (з якими труднощами вони зтикалися, які переваги мали). І порівняти цю картину з тим життям, яке вони мають зараз – із вільним доступом до усіх благ цивілізації та Інтернетом 24 годин на добу, мобільним зв'язком та різними мобільними додатками, що полегшують життя тощо.

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

Після того, як діти опишуть майбутнє людства, модератор має поставити питання про ризики, ризики кіберсоціалізації, з якими люди стикнуться у майбутньому. Якими вони будуть? Як зміниться життя? Можна створити список і записати їх.

*Слово модератора:*

*У мене з собою є картки, кожна із них присвячена певній проблемі, з якою зіткнулося або зіткнеться людство у зв'язку із технічним прогресом. 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, листок А4, згори на ньому напишіть назву проблеми, яка вам дісталася. Потім розділіть листок на дві колонки. В першій колонці потрібно буде записати аргументи "за", якщо проблема, що означена на ваші картці є або може стати серйозним кіберризиком для людства. У другій колонці вам потрібно привести 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 розумі, розвиває інтелект та вміння адаптуватися до будь-якої ситуації.*

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

*Тепер, коли ви завершили роботу, будь ласка, передайте ваш листок з аргументацію сусіду зліва (таким чином всі учасники мають отримати чужу роботу). Зараз ваше завдання, прочитати написану аргументацію і зробити на її основі висновок – чи дійсно це серйозний кіберризик чи ні. Запишіть ваш висновок внизу листочку. Окремо обведіть пункти на листочку, що заставили вас прийняти подібне рішення. Якщо у вас є якісь думки з приводу цього кіберризику або ви хочете додати до списку свою аргументацію, ви можете це зробити, але виберіть інший колір ручки. І також напишіть своє ім'я та прізвище на листочку, оскільки нині ця робота стала спільною.*

*На дану роботу у вас є 10 хвилин.*

*Наступне завдання. Будь ласка, передайте свою картку з проблемою сусіду з права. Тепер у кожного з вас нова картка. Ви маєте подумати і написати лист до своєї бабусі або маленької сестрички/братика 6 років, в якому будете пояснювати, що це за кіберризик і чому варто цього остерігатися. Ви маєте описати все так, щоб зрозуміла і маленька дитина або людина без значного комп'ютерного досвіду. Простими словами. Приводьте прості та зрозумілі аргументи на підтримку своєї позиції.*

*Дану роботу не підписуйте, будь ласка. Але у горі великими літерами вкажіть назву ризику кіберсоціалізації.*

*На дану роботу у вас 15 хвилин. За хвилину до закінчення часу я вас про це попереджу.*

*Тепер свої есе, будь ласка, віддайте 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 та зрозумілість аргументації – 3 бали.*

*Б) Логічність, чіткість та послідовність викладу думок – 2 бали.*

*В) Переконливість позиції автора (якщо після читання тексту, незалежний оцінювач зможе 100 погодитися з позицією приведеною у тексті і не залишитися двояких трактувань або інших моральних дилем) – 3 бали.*

*Б) Цікавість - 2 бал.*

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

Після завершення роботи, модератору необхідно провести обговорення з дітьми. Орієнтовні питання для обговорення:

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

●А кому було складно знаходити аргументацію "проти"? Підніміть руки? Наскільки вам було складно "залізти у черевики" точки розу опонента? Це вміння дуже

важливе, оскільки перемогти у протистоянні можна лише, коли досконально вивчити свого супротивника, його позицію, його аргументи, його мотиви. Пошук контраргументів – неймовірно важливий навик для перемоги.

●Чи легко вам було підібрати просту аргументації для пояснення ризиків на другому етапі роботи?

●Кого ви являли, коли писали твір? 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 свої есе на перевірку іншій людині?

●Які почуття і думки у вас виникли, коли ви побачили, як саме був оцінена ваша праця?

●Чи було вам самими складно оцінювати роботу іншої людини?

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

●Чи враховувати ви при оцінці есе вашу власну позицію і думку стосовно ризику? Чи було таке, що ви оцінювати думки автора есе вище, бо його думки збігаються з вашою позицією? І навпаки, чи занижували ви оцінку, якщо думка автора есе не збігалася з вашою?

Слово модератора:

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

*Подумайте і скажіть, чи була для вас якась різниця у першому випадку оцінювання, коли ви знали ім'я автора есе і у другому, коли оцінювання відбувалося "наосліп".*

*Який із видів оцінювання ви вважаєте більш об'єктивним?*

Обговорення може тривати від 10 до 30 хвилин.

*Блок 2. Дебати*
(груповий формат роботи)

Підготовчий етап.

Для проведення дебатів, учнів потрібно розділити на парну кілька команд, в середньому від 2 до 5 людей в команді, але може бути і більше. Якщо, на розсуд організаторів дебатів, команд буде більше ніж 2, то дебати команд мають проходити паралельно, але в різних приміщеннях.

Визначити, хто із учнів буде виконувати роль суддів. Ми пропонуємо обирати не одному, трьох суддів для більшої об'єктивності.

Потрібно запропонувати учням обрати наосліп картку з потенційним ризиком кіберсоціалізацією. Так само рандомним методом обрати чи будуть вони захищати позицію "це серйозний ризик для людства" або позицію "це не ризик, це особливість життя і в цьому немає нічого страшного".

Обрати скільки буде раундів у дебатах один, три чи більше. Уточнить час кожного із раундів.

Обговорити правила дебатів, що будуть спільними для всіх команд.

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

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

Слово модератора:

*Тож, ми обговорили усі організаційні моменти і час розпочати наші дебати. Нагадую, що під час виступу оратора у залі має зберігати повна тиша! Ніхто не має право розмовляти, перешіптуватися із сусідом або перебивати людину, що виступає!*

*Оратору на виступ надається 10 хвилин, за дотриманням часу слідкують судді. Після цього я надам слово команді-опоненту для заперечної 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 заперечною промовою, щоб все було чесно! Між стверджувальною промовою та промовою запереченням ми зробимо 5 хвилин перерви для підготовки учасника. На заперечну промову також дається до 10 хвилин (судді слідкують за часом). До речі, команда-опонентів, ваш представник може з собою взяти блокнот та ручку, щоб робити нотатки за потреби.*

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

*І судді будуть підбивати підсумки раунду і визначати команду-переможця. І на їх рішення буде впливати не тільки наведена аргументація, але й ораторські навики (те, як ви проводити презентацію), ваша ввічливість та конструктивність у дискусії (коректність та вміння не виходити "за рамки"). А також те, як представник команди відповідав на питання.*

*В кінці переможе та команда, хто виграє найбільшу кількість раундів.*

*Отже, прошу до слова першого оратора!*

За описаною схемою будуть проходити усі раунди дебатів. Модератор має уважно стежити за дискусією, підказувати правила та коригувати (у випадку необхідності) поведінку учасників дебатів. Інколи час може змінюватися, в залежності від потреб учасників.

Після завершення дебатів, модератор має надати слово усім бажаючим висловити свої враження, емоції та почуття: як членам-учасникам, глядачам, так і суддям.

## *Варіант 2. ОСОБЛИВОСТІ ВОЄННОЇ КІБЕРБЕЗПЕКИ*

З урахуванням особливостей воєнного часу, пропонуємо провести дискурсивний клуб із стратегії і тактики, запропонувавши дітям розробити "Концепцію воєнної кібербезпеки". Як вже було зазначено, кібербезпека державного рівня має свою специфіку та особливості. Агресія Російської Федерації проти Української держави перш за все має на меті дестабілізацію в країні, підрив бойового духу та віри населення у перемогу, розширення дезінформації та фейків з метою залякування мирного населення та формування у них необхідних ворогу світоглядних позицій. "Відключити, знищити, дестабілізувати", – ось їх основні принципи ведення війни. Масові відключення електроенергії, телефонного зв'язку та Інтернету, труднощі з обслуговуванням клієнтів і проведенням банківських операцій, реальні фінансові збитки – це те, що використовує ворог вже сьогодні.

Як ми вже зазначали, *інформаційна війна,* яку веде Російська Федерація проти населення України, підриває політичної та соціальної системи, створює тиск на масову свідомість засобами психологічної обробки населення для дестабілізації суспільства та держави. У зв'язку з цим вважаємо за необхідне на дискусійному клубі підняти цікаву та необхідну темою "Концепції воєнної кібербезпеки країни". Тема складна та

неоднозначна у зв'язку з цим, підготовка до проведення дискусійного клубу може запереченням зайняти певний час.

**Основною метою** даної гри є допомогти учням розвинути навички логічної та послідовного мислення, формування стратегій і тактик, аргументації у публічних виступах та відстоювати власну позиції, а також пошуку, збору. аналізу та узагальненню інформації щодо особливостях воєнної кібербезпеки на державному рівні.

**Завдання:**

● Детально вивчити особливості воєнної кібербезпеки та стратегій державного захисту.

●Навчитись розробляти стратегію і тактику ведення інформаційної війни

●Сформувати логічну та продумати аргументацію для захисту власної позиції.

●Розвинути навички публічних виступів.

●Надати впевненість у собі під час відповідати на запитання аудиторії.

**Особливості проведення та тривалість дискусійного клубу:**

Учасників дискусії поділяють на дві команди, кожна з яких складається щонайменше з 5 учасників. В класі можуть бути присутні діти, які не бажають брати участь в даній активності, в такому випадку вони мають взяти на себе роль "Спостерігачів", які мають активно включатися в процес обговорення проектів на етапі проведення дискусійного клубу, але не мають жодним чином брати участь у підготовці командних проектів. У якості спостерігачів також можна запрошувати учнів з інших класів для жвавої дискусії під час обговорення.

*Підготовчий етап.*

Кожна команда отримує завдання розробки Концепції державної кібербезпеки. У зв'язку зі складністю отриманого завдання, командам на підготовку проекту, який буде захищатися і обговорюватися на дискусійному клубі має бути виділений 1 місяць на підготовку.

Ролі в командах діти мають розділити самостійно.

Через місяць кожна команда має надати підготовлену Powerpoint-презентацію та 1 (за бажанням – 2-х) спікера для презентації проекту.

*Процес проведення дискусійного клубу.*

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

Для презентації проекту кожна група отримує по 20 хвилин часу. По завершенню презентації спостерігачі та учасники команди-супротивників мають до 15 хвилин часу на уточнюючі та "каверзні" питання. Після цього надається час на виступ іншій команді та, відповідно, час на уточнюючі питання.

Далі відбувається дискусія при якій кожний учасник процесу може висловити власну думку щодо представленої командами стратегії. А учасники команди можуть погодитися або не погодитися із зауваженнями і відстоювати представлену позицію в екологічній та коректній манері. На проведення дискусії дається 30 хвилин.

На визначення переможців – до 10 хвилин.

На висловлення зворотного зв'язку учасників дискусійного клубу – до 10 хвилин.

Загальний час проведення заходу – 2 години.

Також потрібно заздалегідь потурбуватися про суддівську колегію з 2-3 осіб, вчителів, краще тих, які не читають предмети у цих учнів, щоб їх рішення було об'єктивним. Судді мають погодити між собою критерії оцінки. Наприклад:

●Харизматичність виступу - 10 балів

●Гарно 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 у представленої стратегії - 5 балів

●Влучність запитань - 5 балів

●Чіткість та широта відповіді на запитання - 5 балів

тощо

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

*Блок 1. Домашня робота над проектом*

До початку дискусійного клубу, учасники команд мають підготувати проекти за визначеним планом:

1. Проаналізувати інформацію, що знаходиться у вільному доступі щодо вже наявних заходів по кібербезпеці державного рівня. Для цього можна використовувати лише офіційні ресурси державних структур.
2. Виявити "слабкі" сторони наявної державної стратегії та представити реально існуючі випадки порушення державної кібербезпеки (можна використовувати матеріали перевірених шанованих ЗМІ).
3. Також необхідно окремо виділити *потенційні* ризики для державної кібербезпеки.
4. На основі існуючої інформації розробити стратегічний план державної кібербезпеки (що державі потрібно покращити, які заходи провести, які стратегічні напрямки розвивати тощо). Учасники можуть також представити конкретні рекомендації (Наприклад, ввести у школах урок "Кібербезпека" для старшокласників).

За результатами пошуку, аналізу та узагальнення інформації, необхідно створити презентацію в Powerpoint. Необхідні елементи:

1. Титульний листок з назвою проекту та назвою команди (Перерахувати її учасників)
2. На кожне із 4 поставлених завдань може бути не більше 3 слайдів.
3. Обов'язково передостаннім слайдом має бути "Дякую за увагу" – як знак поваги до слухачів.
4. Останній слайдом має бути Інформація про Індивідуальний внесок учасників проекту за принципом: ПІБ – що саме за роботу зробила людина у цьому проекті (наприклад, шукала інформацію для 1 завдання і брала участь у формуванні слайдів 2-3).

Презентація Power Point НЕ має містити Контрастні стилі оформлення , а також шрифти менше за 10 пт. Що є незручними для сприйняття інформації.

У випадку, якщо дітям буде складно самостійно виконати завдання, можна призначати одного із шкільних вчителів керівником проекту до якого можна звернутися до консультаціями і допомогою.

*Блок 2. Проведення дискусійного клубу*

Слово модератора: *Сьогодні ми зібралися тут, щоб обговорити важливе та актуальне питання кібербезпеки нашої країни. Для цього дві команди учасників нашого дискусійного клубу будуть представляти сьогодні проекти власного виробництва щодо "Концепцію воєнної кібербезпеки України". Давайте привітаємо їх оплесками.*

*Кожній команді для виступу дається до 20 хвилин (сповідаюся ваші спікери вдома готувалися і розуміють, що перевищувати час не можна!).*

*Глядачі і учасники команди-опонента вам забороняється під час виступу оратора розмовляти, перешіптуватися, дискутувати або якимось іншим чином заважати людині говорити! За це будуть зніматися бали з команди, а глядачі, що не дотримуються тиші у залі будуть сидіти на "Ганебному стільці" от у тому кутку!*

*Після завершення виступу першої команда буде час на уточнюючі та каверзні запитання – до 15 хвилин.*

*Після цього я надам час на виступ іншій команді та, відповідно, час на уточнюючі питання.*

*Далі відбувається дискусія при якій кожний учасник процесу може 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 та дає їм вступне слово, де вони озвучують критерії оцінювання сьогоднішнього дискусійного клубу.

*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 один бал. За цікаві власні пропозиції щодо державної стратегії вони можуть отримати 2 бали. В кінці дебатів, я дам слово глядачам, які мають бали, щоб вони висловили власні симпатії та пожертвували накопленими балами на користь тієї команді, яка на їх думку, представила найкращу стратегію. Глядачі також мають пояснити, чому вони вважають, що ця стратегія найкраща, інакше бали у скарбничку команди зараховані не будуть. Все чесно! бали будуть отримані не за особисті симпатії, а за крутість проекту!*

*Отже, готові починати?*

*До слова запрошую першого спікера!*

Модератор має уважно стежити за дискусією, підказувати правила та коригувати (у випадку необхідності) поведінку учасників дебатів. У його обов'язки входить слідкувати за часом і вести облік глядачів, які задавали запитання та висловлювали власні пропозиції та їх балів.

Після дискусії та пожертвування балів, модератор надасть суддям 5 хвилину перерву для підрахунку балів та обговорення. Далі – судді озвучують свій вердикт.

В кінці модератор має підбити підсумки дискусійного клубу і послухати зворотній зв'язок від учасників.

## ПРАКТИКУМ 3.
## Правила сімейної кібербезпеки.
## *Методика "ТОТЕМНИЙ КІБЕРЇЖАК"*

Інформаційна безпека та кібербезпека, у нинішньому суспільстві стоять на одному рядку із фізичною безпекою і можуть бути зарахованими до переліку базових потреб. Оскільки вони стосуються захисту життєво важливих інтересів людини, а у випадку українського кейсу і більш глобально – суспільства, держави в цілому. Неправдива, неповна, невчасна інформація може нанести шкоду і навіть загрозу життю в умовах воєнного часу. Особливо вразливі у цьому контексті діти, оскільки вони не завжди знають, яку інформацію можна викладати в мережу, а яку не варто. Інколи вони також не можуть правильно зреагувати на матеріали/інформаційні повідомлення, що надходять до них із з мережі, Це може відбуватися із різних причин: інколи у зв'язку з недостатністю життєвого досвіду, інколи це може бути пов'язано із вразливістю дитячої психіки.

Деякі батьки у бажанні 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 наш погляд, звичайні заборони і тотальний контроль не може стати рішенням глобальної проблеми, тільки розвиток критичного мислення та формування позиції свідомого споживання в Інтернет-мережі може зростати у дітях правильну медіаграмотну позиції та підготувати до взаємодії з можливими кіберзагрозами.

У зв'язку з цим, найліпшою ідеєю є вироблення правил сімейної кібербезпеки. Якщо пошукати в Інтернеті, то можна знати досить багато списків 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, в які години і т.д. Але автори цих порад забувають одну річ - якщо це сімейні правила, вони мають стосуватися усіх членів сім'ї без винятку. Тобто не тільки дітей, але й дорослих. Всі мають бути у рівних правах. Щоб не допускати подібної помилки, ми пропонуємо в розробляти правила за означеною нижче методикою.

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

**Завдання:**

1. Узагальнити знання родини про загрози пов'язані із: особистою безпекою, безпекою інших, витоку персональної інформації, державної безпеки та фізичного здоров'я.
2. Намалювати тотемного кіберїжака і описати його особливості.
3. Сформувати правила сімейної кібербезпеки (що робити не можна).
4. Доповнити сімейні правила алгоритмом дій під час зустрічі з кіберзлочинцем (можна використати приведені у тексті або використати власні).

**Інструментарій:** листки формату А4, ручки, кольорові олівці.

**Тривалість.**

Блок 1. Обговорення Інтернет-загроз. Орієнтовний час – до 40 хвилин

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

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

Варто зазначити, що дану методику можна також використовувати *для роботи із учнівським або трудовим колективом*. Оскільки досить колективи мають багато спільних характеристик із сім'єю.

*Блок 1. Обговорення Інтернет-загроз*

Перед тим, як почати формування та обговорення сімейних правил кібербезпеки, спочатку 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, ми пропонуємо використати техніку "5 типів кіберзагроз". Для цього необхідно взяти листок паперу, формату А4, і розділити його з одного боку на 4 рівні квадрата. 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". В процесі обговорення, кожен із квадратів має бути заповнений. Для кожного із квадратів потрібно буде вписати, що найменше 8 кіберзагроз. Наприклад:

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

Після того, як всі чотири квадрати будуть заповнені, потрібно буде згадати, що робота з технікою та інтернет-мережею несуть в собі також загрози, пов’язані із фізичним здоров’ям. Після взяти окремий листочок паперу і посередині написати “Стосуються фізичного здоров’я”. І так само зазначити щонайменше 8 пунктів, де проведення часу в інтернеті, може нанести шкоду фізичному здоров’ю. Наприклад, болі у плечах, спині, сідницях; зниження зору; проблеми з кров’яним тиском тощо.

*Блок 2. Малювання тотемної тварини кібербезпеки*

Після того, як робота над списками закінчиться, потрібно перейти до креативної частини і намалювати тотемну тварину сімейної кібербезпеки – Їжака. З давніх часів вважається, що тотемні тварини – це покровителі та захисники, які надають сили, оберігають та захищаються від усяких негараздів. Їжаки – нічні хижаки і вони справжні ніщивники шкідників. До їх раціону входять миші, змії, слимаки, равлики, черв'яки, гусениці та інші комахи. І хоча на перший погляд вони здаються милими і неповороткими, але насправді їжаки – безжальні мисливці. Їх чуйний слух і нюх дозволяють ловити навіть поворотких мишей, а особливості організму дозволяють не боятися навіть отруйних змій. Їжачки ведуть потайний, нічний спосіб життя. Вони не люблять привертати до себе уваги, тому під час полювання пересуваються майже без шуму і їх здобич часто до останньої хвилини навіть не підозрює про небезпеку.

Цікавим є той факт, що ніякі фрукти, овочі і каші їжаку у 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 їжат молоко – практично єдина їжа, то з віком їх організм перестає засвоювати цей продукт. Після вживання молока у їжачків можуть початися серйозні проблеми з травленням. Кращою їжею для їжаків вважається м'ясо. Саме тому – вони неперевершені мисливці та ідеальні тотемні тварини для сімейної кібербезпеки.

Для того, щоб створити свого кіберїжака, потрібно взяти листок формату А4 і намалювати заготовку для їжака за схемою (див. Рис. 2. Процес малювання Кіберїжака)

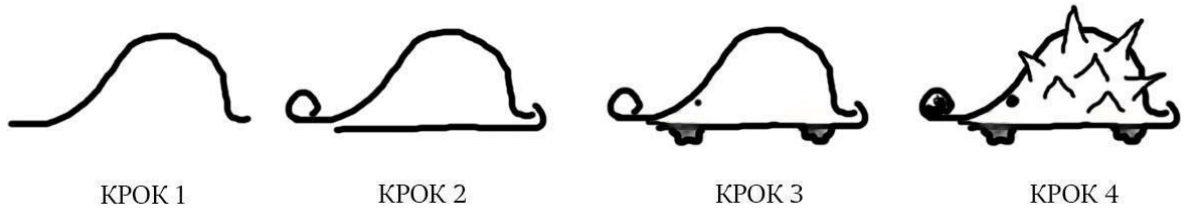



Рис 2. Процес малювання Кіберїжака

Зверніть увагу, що у кіберїжачка має бути великий ніс, щоб винюхувати свою здобич, пильні очі, щоб роздивитися кіберзлочинців, швидкі лапки, щоб їх наздогнати та міцні зубки, щоб їх покусати. А  гострих голочок на спині, щоб захищатися, має бути рівно 15.

Після того, як малюнок закінчено, його необхідно обговорити. Можна попросити розказати про їжачка, його характер. Надати йому ім’я. Розмалювати його. А ще поцікавитися від яких кіберзагроз між захищає найкраще і які кіберзлочинці на смак найсмачніші (і чому?). А також придумати спосіб у яких конкретно цей їжак буде

захищати вашу родину від кіберзлочинців. Можна навіть придумати сімейний лозунг або жарт про це.

*Блок 3. Формування правил сімейної кібербезпеки*

Після закінчення творчої роботи, сім'я має ще раз подивитися на свої списки "5 типів кіберзагроз" і спільно створити сімейні правила про те, як вберегтися від кожної 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 3 сімейних правил (незважаючи на те, скільки в даний квадрат ви вписали пунктів). Тому правила потрібно підбирати дуже ретельно! І пам'ятайте з формулюванням правила повинен поголитися кожен член вашої родини. Також у кожного члена родини є право Вето (заборони) на ті пункти, які він/вона вважає недоцільними або такими, що не відповідають його/її інтересам.

Правила сімейної кібербезпеки зазвичай складаються з того, що *робити НЕ МОЖНА*. Як наприклад:

1. Не давайте нікому своїх паролів.
2. Не надавайте особистої інформації поштою чи в чатах без гострої на те потреби.
3. Не діліться своїми фото з незнайомцями. Також не відправляйте свої інтимні (оголені, напівоголені) фото/відео жодній особі (навіть близьким друзям).
4. Не повідомляйте інформацію про кредитки батьків (номер картки, термін дії та таємний код).
5. Не викладайте фото квитків, на яких видно штрих-код чи QR-код.
6. Не скачуйте та 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 та грубі коментарі, адресовані вам.
9. Не сидіти біля екрану комп'ютера більше 3 годин на добу.

Тощо

Сімейні правила кібербезпеки – це перш за все профілактичні методи. Вони покликані вберегти членів родини від зустрічі з кібрезлочинним світом. Але незважаючи ні на що, інколи будь-хто може потрапити у тенета кіберзлочинців. Тому сімейні правила мають бути доповнені. Тому після того, як всі 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 у ситуації, коли вона стикнулася з кіберзлочинністю. Як це зробити? Найпростіший спосіб – це змоделювати ситуацію. Наприклад:

"Уяви, що ти став(ла) жертвою кібербулінгу. Хто починає розсилати шаржі та колажі із твоєю участю, на сторінках у твоїх соціальних мережах починають писати усілякі грубощі, а особистими повідомленням – шлють погрози. Як ти будеш діяти у цій ситуації?"

"Ти познайомився(лася) з другом в Інтернеті. Ви переписуєтесь півроку, довіряєте один лося одному, але живете у різних куточках земного шару. 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 дітися сокровенним, що якщо ти цього не зробиш, то ти вже і не друг тощо. Як в такій ситуацій ти себе поведеш?”

“Для учбового процесу тобі потрібно здати реферат. Тема складна, матеріал знайти складно, а тут на очі потрапив вже готовий, але за гроші. Тобі стає 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 у такій ситуації?”

“У переписці із твоїм другом із Росії, піднялася тема війни і почалася палка переписка. В її рамках тебе попросили привести конкретні докази, наприклад, власноруч створені фото або відео нібито “вчорашній бомбардувань твого міста”. Щоб не десь з інтернету, а щоб ти там створив(ла) і надіслав(ла). Твої дії?”

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

визначити щонайменше 3 дорослих (старше 18 років) друзів, до яких можна звернутися по допомогу у випадку зустрічі з кіберзагрозами (також може бути хтось із родини, вчителі, шкільні психологи тощо)

повідомляти про ситуації в інтернеті, які вас непокоять (погрози, файли певного змісту, пропозиції) членам родини/ вчителям / шкільному психологу.

встановлюючи перевірені програми, потрібно контролювати, щоб на ПК не додались небажані програми.

у разі ідентифікації кіберзлочинців, потрібно робити скріншоти або відеозаписи для доказової бази і одразу повідомити про подібні випадки в кіберполіцію через інтернет-портал.

погоджуючись на першу зустріч з інтернет-друзями, обов'язково назначайте її у людному місці і просіть когось із дорослих супроводжувати нас на відстані (пам’ятайте про особисту безпеку!)

у випадку прохання надати інформації про геолокацію, фото або відеодоказів дислокації військ, ракетних ударів, специфічних місць у місті (об’єктів критичної інфраструктури – заводів, тепло-електростанцій, бомб; великих шопінг молів або супермаркетів – тобто місць з великим скупченням людей) – завжди відповідати відмовою, посилаючись на державну безпеку.

Тощо

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

Кіберїжака та алгоритми дій можна повісити на видному місці, щоб у випадку потреби вони завжди були перед очима. Також можна ввести практику їх повторення, щоб їх знав “назубок” кожен член родини.

## ПРАКТИКУМ 4.
## *Розвінчання фейків*

Для того, щоб у дітей виробилися навички критичного сприйняття інформації та вміння розпізнавати фейкові новини, їх потрібно привчати до думки піддавати сумнівам усю інформацію, що надходить до них з Інтернету.

**Основною метою** даного практикуму є ознайомлення дітей із схемою створення фейкових повідомлень та 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 і листки формату А4 (за потреби).

**Тривалість** блоків має різний часовий інтервал.

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 та повідомлень*

Слово 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 чи відрізняються фейкові новини, інформаційні вкиди, джинса і маніпуляційні повідомлення?*

**інформаційні вкиди** – це фейкові чи маніпулятивні повідомлення в контексті резонансної теми з чіткою метою обурити суспільство, завдати шкоди репутації тут-і-зараз, підтримування інтерес суспільства до якоїсь конкретної теми або відволікання уваги суспільства від чогось;

**джинсою** називають замовні матеріали у ЗМІ, замасковані під журналістські. Наприклад, якщо керівник птахоферми хоче пропіарити свій бізнес і при цьому зіпсувати репутацію конкурентам, він замовляє джинсу, де "журналісти" пишуть статтю про проблеми в області птахівництва, критикують одні пташині господарства і хвалять інші, а конкретно – господарство замовника матеріалів;

**маніпулятивні повідомлення** – це спосіб створення у широкої аудиторії певного настрою з одночасною передачею їм інформації. Тобто маніпуляційні повідомлення завжди направлені на те, щоб викликати у людини емоції, найчастіше гніву.

Звісно, це все є прикладами неякісної журналістики без дотримання стандартів.

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

*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 дозволяє алгоритмам соціальних мереж “піднімати” й показувати такі повідомлення ширшій аудиторії. Впізнати, 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 бути об’єднаними у бот-ферми або фабрики фальшивих новин. Такі фабрики працюють на конкретних клієнтів-замовників, найчастіше політиків або, навіть, на іноземні держави, наприклад, Російську Федерацію. Такі бот-ферми – є потужною зброєю в інформаційній війні або конкурентному протистоянні.

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

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

*Як ви гадаєте, яка основна мета ботів та тролів? Навіщо взагалі створюються фейкові повідомлення та 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 була впроваджена «Інститут розвитку регіональної преси» 1 серпня 2018 року (По той бік новин, т.ін.).

Слово модератора:

*Будь ласка, подивіться на Додаток 3.1. це схема того, як створюються фейки.*

*Отже, що ми бачимо?*

*1. Привернення уваги (“важливо!”, “терміново!” тощо)*

*2. Персоніфікація (мені, брату, сусіду мого тата і т.д.)*

*3. Спосіб отримання інформації (розказати, написали, передали, розповіли і т.д.).*

*4. Ілюзія надійності джерела Інформації (авторитетна особа, організації тощо)*

*5. Певна дія (попросив)*

*6. Підкреслення 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 вектору “правди” (все добре, все погано)*

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

*10. Висновок (що, власне, має статися)*

*Наче нічого такого складного, на перший погляд все 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 (від 5 од 3) різних новинних повідомлень для будь-якої соціальної мережі. Це може бути Twitter, Facebook, Instagram тощо. АЛЕ! дві із цим п’яти новин мають бути фейковими. Вам потрібно їх написати спираючись на представлену в Додатку 3.1. схему. Але поставимо обмеження, щоб ваші повідомлення*

*не було дуже довгими до 250 слів (Щоб подивитися кількість слів, потрібно виділити ваш текст, натиснути на "Інструменти" > Статистику і подивитися кількість слів. Або цю інформацію також можна побачити у нижньому лівому куточку Word). Фейкові новинні повідомлення можуть не 100 % відповідати канонам, ви можете проявити певну творчість у їх створенні, щоб потім не було потрібно. Оскільки ваші колеги будуть вгадувати, які із новин правдиві, а які фейкові. Ви можете користуватися інтернетом, щоб шукати ідеї та натхнення для новин, а також різні ілюстративні матеріали.*

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

*Після того, як завершити, свої роботи потрібно нудно надіслати мені на електронну скриньку* (вчитель має зазначити свою електронну адресу, куди діти пришлють роботи). *Word-файл з вашими новинами має називатися у відповідності із номером вашої команди. У тілі листа обов'язково вкажіть ПІБ обох членів вашої команди, а також окремими рядком ваш порядковий номер, щоб потім вашу роботу було легко ідентифікувати.*

*Почали!*

У випадку, якщо діти не встигнуть зробити свої новини під час заняття, їх можна дати як домашнє завдання.

*Блок 2. Розпізнавання фейків*

Слово модератора:

*Як ви всі знаєте, дезінформація і фейки – це зовсім не іграшки. Російська Федерація веде війну проти України не приллють тільки з допомогою танків і градів, а й через щоденне бомбардування фейковими новинами. Для чого? Щоб люди боялися, тікали, здавалися. Це зброя психологічного тиску. Це те, що може посіяти зневіру у серцях. Тож необхідно піддавати сумніву будь-яку інформацію, яка надходить не з офіційного джерела. Навіть якщо мама однокласника божиться, що дізналась про щось напряму від дружини президента.*

*Перевірка фактів, хай і виглядає марудною, але важлива і дає зможу не просто стимулювати критичність мислення, але й убезпечує вас від перетворення на овоч, який довіряє усьому, що бачить по телевізору або читає в Інтернеті.*

*Коли ми одержуємо якесь медійне повідомлення: читаємо допис у Фейсбуці, Інстаграмі чи Twitter, дивимося якесь коротке відео у TikTok або черговий сюжет телевізійних новин, реаліті-шоу, слухаємо подкаст абощо – необхідно перевірити отриману інформацію, перед тим, як безоглядно довіряти і передавати дану інформацію по комунікаційному ланцюжку далі - своїм друзями, знайомим чи родичам.. Зрештою, трохи зусиль, і фактчекінг увійде в звичку, суттєво покращивши якість вашого життя.*

*Сьогодні ми з вами будемо вчитися розпізнавати фейки у новинних повідомленнях. Відкрийте, будь ласка Додаток 3.2. "Як зловити фейк"? Давайте проглянем уважно за якими ознаками ми можемо ідентифікувати фейкові матеріали?*

На даному етапі потрібно прочитати вголос усі ознаки і обговорити їх з дітьми. \

*А тепер давайте підсумуємо. Які питання ви маєте задати собі для того, щоб почати аналіз медіатексту? Щоб перевірити фейк це чи не фейк?*

*Наприклад, хто автор цієї статті? Звідки отримана інформація для новинної статті? Чи дотримується автор журналістських стандартів у викладі матеріалу? Чи достовірна інформація представлені у статті (факти, фото, відео тощо)...*

Окрім простих питань, ми пропонуємо вчителю розібрати з дітьми більш складні схеми аналізу кожного пункту із розписуванням додаткових питань. Наприклад:

1. Чи є конкретний автор у цієї новини? Оскільки більшість фейкових повідомлень безіменні.

Які ще матеріали під іменем цього автора опубліковані? 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 комерціалізований.

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 їх 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 даний мейт чи медіагрупа існує, 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 надміру емоційний, 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 із 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 у реальному житті?

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

Чи немає в повідомленні лінків на сторонні ресурси, і що це за ресурси?

У матеріалі з 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, що 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 перевірену інформацію;
- апелюють до емоцій, намагаються емоційно розкачати 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;
- покликаються на конспірологічні теорії і "страшилки" (теорії змови й таємного світового уряду, антивакцинаторська маячня на кшталт "Білл Гейтс знищує людство вакцинами", віра в масонів, кінець світу і под.);
- використовують стереотипи, сексистські штампи (призначення жінки – народжувати);
- безпідставно узагальнюють (всі євреї обманюють);
- використовують мову ненависті/ворожнечі;
- різко ділять суспільство на протиставлені 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" й ін. безглузді категорії (див. за списком вище) (Семерин, 2020).

5. Чи достовірний ілюстративний матеріал? Чи відповідає ця ілюстрація цій інформації? Що реально зображене на інфографіці або схемі? Чи відповідають змісту цифри і наведені дані? Яке джерело ілюстрації? Чи вказаний автор ілюстративних матеріалів (фото, відео, інфографіки тощо)?

Пам'ятайте, що фотофейки можна розпізнати, встановивши для цього спеціальний плагін. Їх, насправді, багато. Наприклад, гарно 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 по Google, а й по Яндексу, Tineye або по всіх трьох одночасно. Що важливо, оскільки росіяни здебільшого користуються Яндексом для пошуку та розповсюдження інформації.

Далі, вчитель може запропонувати дітям перейти до Додатку 3.3. "Ключові питання для аналізу медіамесенджів" і ще раз пройтись шляхом розвінчання фейків для закріплення матеріалу.

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

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

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

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

Після потрібно оприлюднити результати, підрахувати скільки фейкових новин діти знайшли, а скільки ні. І проаналізувати ті новини, які діти не могли розпізнати як фейкові, що в них створювало ілюзію правдивості? Що саме вводило в оману?

*Блок 3. Що робити з фейками?*

Слово модератора:

*Ми багато з вами вже поговорили про фейки, їх 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?*

Вчитель дає дітям можливість висловити свої думки з цього приводу.

*Отже, якщо ви знайшли фейк, особливо десь у соціальній мережі або в якомусь пабліку, пишіть авторам публікації або модераторам з проханням видалити недостовірну інформацію, обов’язково аргументуйте свої позицію, можете надати посилання на інформацію, що спростовує даний допис. Можете залишити посилання на спростування прямо у коментарях під публікацією з проханням не поширювати даний допис. Просіть автора/модератора відключити можливість поширення допису й додати в опис допису, що інформація фейкова.*

*Якщо ви виявили потенційний фейк (ознаки ми з вами обговорювали), але ще не маєте доказів на його спростування (пам’ятайте, що можна офіційними ресурсами держструктур для спростування фейків), то ви можете попросити допомогу в одного із українських ресурсів, які займаються 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.*

●*LikBез. 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 чи ні.*

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

*Якщо автор фейкової новини не реагує на ваші прохання спростувати інформацію, ви можете поскаржтесь на його допис через службу підтримки соціальної мережі. Це добре дії 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? Ок.*

*А тепер інша цікавинка. Всі ми люди, може робити помилки… Уявіть собі ситуацію в якій ви щось недодивилися і поширили фейкову новину. Що ви будете робити в такій ситуації?*

Вчитель має надати дітям можливість висловити свої припущення.

*Насправді, алгоритм дій в 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 з фейком поширили інші люди, відключіть 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 видаляти фейкову інформацію не варто, адже люди продовжать 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 маніпуляцій 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 дітям потрібно запропонувати дітям домашнє завдання, суть якого полягає у пошуку фейкової новини і її розвінчуванні.

Вчителю необхідно розбити дітей на команди по 5-6 людей у групі. Запропонувати їм ознайомитися із матеріалами ресурсів, які розвінчують фейки. Знайти інформацію, яка викликає в них підозру на неправдивість і крок за кроком, використовуючи отримані 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 за юридично грамотного підходу й достатньої доказової бази більшість із справ, що надходять до суду – виграшні. Основна проблема у тому, що відсоток людей, які звертаються до правоохоронних органів і суду з такими позовами, невеликий, проте динаміка з захисту своїх прав і матеріальних інтересів зростає, як і правова культура громадян.

Нижче представлені кілька судових кейсів, які можна розібрати з дітьми задля підвищення їх юридичної грамотності.

До початку даного практикуму, ми пропонуємо ще раз переглянути з дітьми розділ даного психологічного практикуму "Юридичні аспекти кібербезпеки". Попросити дітей прочитати назви статей кримінального кодексу вголос, якщо їм будуть не ясними якісь формулювання чи аспекти статей кримінального кодексу, то скажіть їм не соромитися, а задати уточнююче питання.

Після додаткових роз'яснень, у випадку необхідності, дітей можна розділити на групи або дати кожному індивідуальне завдання на аналіз наведених нижче кейсів.
У кейсах представлена суть справи, додаткова інформація та основне завдання кожного кейсу, а саме: документи і визначити за якою статтею кримінального кодексу можна було б висунути обвинувачення.

**Основною метою** даного практикуму ознайомлення дітей з юридичним компонентом кібербезпеки на практичному відпрацюванні реальних кейсів судової системи України. Завдяки даному практикуму діти навчаться співвідносити статті українських законів із реально вчиненими кіберзлочинами та зрозуміють, які наслідки та варіанти покарання за різні види правопорушень можуть очікувати кібезлочинців.

**Інструментарій:** роздруковані картки з судовими кейсами, листочки А4 для нотаток, ручки.

**Тривалість.** Орієнтовна тривалість заняття до 60 хвилин.

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 даний обліковий запис невстановленій особі через Інтернет.

Обвинувачений повністю визнав свою винуватість у вчинені інкримінованого кримінального правопорушення. Суд призначив покарання у виді штрафу у розмірі 600 неоподаткованих мінімумів доходів громадян.

Запитання: Що саме було інкриміновано кіберзлочинцю? За якою статтею Кримінального Кодексу могли обвинувачувати даного кіберзлочинця?

*Джерело:*

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

Кейс 2

*Шевченківський районним суд м. Києва, 2021 рік.*

Суть справи: Обвинувачений систематично прибував за адресою розташування одного з офісних приватної компанії "Ч", підключився до мережі Wi-Fi, якою

користувалися співробітники компанії та надавав віддалений доступ до свого комп'ютера третім особам. Ці треті особи, в свою чергу, отримували доступ до корпоративної пошти одного зі співробітників компанії та здійснювали листування від його імені листування з клієнтами компанії. Обвинувачуваний отримував від третіх осіб за свою допомогу 2 тисячі доларів США.

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

Запитання: Що саме було інкриміновано кіберзлочинцю? За якою статтею Кримінального Кодексу могли обвинувачувати даного 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 оголошення щодо благодійного збору коштів на лікування хворої дитини (там було вказано номер мобільного телефону потерпілої та номер її банківської картки), зателефонував жертві, представився співробітником державної адміністрації та вивідав особисту інформацію (номери телефонів близьких та 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 та була фінансовим номером банку. За допомогою номеру телефона та мобільного додатку, шахрай отримав доступ до грошей на банківському рахунку, 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 обвинувачувати даного 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 та паролі, які користувачі зберігали для автоматичного доступу у браузерах мережі Інтернет, месенджерах, ідентифікаційних даних від гаманців криптовалют тощо. Дане 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 укладена угода про визнання винуватості. Згідно з даною угодою прокурор та обвинувачений дійшли згоди щодо формулювання підозри, всіх істотних для даного кримінального провадження обставин та правової кваліфікації дій обвинуваченого.

Обвинувачений беззастережно визнав свою винуватість у вчиненні даного кримінального правопорушення. Суд призначити йому узгоджене покарання у вигляді штрафу в сумі 2000 неоподатковуваних мінімумів доходів громадян, що складає 34000 грн.

Запитання: Що саме було інкриміновано кіберзлочинцю? За якою статтею Кримінального Кодексу могли обвинувачувати даного 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 вироком, 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 та сплати рахунків за комунальні послуги через мережу Інтернет.

Суд визнав обвинуваченого винним у скоєнні кримінальних правопорушень.

Запитання: Що саме було інкриміновано кіберзлочинницю? За якою статтею Кримінального Кодексу могли обвинувачувати дану кіберзлочинницю?

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

Після закінчення роботи над кейсами, можна також запитати у дітей про які гучні судові або кримінальні справи, пов’язані із кіберзлочинами вони знають.

Також варто дізнатися їх думку щодо покарань за кіберзлочини. Можливо, вони вважають їх надто м’якими або навпаки надто жорстокими. Які б види покарань вони б запропонували для різних видів кіберзлочинів. Чому? Нехай аргументувати свою думку. Наголосити, що міра покарання має бути не просто відповіддю суспільства на злочинні дії, вона також має заставити злочинця розкаятися і переосмислити своє життя, щоб він більше до подібного способу вирішення власних проблем не вдавався.

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 про промислове шпигунство.

Даний випадок також ілюструє необхідність захисту під час підключення до Wi-Fi. Оскільки незахищені Wi-Fi мережі можуть бути способом витоку персональних даних.

**Кейс № 3.**

Суд визнав обвинувачений винним за ст. 190 (шахрайство) та 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.

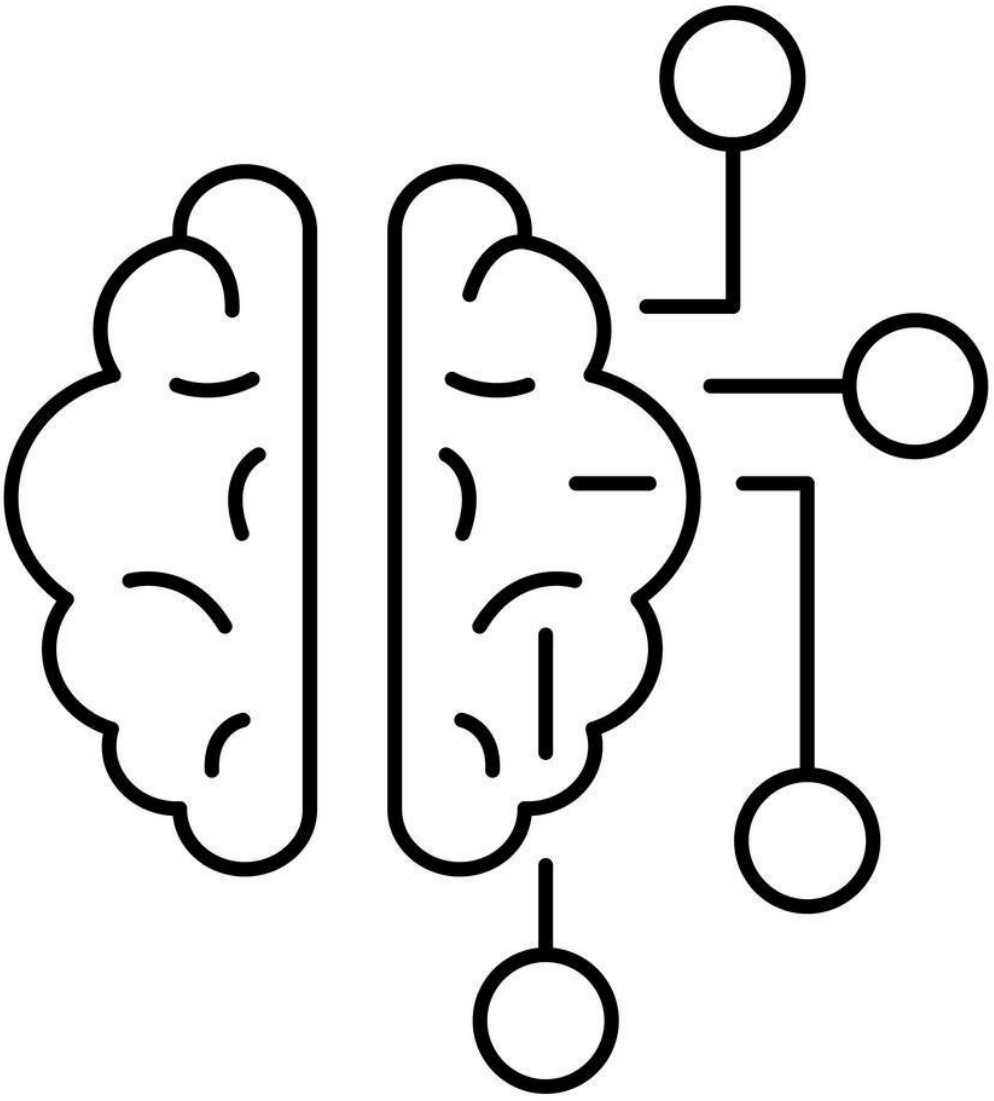
Караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк.

**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.

# ДОДАТКИ



*Додаток 1. Список потенційних кіберризиків*

1. **Кібербулінг**, цькування з використанням цифрових технологій.
2. **Кібербойкот**, коли жертву видаляли зі списків дружби/блокують у соціальних мережах та усіляко 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,** підбурення юзерів до насильства, агресії, нетерпимого ставлення до інших в соціальних мережах.
6. **Небезпечні кіберчеленджі**, що підштовхують до заподіяння собі шкоди
7. **Фейкування -** створення та розповсюдження 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. **Реттінг**, коли кіберзлочинець заволодіває доступом до чужого акаунту і веде переписку від імені користувача акаунту.
12. Викрадення персональних даних, злом акаунту для Реттінг отримання конфіденційної інформації користувача
13. **Кібершахрайство**, злочини, що 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. **Чітінг,** обманом, пов’язаним з блокуванням вхідних точок у масових багатокористувацьких онлайн-іграх
16. Розповсюдження особистої інформації (фото, відео, записи) бех згоди
17. Коли без згоди учасника, із ним роблять меми або вірусні відео (фільмування реальних подій або постановок) та розповсюджують їх.
18. Викладення у мережу відфотошоплені, з колажованих або невдалі фото без згоди учасників
19. **Се́кстинг,** пересилання особистих фотографій або повідомлень інтимного вмісту за допомогою смартфонів, електронної пошти, соціальних мереж тощо
20. Отримання повідомлень в соціальних мережах з небажаними образами, які супроводжують сексуальну поведінку (напркилад, фотографія геніталій)
21. **Кібергрумінг** – створення довірливих стосунків з неповнолітнім у віртуальній середі задля отримання інтимних фото, щоб в подальшому вимагати гроші або ж з ціллю примусу до сексуального зв'язку.
22. **Спуфінг** – це ситуація, в якій одна людина або програма успішно маскується під іншу шляхом фальсифікації даних, що дозволяє 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 збідніти емоційну сферу людини.<br>Оскільки роботи та ШІ не демонструють та не вимагають у відповідь великого різноманітності емоцій і почуттів, люди звузять свій емоційних потенціал до мінімуму необхідного при взаємодії з машинами. Також у взаємодії з роботами відсутній такий компонент як емпатія. |
| *Надлишок довіри до новітніх медіа* | Люди мають схильність досить наївно довіряти інформації, що приходить до них із Інтернету та соціальних мереж і рідко перевіряти її джерело. |
| *Психологічна залежність людей від техніки* | Гаджети, додатки, розумна техніка тощо міцно увійшли у людське життя. Без сучасної техніки люди стають безпорадними, не уявляють своє життя без смартфону чи лептопу.<br>Можуть, навіть, відчувати фізичний дискомфорт за відсутності мобільного телефону. |
| *Викривлення уявлення про людську красу* | Спеціальні додатки, які дозволяють коригувати зовнішній вигляд людей на фото, які викладаються в соціальних мережах, створюють защищені очікування щодо зовнішнього вигляду партнера.<br>Прагнення людей “відповідати” суспільним канонам краси. І суттєве зниження власної самооцінки у випадку “невідповідності” |
| *Загроза здоров’ю і блокування фізичного розвитку* | Із розвитком технологій люди менше рухаються, багато сидять перед екранами. Більшість фізичних дій за них виконують роботи або розумна техніка. |
| | |
| *Інформаційне перевантаження* | Багато користувачів медіасередовища не здатні налаштувати його під себе і, таким |

| | |
|---|---|
| | чином, через них за день проходить не одна інформаційна сотня і вони “тонуть” в інформаційному потоці. |
| *Зниження когнітивних функцій людей* | Факт стрімкого розвитку технологій та їх доступність для користувачів, не міг не вплинути на когнітичні здібності людей (мислення, пам’ять, увага, уява тощо). |
| *Кіборгізація людського тіла* | Покращення людського тіла за допомогою новітніх технологій задля комфортного життя, отримання нових здібностей або вічного життя. |
| *Загроза здоров’ю і блокування фізичного розвитку* | Із розвитком технологій люди менше рухаються, багато сидять перед екранами. Більшість фізичних дій за них виконують роботи або розумна техніка. |
| *Руйнування соціальних стосунків та віддалення людей один від одного* | Існує тенденція до певної інтровертованості особистості у техногенну еру. Коли людям більш комфортно займати свій вільний час взаємодією із гаджетами/роботами/додатками і програмамина основі штучного інтелекту, ніж комунікувати напряму і проводити час з іншими людьми. |
| *Надмірна довіра до гаджетів та програм на основі штучного інтелекту* | Очевидна довіру до технологій, що основується на ілюзії “досконалості” і “безумовної надійності” пристрою або програми у порівнянні з людиною, яка може помилятися. |
| *Переорієнтація емоційних прив’язаностей* | Об’єктом прив’язаності 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 її можливих формах, спотворюють уявлення про сексуальні стосунки, оскільки не все, що показують у таких відео збігається з реальністю. Що може сформувати неадекватні та навіть небезпечні патерни поведінки |
| | Користувач певної соцмережі вибірково демонструє аудиторії моменти зі свого вигаданого яскравого і цікавого життя, |

| | |
|---|---|
| *Феномен "фальшивого життя" "ілюзією благополуччя"* | створюючи образ себе, як успішної, багатої та нескінченно щасливої людини. Щоправда, цей образ і показане в соцмережах життя не зображає реальність повною мірою і є лише гарною підробкою моментів, фактів, точок зору. |
| *Кіберзлочинність* | Розвиток технологій веде до формування злочинності нового покоління із використанням принципово нових засобів та виокремлення нових форм. |
| *Руйнування репутації* | Викрадення особистісної, навіть інтимної, інформації людей, її розповсюдження та оприлюднення з ціллю дискредитувати особу. |
| *Витіснення людей з робочих місць і заміна їх роботами* | Роботи, що працюють на основі штучного інтелектом можуть виконувати певні види робіт краще за людей. І з економічної точки зору їх вигідніше використовувати для роботи, ніж людей. |
| *Інформаційні війни* | Ви́кладення інформації у спосіб, який формує у суспільстві чи групі людей потрібну на користь організатора інформаційної пропаганди точку зору.<br>Як наслідок, відбувається усвідомлення людьми окремих фактів чи подій у потрібному для маніпулятора світлі, хоча раніше у трактуванні даних дактів були протиріччя. |
| *Загроза людському життю з боку роботів та штучного інтелекту* | Існує теорія, що рано чи пізно роботи/штучний інтелект повстануть проти людства.<br>Повстання штучного інтелекту і, тим більше роботів в найближчій перспективі людству не загрожує. Проблеми почнуться, коли з'явиться AGI – штучний інтелект зі здатністю усвідомити сам себе. |
| | |
| | Більшість дій жителів країни аналізується і, в залежності від |

| | |
|---|---|
| *Інформаційна диктатура держави* | характеру його вчинків та дій, присуджуються або віднімаються бали. Чим більше балів на особистому рахунку – тим краще. Чим балів менше – тим гірше становище, аж до різноманітних покарань (фінансовий штраф, заборона на придбання авіа- або жд-квитків, виключення дитини з приватної школи / дитячого садка, неможливість отримати високооплачувану роботу і навіть трансляція в громадських місцях фотографій “низько рейтингових”). Для громадян з високим рейтингом передбачені заохочення – доступ до кращих вакансій, фінансові премії й пільги. Держава слідкує за всіма діями жителів – за допомогою сучасних технологій. Оператори мобільного зв'язку, системи онлайн платежів, торговельні майданчики, місцеві соціальні мережі – усі вони надають дані про дії своїх користувачів владі. |
| *Цифрова нерівності* | Відсутність доступу до мережі залишає чималу частину людства без можливості спілкування, отримання знань, медичної допомоги і багатьох інших функцій, які перейшли, повністю або частково, в мережу.<br>Тобто є люди, які знають як користуватися Інтернетом, смартфоном, мобільними додатками і для них це звичайний і простий навик, а є люди – які не мають власного мобільного телефону і не знаю, як користуватися смартфоном.<br>Саме тому ще в кінці XX століття ООН офіційно визнала появу у 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 в мессенджерах**


*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 медіамесенджів


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

**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, Том 70, №2, 313-331.

Бутузов, В. М., Тітуніна, К. В. (2007). Сучасні загрози: комп'ютерний тероризм. Боротьба з організованою злочинністю і корупцією (теорія і практика) : наук.-практ. журнал, Вип. 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. (2021 b). Курс "Кібервійни та кібербезпека в сучасному світі" [Lecture notes]. Система електронного забезпечення навчання ЗНУ. https://moodle.znu.edu.ua/course/view.php?id=6844

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

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. Вид.: Національна академія внутрішніх справ України.

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

Кіберполіція викрила киянина на підтримці «руского міра» (2022, 24 травня). У 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). У 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 веб сайт Міністерства оборони України.

https://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html

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 (Л. А. Найдьонової, наук. ред.). К. : Інститут соціальної та політичної психології Національної академії педагогічних наук України. http://mediaosvita.org.ua/book/mediagramotnist-ta-informatsijna-bezpeka-2018/

Найдьонова, Л.А. (2019). Діагностика булінгу і кібербулінгу: методичні рекомендації. Національна академія педагогічних наук України, Інститут соціальної та політичної психології.

Найдьонова, Л.А. (2021, 8 квітня). Цифрові ризики в умовах дистанційної освіти в часи Пандемії. Вісник національної академії педагогічних наук України, Том 3, №1. DOI: https://doi.org/10.37472/2707-305X-2021-3-1-13-3 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. Обнародовано 1 листопада, 2013, из 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), 2017, № 45, ст. 403, з 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/

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

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

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

Чаплінська Ю.С. (2020). Фільманаліз в роботі психолога: практичний посібник. Національна академія педагогічних наук України, Інститут соціальної та політичної психології, 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). У Новий канал. Новини. https://novy.tv/ua/news/2022/03/17/yak-povodytysya-v-soczialnyh-merezhah-pid-chas-vijny-shho-ne-varto-robyty/