ПРЯМУЄМО РАЗОМ

ПРОЕКТ ФІНАНСУЄТЬСЯ ЄВРОПЕЙСЬКИМ СОЮЗОМ

ПОЛІЦІЯ

БЛАГОПОЛУЧЧЯ ДІТЕЙ УКРАЇНСЬКИЙ ФОНД

ВОЛОНТЕР Всеукраїнський громадський центр

LHSI Соціальні ініціативи з охорони праці та здоров'я

ПІДГОТОВКА ПОЛІЦЕЙСЬКИХ ПІДРОЗДІЛІВ ПРЕВЕНТИВНОЇ ДІЯЛЬНОСТІ, СЛІДСТВА ТА ДІЗНАННЯ, КІБЕРПОЛІЦЕЙСЬКИХ З ПИТАНЬ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДІТЕЙ У КІБЕРПРОСТОРІ

навчально-методичний посібник

ПІДГОТОВКА ПОЛІЦЕЙСЬКИХ ПІДРОЗДІЛІВ ПРЕВЕНТИВНОЇ ДІЯЛЬНОСТІ, СЛІДСТВА ТА ДІЗНАННЯ, КІБЕРПОЛІЦЕЙСЬКИХ З ПИТАНЬ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДІТЕЙ У КІБЕРПРОСТОРІ

НАВЧАЛЬНО-МЕТОДИЧНИЙ ПОСІБНИК

Київ – 2024

УДК 351.74+004.946.5.056(075)(477)

ISBN 978-617-8197-23-0

Рекомендовано до друку рішенням Вченої ради Одеського державного університету внутрішніх справ (протокол №5 від 25 листопада 2024 року).

Підготовка поліцейських підрозділів превентивної діяльності, слідства та дізнання, кіберполіцейських з питань забезпечення безпеки дітей у кіберпросторі: навчально-методичний посібник / за заг. ред. Журавель Т.В., Ковальової О.В. Видавництво ФОП Буря О.Д. – Київ, 2024. 360 с.

Авторський колектив:

Апетик Анастасія Миколаївна, юристка, незалежна консультантка з цифрової безпеки, керівниця Apetyk consult, членкиня правління, керівниця з стратегічного розвитку ГО «Мін3мін» (Тема 1.1, Тема 1.5).

Дьякова Анастасія Дмитрівна, голова правління #stop_sextинг (Тема 1.1, Тема 1.3, Тема 2.1.3).

Ковальова Олена Володимирівна, кандидатка юридичних наук, старша наукова співробітниця, доцентка, професорка кафедри адміністративної діяльності поліції Одеського державного університету внутрішніх справ (Тема 1.7, Тема 1.9, Тема 1.10, Тема 1.12, Тема 2.1.3, Тема 2.1.4).

Козлова Анна Георгіївна, докторка філософії у галузі психології; доцентка кафедри психології та педагогіки професійної освіти факультету лінгвістики та соціальних комунікацій Національного авіаційного університету (Тема 1.11).

Манжай Олександр Володимирович, кандидат юридичних наук, професор, підполковник поліції, завідувач кафедри протидії кіберзлочинності ННІ №4 Харківського національного університету внутрішніх справ (Тема 1.4, Тема 1.6, Тема 1.8, Тема 2.1.1, Тема 2.2.1, Тема 2.3.1, Тема 2.3.2).

Мердова Ольга Миколаївна, кандидатка юридичних наук, доцентка, завідувачка кафедри адміністративно-правових дисциплін факультету №2 Донецького державного університету внутрішніх справ (Тема 1.1, Тема 1.2, Тема 2.1.2.).

Мілорадова Наталія Едуардівна, докторка психологічних наук, професорка кафедри педагогіки та психології ННІ №3 Харківського національного університету внутрішніх справ (Тема 1.1, Тема 1.2, Тема 1.3, Тема 1.11, Тема 2.1.2.).

Пашко Наталія Олександрівна, психологиня, психотерапевтка, координаторка по роботі з дітьми та підлітками ГО «Інститут психології здоров'я», модераторка дивізіону ювенальної психології (Тема 1.3, Тема 1.11).

Юртаєва Ксенія Володимирівна, кандидатка юридичних наук, доцентка, LL.M, доцентка кафедри кримінального права і кримінології ННІ №1 Харківського національного університету внутрішніх справ (Тема 2.2.2).

Філоненко Василь Іванович, тренер-методолог Громадської організації #stop_sextинг (Тема 1.1, Тема 1.2, Тема 2.1.3).

Рецензенти:

Богдан Василь Володимирович, начальник управління ювенальної превенції Департаменту превентивної діяльності Національної поліції України, полковник поліції.

Вітвіцький Руслан Олегович, т.в.о. заступника начальника 4-го відділу 1-го управління Департаменту кіберполіції Національної поліції України, майор поліції.

Корнієнко Максим Вікторович, проректор Одеського державного університету внутрішніх справ, д.ю.н., професор, полковник поліції.

Загальна редакція:

Журавель Тетяна Василівна, кандидатка педагогічних наук, виконавча директорка Громадської організації «Всеукраїнський громадський центр "Волонтер"».

Ковальова Олена Володимирівна, кандидатка юридичних наук, старша наукова співробітинця, доцентка, професорка кафедри адміністративної діяльності поліції Одеського державного університету внутрішніх справ.

Координація розроблення програми:

Янковець Вікторія Вікторівна, магістерка соціальної роботи, координаторка проєктів Громадської організації «Всеукраїнський громадський центр "Волонтер"».

Навчально-методичний посібник призначений для викладачів, які здійснюють професійне навчання поліцейських, та спрямований на посилення навчально-методичного інструментарію підготовки поліцейських підрозділів превентивної діяльності, слідства та дізнання, кіберполіцейських з питань забезпечення безпеки дітей у кіберпросторі. Навчально-методичний посібник може використовуватись для проведення навчальних занять під час первинної професійної підготовки поліцейських, підготовки у закладах вищої освіти зі специфічними умовами навчання, післядипломної освіти та службової підготовки поліцейських.

Навчально-методичний посібник підготовано за фінансової підтримки Європейського Союзу. Його зміст є виключною відповідальністю ГО «Всеукраїнський громадський центр «Волонтер» і не обов'язково відображає позицію Європейського Союзу.

ЗМІСТ

ПЕРЕДМОВА

Забезпечення безпеки дітей є одним із пріоритетних завдань держави. В умовах стрімкого цифрового розвитку виникають нові виклики та загрози благополуччю дітей, що вимагає пошуку ефективних інструментів для їх подолання та впровадження комплексного підходу до забезпечення безпеки дітей в кіберпросторі.

Комплексний підхід включає, зокрема, належний рівень підготовки фахівців суб'єктів, до компетенції яких входить запобігання та реагування на загрози безпеці дітей в кіберпросторі. Особливе місце серед суб'єктів належить органам Національної поліції України, зокрема підрозділам превентивної діяльності, слідства та дізнання, кіберполіцейським. Від їх професійності, небайдужості та неупередженості залежить своєчасне виявлення загроз для безпеки дітей в кіберпросторі, оперативне припинення їх негативного впливу, надання ефективної допомоги постраждалим дітям, а також забезпечення невідворотності притягнення правопорушників до відповідальності. Тому питанням підготовки поліцейських з питань забезпечення безпеки дітей у кіберпросторі слід приділяти належну увагу. Ефективність підготовки фахівців безпосередньо залежить від якості навчально-методичного забезпечення.

Навчально-методичний посібник «Підготовка поліцейських підрозділів превентивної діяльності, слідства та дізнання, кіберполіцейських з питань забезпечення безпеки дітей у кіберпросторі» складається з загальної та особливої частин, які представлені у вигляді тренінгових занять. Викладання тем у межах загальної частини посібника передбачені для підготовки працівників різних структурних підрозділів Національної поліції України та окреслюють питання щодо безпеки дітей у мережі та викликів, зокрема під час воєнного стану; онлайн-ризиків та небезпек, з якими стикаються діти; базові правила та підходи до цифрової безпеки; систему захисту прав дітей та взаємодію підрозділів поліції під час реагування на випадки онлайн-насильства над дітьми, а також убезпечення дітей від насильства у кіберпросторі. Теми, запропоновані для вивчення у межах особливої частини, передбачені для підготовки окремих категорій поліцейських (превентивної діяльності, органів досудового розслідування та кіберполіції) у контексті безпеки дітей в мережі інтернет та у межах їхньої компетенції. Усі запропоновані теми у посібнику можуть обиратися для викладання з урахуваннями наявних у поліцейських знань та досвіду з проблематики та можуть бути диференційовано використані як в межах первинної професійної підготовки, так і підготовки в закладах вищої освіти зі специфічними умовами навчання, які здійснюють підготовку поліцейських, службової підготовки та підвищення кваліфікації. Перед проведенням занять, викладачам доцільно перевірити актуальність посилань і джерел, особливо з питань правового забезпечення, та у разі необхідності, внести відповідні зміни та доповнення.

Вказаний у посібнику час на виконання вправ є орієнтовним і може змінюватись в залежності від динаміки групи. Наприкінці кожного заняття зазначені тестові питання, які можна використовувати для контролю знань здобувачів освіти як перед проведенням заняття, так і після нього.

Упродовж серпня 2023 по лютий 2024 років дана програма була апробована з здобувачами освіти, слухачами первинної підготовки, курсів підвищення кваліфікації та поліцейських в рамках службової підготовки за участю викладачів-тренерів у 6 закладах вищої освіти зі специфічними умовами навчання, які здійснюють підготовку поліцейських (Дніпровський державний університет внутрішніх справ, Донецький державний університет внутрішніх справ, Львівський державний університет внутрішніх справ, Національна академія внутрішніх справ, Одеський державний університет внутрішніх справ, Харківський національний університет внутрішніх справ). Результати апробації програми довели її актуальність та практичний інтерес як зі сторони здобувачів освіти, так і зі сторони викладацького колективу. Програма є гнучкою, адаптивною у застосуванні форм та методів роботи, способів взаємодії із аудиторією.

Будемо вдячні за відгуки та пропозиції, які з'являться у користувачів програми за результатами її проведення, та запрошуємо надсилати їх на адресу: aupc.volunteer@gmail.com

З повагою,
колектив авторів.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЄС – Європейський Союз

ЗКТ – засоби комп'ютерної техніки

ІКТ – інформаційно-комунікаційні технології

ІПСО – інформаційні психологічні спеціальні операції

ККУ – Кримінальний кодекс України

КМЄС – Консультативна місія Європейського союзу

КУпАП – Кодекс України про адміністративні правопорушення

ICSE – Міжнародна база даних Інтерполу щодо матеріалів сексуальної експлуатації дітей

INHOPE – міжнародна мережа «гарячих ліній» для повідомлень про матеріали сексуального насильства та сексуальної експлуатації щодо дітей онлайн

ITU – Міжнародний союз електрозв'язку

IVR – система голосових меню/інтерактивна голосова відповідь

CSAM – матеріали, пов'язані з сексуальним насильстовм щодо дітей

CSEM – матеріали, пов'язані з сексуальною експлуатацією дітей

UNICEF – агентство ООН у справах дітей

ГЛОСАРІЙ

Дитяча порнографія – зображення у будь-який спосіб дитини чи особи, яка виглядає як дитина, у реальному чи змодельованому відверто сексуальному образі або задіяної у реальній чи змодельованій відверто сексуальній поведінці, або будь-яке зображення статевих органів дитини в сексуальних цілях.

«Зелена кімната» – методика, яка полягає в отриманні достовірних свідчень дитини в умовах мінімізації та недопущення повторного її травмування.

Інформаційна бульбашка – явище, яке обмежує доступ користувача до повного спектру новин та іншої інформації в інтернеті шляхом алгоритмічного визначення пріоритетів вмісту, що відповідає демографічному профілю користувача та онлайн-історії, або виключаючи вміст, який йому не відповідає.

Інформаційно-телекомунікаційні системи – сукупність інформаційних та електронних комунікаційних систем, які використовують технологію обробки інформації з використанням технічних і програмних засобів.

Кібербулінг (цькування) – психологічне, фізичне, економічне чи сексуальне насильство, тобто будь-яке умисне діяння (дія або бездіяльність) із застосуванням засобів електронних комунікацій, яке систематично вчиняється особою стосовно дитини, з якою вони є учасниками одного колективу, або дитиною стосовно іншого учасника одного колективу та яке порушує права, свободи, законні інтереси потерпілої особи та/або перешкоджає виконанню нею визначених законодавством обов'язків.

Кібергігієна – дотримання правил безпечної поведінки у кіберпросторі.

Кіберсталкінг – дії зловмисника, які спрямовані на постійне спостереження та привертання уваги через соціальні мережі, дзвінки (як на мобільний телефон, так і у месенджерах), докучання та переслідування онлайн.

Медіаграмотність – навички та знання, які надають користувачам можливість ефективно і безпечно користуватися медіа-сервісами.

Неналежний контент – перегляд контенту, що не відповідає віковим обмеженням.

Онлайн-грумінг – формування дорослим або групою дорослих довірливих стосунків з дитиною з метою сексуального насильства онлайн чи у реальному житті.

Ошуканство, видурювання конфіденційної інформації та її розповсюдження (outing & trickery) – отримання персональної інформації в міжособовій комунікації й передача її (текстів, фото, відео) в публічну зону інтернету або поштою тим, кому вона не призначалась.

Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Профілактика – комплекс заходів, спрямованих на запобігання будь-яким негативним явищам та/або усунення факторів ризику.

Секстинг – пересилання особистих фотографій, повідомлень інтимного змісту.

Секторшен – налагодження незнайомцями довірливих стосунків в інтернеті з дитиною з метою отримання приватних матеріалів, інтимних фото або відео, шантажування ними та вимагання грошей чи додаткових матеріалів.

Соціальна інженерія – психологічна маніпуляція, яка передує заволодінню персональними даними та використовується у більшості атак.

Тролінг – розміщення провокативних повідомлень з метою спричинення конфлікту або цькування особи.

Фішинг – одна з форм шахрайства, що проявляється у вигляді певних різновидів атак з використанням соціальної інженерії, який часто використовується для крадіжки персональних даних користувачів, зокрема даних для входу в облікові записи та номерів кредитних карток, для подальшого їх використання із злочинною метою.

Хепі-слепінг – створення насильницького контенту та його розміщення в інтернеті заради розваг.

Хеш – унікальний цифровий відбиток, що властивий цифровим файлам, зокрема тим, які представляють матеріали сексуального насильства над дітьми.

Шкідливий контент – створення та поширення інформації, яка може зашкодити дитині (наприклад фото/відео з місця катастроф, катування військовополонених тощо).

І. ЗАГАЛЬНА ЧАСТИНА

ТЕМА 1.1. Безпека дітей в мережі інтернет: актуальність, виклики, сучасний стан

Заняття 1.1.1. Актуальність забезпечення безпеки дітей: можливості та ризики в мережі інтернет

Мета: оцінити рівень поінформованості учасників щодо безпеки дітей у мережі інтернет, сформувати спільне розуміння актуальності зазначеної проблеми.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Вступ до тематики	Інформаційне повідомлення	5 хв	
2.	Безпека в інтернеті – це… Небезпека в інтернеті – це…	Мозковий штурм	15 хв	Фліпчарт, маркери
3.	Інтернет в моєму житті та в житті дитини	Групова робота	40 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери
4.	Небезпечна мережа	Інтерактивна вправа	30 хв	Аркуші паперу для фліпчарту, маркери, Додаток 1.1.1

ХІД ЗАНЯТТЯ

1. Інформаційне повідомлення «Вступ до тематики»

Мета: надати учасникам інформацію щодо актуальності розгляду питання стосовно безпеки дітей у мережі інтернет.

Час: 5 хв.

Хід проведення:

Тренер/тренерка звертається до учасників:

«Цифрове середовище, зокрема мережа інтернет, сьогодні є не лише важливим джерелом інформації, але і способом комунікації, який нівелює перепони для спілкування. Через військову агресію росії проти України багато людей проводять дедалі більше часу в інтернеті. Україна перебуває на етапі швидкого технологічного розвитку, де комп'ютерна грамотність стає невід'ємним компонентом загальної освіти і показником освіченості. Глобальна інформаційна мережа інтернет стає важливою частиною повсякденного життя сучасних людей. Інтернет несе в собі великий інформаційний та освітній потенціал і є засобом гармонійного розвитку, проте водночас містить і певні ризики. Сучасне покоління дітей народжується та зростає в умовах швидкого розвитку цифрових технологій і цифрової трансформації багатьох галузей. Ці зміни молодь сприймає як звичні явища, це їхній природний світ, в якому вони легко орієнтуються й сприймають нові формати взаємодії. З появою та розвитком всесвітньої мережі інтернет виникли нові способи вчинення злочинів, зокрема доведення до самогубства, які набирають обертів

у світі разом із зростанням кількості постійних користувачів інтернету. Попри те, що інтернет проникає у всі сфери нашого життя, безпеці не приділено достатньої уваги. Особливо важливою є проблема дитячої онлайн-безпеки, яка є пріоритетною для розвинених країн. Участь підлітків у так званих «групах смерті» дедалі частіше стає проблемою не лише родини, а й суспільства загалом. Зараз в Україні майже 22 млн користувачів інтернету, тому питання безпеки в мережі є більш ніж актуальне. У цьому контексті турбота про дітей набуває більших масштабів. Якщо раніше треба було говорити з дітьми про їхню безпеку поза домом тощо, то тепер має сенс застерігати їх від небезпек під час перебування в інтернеті».

2. Мозковий штурм «Безпека в інтернеті – це... небезпека в інтернеті – це...»

Мета: актуалізувати знання учасників щодо розуміння понять безпека та небезпека в мережі інтернет.

Час: 15 хв.

Необхідні матеріали: фліпчарт та маркери.

Хід проведення:

Тренер/тренерка розділяє аркуш фліпчарту на дві колонки із заголовками:

«Безпека в інтернеті – це...» «Небезпека в інтернеті – це...»

та пропонує учасникам по черзі завершити фрази.

Тренер/тренерка фіксує основні висловлювання учасників й підбиває підсумок.

До уваги тренера/тренерки!

Підбиваючи підсумки, тренер/тренерка наголошує, що інтернет-безпека – це галузь комп'ютерної безпеки, яка стосується не тільки інтернету. Цей термін охоплює також безпеку браузера та Всесвітньої павутини, а також безпеку мережі, оскільки вони пов'язані з іншими програмами або операційними системами загалом. Основною метою є встановлення правил та заходів для протидії атакам через інтернет.

Необхідно знайти правильні способи захисту приватного життя, коли ми перебуваємо онлайн. Інформаційна безпека стосується захисту життєво важливих інтересів людини, а також суспільства і держави загалом. Неправдива, неповна чи невчасна інформація може завдати шкоди. У цьому контексті діти є особливо вразливими, оскільки вони можуть не знати, яку інформацію слід викладати в мережу, а яку краще тримати при собі.

Запитання для обговорення:

- *Чим була корисна ця вправа?*
- *На які аспекти безпеки в інтернеті необхідно звертати увагу?*
- *Що може викликати відчуття небезпеки в мережі інтернет?*
- *Чи завжди дитина може зрозуміти та відчути небезпеку, знаходячись в мережі інтернет?*

3. Групова робота «Інтернет в моєму житті та в житті дитини»

Мета: сформувати в учасників готовність до розуміння необхідності дотримання безпеки в інтернеті та розуміння позитивних та негативних сторін його використання.

Час: 40 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери.

Хід проведення:

Тренер/тренерка об'єднує учасників у чотири групи та пропонує обговорити в групах:

Група 1 та група 3 – які можливості та які ризики для дорослої людини має використання мережі інтернет;

Група 2 та група 4 – які можливості та які ризики для дитини має використання мережі інтернет.

На виконання завдання у групі відводиться 15 хвилин.

Після завершення виконання завдання кожна група протягом п'яти хвилин презентує напрацьовані результати.

Запитання для обговорення:

- *Чим була корисна ця вправа?*
- *Що було складніше визначити – можливості чи ризики?*
- *Чим відрізняються можливості та ризики використання мережі інтернет для дорослої людини та дитини?*

4. Інтерактивна вправа «Небезпечна мережа»

Мета: закріплення знань стосовно розуміння інтернет-небезпеки для дітей та необхідності посилення уваги до цього питання.

Час: 30 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, картки із запитаннями та відповідями (Додаток 1.1.1.1).

Хід проведення:

Перший етап. Тренер/тренерка об'єднує учасників у чотири групи. Кожна група отримує картки-запитання, на які необхідно відповісти. На знаходження та обговорення відповіді надається 10 хвилин.

Другий етап. Тренер/тренерка надає групам картки-відповіді. Учасники порівнюють свої відповіді із запропонованими. Висловлюють згоду або незгоду, пояснюючи свою позицію. Час виконання – 10 хвилин.

Третій етап. Тренер/тренерка пропонує обговорення відповідей у груповому колі. Картки-запитання – однакові для всіх. Час для обговорення – 10 хвилин.

До уваги тренера/тренерки!

Для роботи в групах необхідно роздрукувати стільки комплектів карток «запитання-відповідь», скільки буде груп учасників.

Запитання для обговорення:

- *Чим була корисна ця вправа?*
- *Які запитання викликали труднощі у знаходженні відповіді?*
- *Як ви вважаєте, діти знайшли б відповіді на ці запитання?*

Тестові питання до заняття:

1. Інтернет-безпека – це:

А) безпечне навчальне середовище для дітей та дорослих;

Б) галузь комп'ютерної безпеки, яка стосується не тільки інтернету, а і зокрема безпеки браузера та мережі;

В) поточний стан захищеності життєдіяльності людини від безпосередніх загроз її життю, здоров'ю, тілесній неушкодженості, а також особистій свободі;

Г) загальні підходи до розроблення і реалізації відповідних заходів щодо створення і підтримки здорових та безпечних умов життя і діяльності людини.

2. Мета інтернет-безпеки:

А) ввести вікові межі користування інтернетом;

Б) заборонити дітям користування інтернетом;

В) встановити правила та заходи для боротьби з атаками через інтернет;

Г) усі відповіді правильні.

3. Захист дітей в цифровому середовищі охоплює:

А) реагування, підтримку за наявності загрози; запобігання шкідливому впливу;

Б) розуміння та дотримання прав та обов'язків як дітей, так і суспільства;

В) досягнення динамічної рівноваги між захистом та наданням дітям можливості бути цифровими громадянами;

Г) усі відповіді правильні.

4. З якого віку потрібно навчати дітей кібербезпеці?

А) з народження;

Б) з 6 років;

В) з 13 років;

Г) з моменту, коли дитина починає користуватися гаджетами.

5. Інтернет-залежність (адикція) – це:

А) нав'язливе прагнення до застосування інтернету, що призводить до його надмірного використання та довготривалого перебування в мережі, що негативно впливає на життєдіяльність, розвиток і взаємовідносини людини;

Б) прагнення до відходу від реальності за допомогою вживання деяких речовин;

В) постійна фіксація уваги на певних видах діяльності з метою розвитку і підтримки інтенсивних емоцій;

Г) неконтрольована пристрасть до ігор, що руйнує функціональні сфери людини і віднімає реальне життя.

Ключі-відповіді:

1. Б; 2. В; 3. Г; 4. Г; 5. А.

Додаток 1.1.1.1

Картки «Запитання-відповіді»

Картки-запитання	Картки-відповіді
1. Чи можна зробити так, щоб незнайомі люди не могли писати в особисті повідомлення?	**1.** Так. У налаштуваннях особистої сторінки можна активувати режим «Приватний профіль», внаслідок чого інформацію та матеріали, розміщені на сторінці, зможуть переглядати лише «друзі». Писати в особисті повідомлення зможуть лише ті, кому надано дозвіл.
2. Коли варто вказувати свою геолокацію (дозволяти додаткам використовувати геолокацію)?	**2.** Бажано уникати вказування своєї геолокації, адже злочинці можуть використовувати цю інформацію. Якщо геолокація необхідна для функціонування додатка, рекомендується не дозволяти використовувати її постійно, а лише під час використання додатка.
3. З ким можна ділитися логіном та паролем від особистої сторінки?	**3.** Логін та пароль не варто розголошувати іншим людям. З метою безпеки ці дані діти можуть повідомити тільки батькам, але лише під час особистої розмови, а не через інтернет. Також рекомендується не зберігати логін та пароль безпосередньо на гаджетах.
4. Кого можна додавати в друзі в соціальних мережах, чатах онлайн-ігор тощо?	**4.** У соціальних мережах та інших платформах для спілкування варто додавати в друзі лише тих людей, кого ми знаємо в реальному житті.
5. Які фото не можна надсилати друзям?	**5.** Надсилаючи щось в інтернеті, ми автоматично перестаємо володіти цією інформацією, адже ми не можемо контролювати, що наш співрозмовник/співрозмовниця робитиме з надісланим матеріалом – він/вона може його опублікувати, розіслати тощо. Тому перед тим, як щось надіслати, скористайтеся Тестом Білборда: уявіть, що все, що ви хочете написати або надіслати, висить на великому білборді перед школою, який бачать усі. Якщо ця ідея вас засмучує, тоді не варто надсилати такі матеріали.

Заняття 1.1.2. Актуальність забезпечення безпеки дітей в мережі інтернет: визначення понять

Мета: оцінити рівень інформованості учасників, визначити та актуалізувати основні поняття щодо безпеки дитини в інтернеті.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Асоціації	Обговорення	20 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери
2.	Виклики для безпеки дитини в інтернеті та їх мінімізація	Робота в групах	70 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, мультимедійне обладнання, Додаток 1.1.2.1

ХІД ЗАНЯТТЯ

1. Обговорення «Асоціації»

Мета: визначення рівня інформованості учасників, актуалізація основних понять стосовно безпеки дітей в мережі інтернет.

Час: 20 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери.

Хід проведення:

Тренер/тренерка на аркуші фліпчарту пише «Безпека дитини в інтернеті» і пропонує учасникам озвучити асоціації, які виникають у них: «*Сьогодні ми з вами говоримо про безпеку дитини в інтернеті, і я пропоную вам навести пов'язані асоціації, історії, ситуації та явища*».

Тренер/тренерка записує всі відповіді, які надають учасники.

До уваги тренера/тренерки!

Важливо спонукати учасників називати абсолютно всі асоціації, які виникають у них, як позитивні, так і негативні.

Можна використати для цієї вправи інтерактивні платформи Mentimetr або Slido для побудови хмаринки думок.

Запитання для обговорення:

- *Чи складно було знайти відповідну асоціацію?*
- *Чи пов'язані якісь із цих асоціацій з вашим власним досвідом?*

Після обговорення тренер/тренерка підсумовує: «*Безпека дитини в інтернеті – це сукупність заходів, які допомагають забезпечити безпечне користування мережею. Це включає захист від несанкціонованого доступу до особистої інформації, шкідливого контенту, онлайн-булінгу, кіберзлочинності та інших негативних наслідків користування інтернетом. Для забезпечення безпеки дитини в інтернеті дорослі повинні бути проінформовані про загрози, розуміти основні принципи безпеки, а також навчати дітей користуватися*

інтернетом безпечно. Відповідно до дослідження Global Online Safety Survey 2023: Parents' and Kids' Perceptions of Online safety, підлітки стикалися з ризиками в інтернеті частіше, ніж вважають їхні батьки: 74% підлітків повідомили, що зазнавали ризиків в мережі, тоді як лише 62% батьків вважали, що їхні діти стикалися з такими ризиками, що свідчить про різницю в 12%. Наприклад, 39% підлітків повідомили про те, що стикалися з ненавистю в інтернеті, тоді як лише 29% батьків вказали на подібний досвід своїх дітей. Приблизно 19% підлітків стикалися з погрозами насильства, тоді як лише 11% батьків зазначили про це. Цікаво, що відповідно до даних міжнародного дослідницького проєкту ESPAD, лише 6,7% опитаних підлітків в Україні не користуються соціальними мережами».

2. Робота в групах «Виклики для безпеки дитини в інтернеті та їх мінімізація»

Мета: сформулювати визначення основних понять та сприяти усвідомленню можливих способів мінімізації ризиків для безпеки дитини в інтернеті.

Час: 70 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, мультимедійне обладнання, Додаток 1.1.2.1.

Хід проведення:

Тренер/тренерка зазначає: «*Серед зазначених під час виконання попередньої вправи асоціацій траплялись виклики, з якими стикаються сучасні діти в мережі інтернет. Важливо усвідомлювати їх ризики та мінімізувати їх*».
Тренер/тренерка об'єднує учасників у п'ять команд.

Кожна команда отримує по одній темі із викликом.

До уваги тренера/тренерки!

Якщо у відповідях учасників під час виконання попередньої вправи зазначались сучасні виклики, можна обрати саме їх для роботи в групах.

Якщо таких не було, можна підготувати картки з конкретними викликами та запропонувати учасникам команд обрати одну з підготовлених карток:

1 – віртуальні челенджі та TikTok тренди

2 – неналежний контент

3 – онлайн-ігри

4 – штучний інтелект

5 – інтернет-знайомство

Кожна команда має 20 хвилин, щоб зазначити ризики від обраного командою виклику та можливі кроки для їх мінімізації.

Після цього кожна команда презентує усім свої напрацювання до десяти хвилин кожна.

Тренер/тренерка робить узагальнення і показує матеріали із Додатка 1.1.2.1, щоб усі учасники розуміли, де можна дізнатись більше актуальної інформації про онлайн-безпеку.

Тестові питання до заняття:

1. Безпека в інтернеті дитини охоплює:

А) захист від несанкціонованого доступу до особистої інформації;

Б) захист від шкідливого контенту, кібербулінгу;

В) захист від кіберзлочинності та інших негативних наслідків від користування інтернетом;

Г) усі відповіді правильні.

2. Для забезпечення безпеки в інтернеті дитини, дорослі повинні:

А) бути проінформовані про загрози;

Б) розуміти основні принципи безпеки в інтернеті;

В) належним чином навчати дітей користуватися інтернетом в безпечний спосіб;

Г) усі відповіді правильні.

3. Виклики для безпеки дитини в інтернеті:

А) віртуальні челенджі та ТікТок тренди;

Б) заборонений контент;

В) онлайн-ігри;

Г) усі відповіді правильні.

4. У разі виникнення запитань у сфері онлайн-безпеки варто:

А) звернутися на «гарячу лінію» чи до експертів;

Б) негайно телефонувати у поліцію;

В) шукати відео у ТікТок;

Г) усі відповіді правильні.

5. Які ризики існують для безпеки в інтернеті?

А) шахраї;

Б) фішинг;

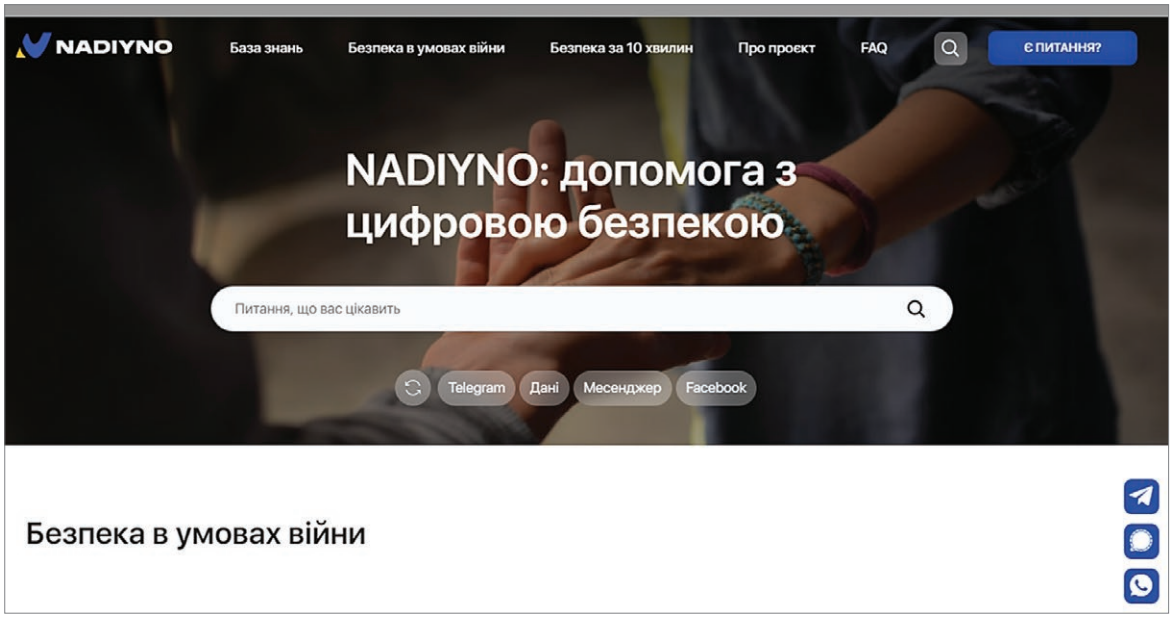
В) слабкий рівень цифрових навичок;

Г) усі відповіді правильні.

Ключі-відповіді:

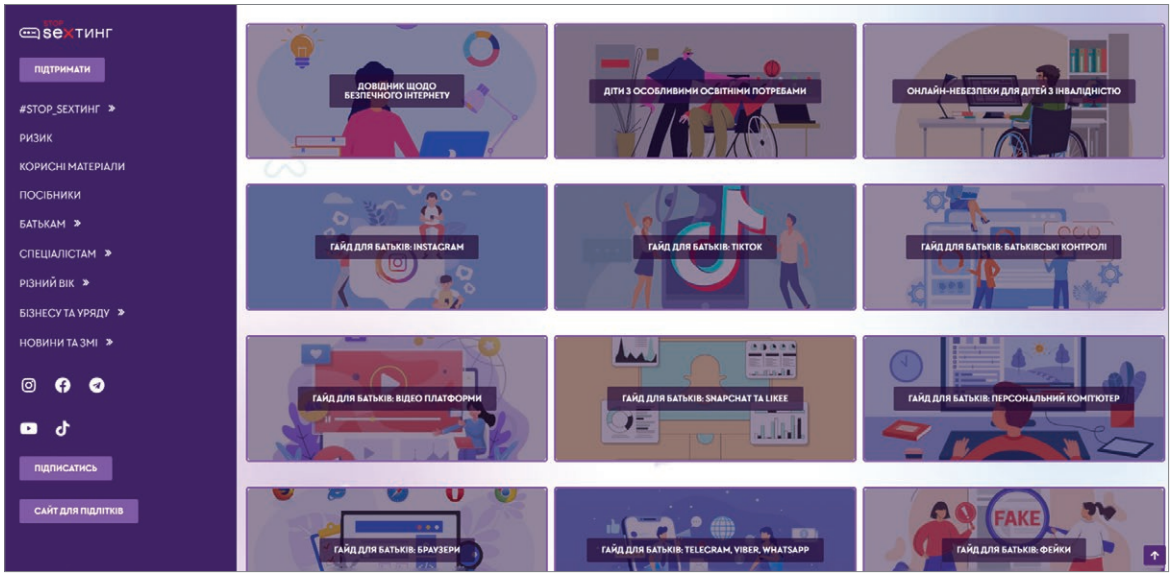
1. Г; 2. Г; 3. Г; 4. А; 5. Г.

Додаток 1.1.2.1



МІНЗМІН

наближаємо людей до змін, а зміни до людей



Заняття 1.1.3. Війна як умова посилення ризиків для дітей в мережі інтернет

Мета: надати інформацію про нові загрози, які очікують на дітей в інтернеті в час війни, та спеціаліальні ресурси допомоги, які можна порадити дітям у випадках онлайн-ризиків.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Ризики для дітей в інтернеті під час війни	Мозковий штурм	25 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.1.3.1
2.	Як може діяти зловмисник/ зловмисниця	Робота в групах	40 хв	Маркери, аркуші паперу для фліпчарту, фліпчарт, Додаток 1.1.3.2
3.	Куди звертатися дітям по допомогу?	Мозковий штурм	25 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.1.3.3

ХІД ЗАНЯТТЯ

1. Мозковий штурм «Ризики для дітей в інтернеті під час війни»

Мета: дізнатися загальний рівень інформованості учасників заходу щодо питань онлайн-безпеки під час війни.

Час: 25 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.1.3.1.

Хід проведення:

Тренер/тренерка звертає увагу учасників на аркуш фліпчарту, де написано «*Які ризики актуальні для дітей в інтернеті у воєнні часи?*», та просить слухачів запропонувати свої варіанти. Тренер/тренерка записує варіанти на аркуші. Після того, як усі варіанти будуть зафіксовані, тренер/тренерка модерує обговорення.

Запитання для обговорення:

- *Які наслідки вони можуть мати для дітей?*
- *Як можна помітити, що дитина залучена до небезпечної ситуації онлайн?*
- *Чому вони особливо актуальні у воєнні часи?*

До уваги тренера/тренерки!

Цю вправу можна провести з використанням інтерактивної платформи Slido.

Під час обговорення доцільно використовувати інформацію з Додатка 1.1.3.1.

Після обговорення тренер/тренерка зазначає: «*Ми з вами побачили, що існує багато ризиків, з якими діти можуть стикатися в онлайн-світі, що має значний вплив на їхній психоемоційний стан, і може загрожувати їхньому життю та здоров'ю. Безпека в інтернеті – це надзвичайно актуальне і гостре питання, особливо під час війни. Багато людей втратили все, що мали, і це спонукає дітей та їхніх батьків шукати*

способи заробітку для підтримання родини. Водночас постійно зростає кількість випадків експлуатації дітей правопорушниками, оскільки діти проводять в інтернеті дедалі більше часу. Причинами цього можуть бути не лише брак соціальних контактів в офлайн-житті, а й особисті проблеми та негаразди у сім'ї. Недостатня інформація про онлайн-ризики, їх причини та способи захисту призводять до того, що діти стають легкою мішенню для правопорушників, які використовують їх для збору розвідувальної інформації».

2. Робота в групах «Як може діяти зловмисник/зловмисниця»

Мета: обговорити, за допомогою яких методів і якими способами зловмисники можуть отримати інформацію у дітей в інтернеті.

Час: 40 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.1.3.2.

Хід проведення:

Тренер/тренерка об'єднує учасників у три групи. Кожна з груп протягом 15 хвилин має обговорити та зафіксувати на аркушах паперу для фліпчарту «алгоритм дій» (способи, методи, засоби), які можуть використовувати зловмисники, щоб дізнатися інформацію у дітей в інтернеті:

Група 1 – алгоритми для отримання інформації про розташування військ;

Група 2 – алгоритми поширення неправдивої інформації (ІПСО) через дітей;

Група 3 – алгоритми отримання оголених фото-/відео-/інших матеріалів з метою подальшого шантажування.

Після закінчення часу на роботу в групах, кожна з команд обирає учасника (-цю), який (-а) буде представляти ідеї.

До уваги тренера/тренерки!

Під час обговорення для доповнення напрацювань учасників доцільно використовувати інформацію з Додатка 1.1.3.2.

Можна додати ефект змагальності: та команда, яка запропонує більше ідей, переможе.

Запитання для обговорення:

- *Чи дізналися ви про нові способи, за допомогою яких злочинці можуть дізнатися у дітей інформацію під час війни?*
- *За яким принципом зловмисник обирає дитину для досягнення своїх цілей, та чи впливає на цей вибір вік дитини?*
- *Чому діти в це вірять?*

3. Мозковий штурм «Куди звертатися дітям по допомогу?»

Мета: проінформувати учасників про спеціалізовані ресурси допомоги, які вони можуть додатково порадити дітям як елемент психологічної підтримки дітей, які постраждали від онлайн-ризику.

Час: 25 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.1.3.3.

Хід проведення:

Тренер/тренерка звертається до учасників із питанням: «*Чому діти рідко звертаються по допомогу у випадках онлайн-ризиків?*» та записує відповіді учасників на аркуші фліпчарту.

До уваги тренера/тренерки!

Перед проведенням цього завдання потрібно ознайомитися із додатками та попередньо роздрукувати потрібні матеріали для повідомлення та уточнення відповідей слухачів. Можна озвучити статистичні дані, наведені у Додатку 1.1.3.3.

Після мозкового штурму тренер/тренерка додає ресурси, куди можна звернутися по допомогу, використовуючи Додаток 1.1.3.3.

Запитання для обговорення:

- *Куди можна порекомендувати звернутися по допомогу дітям та батькам за додатковою психологічною підтримкою у разі, якщо вони постраждали від онлайн-ризиків?*
- *В якому віці й до кого дитина ймовірніше звернеться?*
- *Чому діти не діляться з своїми близькими ситуаціями, що трапляються з ними у мережі інтернет?*

Тестові питання до заняття:

1. Що таке кіберсталкінг?

А) це обмін власними фото/відео/стрімами та іншими матеріалами інтимного характеру;

Б) дії зловмисника, які спрямовані на постійне спостереження та привертання уваги за допомогою соціальних мереж, дзвінків (як на мобільний телефон, так і у месенджерах), докучання та слідкування онлайн;

В) це налагодження незнайомцями довірливих стосунків в інтернеті з дитиною з метою отримання приватних матеріалів, інтимних фото чи/або відео, шантажування ними та вимагання грошей чи додаткових матеріалів;

Г) правильної відповіді немає.

2. Чому діти спілкуються з незнайомцями? (оберіть декілька варіантів)

А) через феномен «ілюзія спальні»;

Б) через шантаж, погрози злочинця;

В) щоб отримати більше уваги від батьків;

Г) інтернет повністю безпечний, і можна спілкуватися з ким завгодно.

3. Чому діти відчувають себе в безпеці вдома і не розуміють, як дії онлайн можуть призвести до проблем у реальному житті?

А) діти вважають, що батьки їх контролюють в інтернеті, тому їм нічого не загрожує;

Б) в інтернеті немає небезпечних людей, тому вони не зможуть дітям ніяк нашкодити;

В) діти добре розуміють, які дії в інтернеті можуть призвести до проблем у реальному житті, та завжди стежать за своїми діями;

Г) це феномен «ілюзія спальні».

4. Як російські військові можуть використовувати дітей, щоб отримати потрібну інформацію?

А) ніяк, від дітей нічого корисного не отримати;

Б) дитину можуть використовувати для розвідки території (наприклад пошуку військових та цивільних об'єктів інфраструктури) та коригування вогню;

В) вивчити особисті та родинні деталі дитини, щоб відшукати батьків та отримати інформацію через них;

Г) усі відповіді правильні.

5. Яка частка дітей побачила вперше сексуальний контент у віці 7-13 років?

А) 97%

Б) 93%

В) 83%

Г) ніхто не бачив.

Ключі-відповіді:

1. Б; 2. А,Б; 3. Г; 4. Б; 5. В.

Додаток 1.1.3.1

Огляд контенту, який діти можуть спостерігати в мережі інтернет

Ворожі диверсанти проникають у наш онлайн-простір. Маскуючись під українські нікнейми та імена, вони приховуються за патріотичними аватарками та фотографіями з синьо-жовтим прапором, намагаючись завоювати нашу довіру та отримати розвідувальну інформацію не лише від дорослих, а й від дітей. Це методи, які використовують злочинці, щоб заволодіти бажаним. Дітей можуть використовувати для розвідки території (наприклад пошуку військових та цивільних об'єктів інфраструктури) та коригування вогню. В інтернеті діти є особливо вразливими через феномен «ілюзія спальні», коли вони почуваються в безпеці вдома і не усвідомлюють, як їхні дії онлайн можуть призвести до проблем у реальному житті. Важливо пам'ятати, що дії, здійснені онлайн, мають наслідки у офлайн-світі.

Організація «Офком» опублікувала результати дослідження, в якому вказує, що 37% дітей віком 12-15 років спостерігали тривожний або неприємний контент в інтернеті. 32% учнів віком 8-11 років також стикалися з таким контентом. Але це дослідження не враховує те, з чим можуть стикатися діти під час війни. Результати обстрілів, вибухів, вбивств, руйнувань – ось те, що може чекати на дитину в інтернет-просторі сьогодні.

Розглянемо можливі ризики для дітей в інтернеті в часи війни детальніше.

- Фейки – публікація свідомо неправдивої інформації з метою маніпуляції суспільною думкою, навмисне поширення дезінформації для розділення суспільства на кілька ворогуючих таборів. Наприклад, фейки про публічні страти українських солдат, інформація про те, що українські військові катують дітей, або утиски російськомовних українців.
- ІПСО (інформаційні психологічні спеціальні операції) – поширення дезінформації, наприклад, на початку війни в повідомленнях з'являлася інформація, що балончиками із фарбою наносять мітки для позначення напрямку руху ворожої техніки, або про «особливу любов ворога» до приурочення своїх обстрілів, наступальних дій до «значущих дат». Це все робиться з метою поширення паніки та відвертання уваги людей і військових від важливих справ.
- Публікація шкідливого контенту – створення та поширення інформації, яка може завдати шкоди дитині. Наприклад, публікація результатів обстрілів, прильотів ракет, фото-/відео-/прямі трансляції з таких місць.
- Боти – програми, створені людьми, які виконують певний алгоритм дій за заданим розробником порядком. Вони можуть бути частиною ІПСО, використовуватися для збору інформації від дітей, атакувати їх у соціальних мережах та провокувати кібербулінг.
- Таємні завдання – прохання надання фото-/відео-/геолокацію для отримання інформації про розташування українських військових або скупчення людей. Приклад: тік-токер, який оприлюднив відео біля ТРЦ «Ретровіль» з українськими військовими, що призвело до удару по ТРЦ артилерією ворога;
- Анонімні чати – додають дитину у чат, де вона нікого не знає, починають комунікацію та завойовують довіру з метою шантажу, вимагання або залякування. Наприклад, створюють телеграм-канал і додають туди десять або більше учасників, після чого грають у ігри у текстовому форматі, спілкуючись у перервах між іграми. Дитина вважає, що спілкується з «справжніми користувачами», тоді як насправді це одна людина, яка спілкується від імені інших, щоб завоювати довіру та отримати потрібну інформацію.
- Онлайн-ігри – неконтрольоване використання ігор. Під час війни діти можуть ненавмисно розкривати будь-яку інформацію. Наприклад, граючи у гру, дитина починає спілкування в чаті з незнайомцем, і між ними зав'язується дружня розмова. Після кількох ігор «друг/по-

друга» запитує, де живе дитина, чим займається, та просить обмінится фото. Далі можуть відбуватися різні сценарії онлайн-ризиків.

- Пошук легкого заробітку – ситуації, коли діти можуть стикатися з букмекерськими конторами, каперами, онлайн-казино, або отримувати прохання від незнайомих дорослих зробити фото себе, локацій. Наприклад, реклама нелегальної букмекерської контори у Україні, яка обіцяє «заробити 2000 грн за кілька хвилин».
- Онлайн-витрати – неконтрольоване батьками використання сімейних коштів на дитячі потреби: онлайн-ігри, покупки перків, бустів, скінів, кейсів, лутбоксів. Особливо особливо актуально під час війни, оскільки дитина може стати постраждалою від впливу російських медіа та ненавмисно донатити російським військовим або витрачати гроші на застосунки.
- Неналежний контент – перегляд контенту, не призначеного для певного віку. Згідно з дослідженням, більшість дітей в Україні (83%) вперше побачили сексуальний контент у віці 7-13 років. 59,8% побачили його неочікувано самостійно. 12,6% – хтось показав неочікувано, лише 7,8% самостійно шукали подібний контент. Щодо дітей молодшого шкільного віку, вони зазначили, що не бачили контенту сексуального змісту. (3,7% – бачили майже кожен день, а 6,3% – бачили щонайменше раз на тиждень). Також до неналежного контенту відносять різноманітний «травмуючий контент», як-от сцени удушення, вбивства, людських тіл після воєнних дій тощо.
- Кіберсталкінг – дії зловмисника, спрямовані на постійне спостереження та привертання уваги за допомогою соціальних мереж, дзвінків (як на мобільний телефон, так і у месенджерах), докучання та переслідування онлайн.
- Кібербулінг – систематичне цькування та вчинення насильства за допомогою засобів електронної комунікації. Наприклад, дитину цькують однокласники в інтернеті за її зовнішній вигляд або відсутність дорогих речей. Вони пишуть у приватні повідомлення з невідомих акаунтів, залишають образливі коментарі, а також можуть використовувати фотошоп для створення принизливих зображень, які публікують на своїх сторінках у соцмережах. Відповідальність регламентується статтею 173-4 КУпАП.
- Секстинг – обмін особистими фото, відео та текстовими матеріалами інтимного характеру з використанням сучасних засобів зв'язку: мобільних телефонів, електронної пошти, соціальних мереж. Наприклад, двоє підлітків з однієї школи (можливо, однокласники або однолітки) добровільно надсилають одне одному свої оголені фото.
- Секторшен – налагодження незнайомцями довірливих стосунків в інтернеті з дитиною для отримання приватних матеріалів, інтимних фото чи відео, шантажування ними та вимагання грошей чи додаткових матеріалів. Наприклад, невідомий користувач починає спілкування з одинадцятикласницею, втирається у довіру і просить надіслати фото чи відео – спочатку в одязі, потім оголену руку, далі оголені плечі і так далі. Після цього починає шантажувати, вимагаючи надіслати більш відверті матеріали, інакше погрожує поширити наявні фото серед друзів, однолітків тощо.
- Онлайн-грумінг – побудова довірливих стосунків дорослою особою або групою дорослих з дитиною з метою сексуального насильства в онлайн-просторі чи у реальному житті.

Додаток 1.1.3.2

Чому діти спілкуються з незнайомцями та передають їм інформацію?

1. «Ілюзія спальні». Діти почуваються в безпеці вдома і не усвідомлюють, що їхні дії в онлайн-середовищі можуть призвести до проблем у реальному житті. Важливо пам'ятати, що дії, зроблені онлайн, мають наслідки у офлайн-світі.
2. Цікавість. Допитливість та прагнення знайти відповіді на запитання, такі як: «А це для чого? А як це працює? А навіщо?» тощо, можуть призводити дітей до травмуючого контенту або до зловмисників.
3. Пропозиції, які викликають інтерес. Наприклад, пропозиції сфотографувати якийсь об'єкт за донат у грі, надіслати свої фото або приватну інформацію про батьків чи себе, чи обіцянка подарувати «скін», «бокс», «лутбокс» (це 3D-моделі, що змінюють вигляд персонажів, зброї, амуніції в онлайн-іграх), або допомогти з апгрейдом персонажа під час комунікації в онлайн-грі.
4. Шантаж, залякування, погрози. Маніпуляції з боку зловмисників, які погрожують розповсюдити контент, уже надісланий дитиною. Погрози можуть включати вбивство когось із батьків чи рідних.
5. Почуття особливості та унікальності. Гонка за кількістю підписників та прагнення бути «кращим (-ою) за інших» може спонукати дітей додавати в соціальних мережах будь-яких незнайомців.
6. Бажання заробити гроші. Підлітки можуть прагнути допомогти батькам, відчути себе дорослим або придбати нові речі.
7. «Унікальність комунікації». Спілкування з новими дорослими може давати дітям відчуття дорослості та самостійності.
8. Психологічна вразливість дітей під час війни (розірвані соціальні контакти, внутрішнє переміщення, біженці, а також батьки, які зайняті вирішенням своїх проблем і не приділяють достатньо часу дітям).

Як можуть почати комунікацію зловмисники/диверсанти:

- додають в анонімний чат;
- незнайомець просить додати у друзі/підписується на профіль дитини;
- невідомий користувач (зловмисник) коментує, ставить «лайки» під контентом;
- пропонує зустрітися офлайн з метою сексуального/фізичного насильства над дитиною, або як наслідок шантажу;
- пише у приватні повідомлення з різноманітними запитами (можливість заробити, просить про допомогу, перейти за посиланням).

Поради, які можна надати дітям для додаткової безпеки:

1. Зберігати спокій.
2. Не повідомляти і не поширювати приватну інформацію про себе, батьків, друзів у соціальних мережах – це включає адреси, номери будинків, квартир, номери телефонів, паролі, особисті дані, а також фото/відео та номери банківських карток.
3. Блокувати користувача/додати його у «чорний список» та скаржитися адміністрації соціальної мережі на спам або неприйнятний контент.
4. Не переходити за посиланнями.
5. Не реагувати на заклики про допомогу від незнайомих акаунтів.

6. Зробити профілі своїх соціальних мереж закритими, щоб доступ мали лише друзі та підписники.
7. Завжди перевіряти та верифіковувати інформацію, адже ви можете натрапити на неперевірену інформацію (фейк).
8. Підтримувати «чистоту» свого смартфону (блокувати його після використання, не ділитися паролями, завантажувати застосунки лише з офіційних магазинів, встановлювати надійні паролі та подвійну двоетапну автентифікацію).
9. Дотримуватися «правил користування спільноти» і не відкривати файлів із позначками 18+ або такими, що «можуть містити сцени насильства» чи «неприйнятний контент», оскільки це може негативно вплинути на вашу психіку.

Додаток 1.1.3.3

Куди можна порекомендувати звертатися по допомогу дітям та їхнім батькам, які постраждали від онлайн-ризиків

Згідно із дослідженням, майже половина дітей НЕ поділились ситуацією, що сталася з ними. Існують ризики, які можуть призвести до кримінальної чи адміністративної відповідальності. Насамперед важливо звернути увагу на причини, *чому діти не звертаються по допомогу до дорослих у разі онлайн-ризиків*:

- погрози, шантаж;
- залякування;
- бояться, що їх будуть засуджувати та звинувачувати у тому, що трапилося;
- дорослі не повірять;
- бояться засмутити дорослих;
- переконання, що їм заборонять бачитися з друзями, грати в телефоні або будуть на них кричати;
- відсутність відкритих розмов з батьками на цю тему;
- не хочуть заважати батькам;
- страх контролю з боку дорослих за кожен крок і дію;
- відсутність довіри до батьків або дорослих;
- сумніви в тому, що дорослі можуть щось зробити («А що вони вдіють?»).

Важливо навчати дітей, батьків та тих, хто працює з дітьми, як зберігати докази, коли та як треба звертатися до поліції для притягнення винних до відповідальності. Крім того, у випадках онлайн-ризиків дітям та їхнім родинам буде цінно звернутися по додаткову психологічну допомогу та інформацію до таких джерел:

1. «Гаряча лінія» допомоги – Урядова консультаційна лінія з питань безпеки дітей в інтернеті – 1545 (далі 3).
2. Чат-бот «ГО стопсекстинг» – чат для дітей та їхніх батьків, який допоможе отримати психологічну допомогу і повідомити про насильство над дитиною онлайн.
3. Чат-бот «Кіберпес» (у телеграмі та у вайбері).
4. Чат-бот @online_kids_bot в телеграмі та на сайті проєкту.

Інформацію, щодо чат-ботів можете знайти на офіційних сторінках ГО «Стоп секстинг» та сайту Мінцифри.

5. Портал повідомлень про контент, який зображає сексуальне насильство над дітьми на сайті: https://report.iwf.org.uk/ua.
6. Чат-не-бот Unsee, якому можна анонімно поскаржитися на небажаний контент у мережі: @Unsee_nebot.
7. Платформи безоплатної психологічної допомоги громадських організацій (проєкти «Ла Страда» «Teenergizer», «Дівчата», «ПОРУЧ»). Це спеціальні проєкти, які були створені психологами для дорослих та підлітків, які можуть потребувати анонімної психологічної, безоплатної консультації з різних причин та максимально швидко.

Зараз в Україні є велика кількість різних способів надати кваліфіковану та якісну психологічну допомогу для дітей та підлітків. Багато хто про неї просто не знає. Наведені вище приклади організацій, чат-ботів, платформ, «гарячих ліній» не є вичерпними. Це тільки найвідоміші та загальноукраїнські проєкти. Цілком можливо, що у вашому регіоні перебування є організації, які також можуть надати психологічну допомогу.

ТЕМА 1.2. Онлайн-ризики та насильство в кіберпросторі

Заняття 1.2.1. Визначення та співвідношення понять щодо онлайн-ризиків та насильства в кіберпросторі

Мета: оцінити рівень поінформованості учасників щодо термінології, пов'язаної зі сферою онлайн-ризиків та насильства в кіберпросторі, визначити та актуалізувати основні поняття у цій сфері.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Вступ до тематики	Інформаційне повідомлення	20 хв	
2.	Нові виклики – нові терміни	Мозковий штурм	15 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери
3.	Пазли	Робота в групах	35 хв	Аркуші паперу для фліпчарту, маркери, клей, конверти, Додаток 1.2.1.1
4.	Визначення понять	Інформаційне повідомлення	20 хв	Мультимедійне обладнання, Додаток 1.2.1.2

ХІД ЗАНЯТТЯ

1. Інформаційне повідомлення «Вступ до тематики»

Мета: актуалізувати питання онлайн-ризиків та насильства в кіберпросторі щодо дітей, а також усвідомлення стрімкого розвитку онлайн-ризиків для дітей.

Час: 20 хв.

Хід проведення:

Тренер/тренерка звертається до учасників: *«Стрімкий розвиток інформаційних технологій призвів до того, що 84% дітей починають користуватись інтернетом у віці 5-11 років, і щороку спостерігається тенденція до «омолодження» віку початку користування інтернетом та соціальними мережами. Від стаціонарних комп'ютерів інтернет перейшов до смартфонів, що дає змогу дітям перебувати онлайн постійно: спілкуватися, підтримувати стосунки, грати, шукати і обмінюватися інформацією. Це є позитивною стороною інтернет-комунікацій, проте ці процеси супроводжуються й негативними аспектами, зокрема поширенням у онлайн-середовищі небезпечних тенденцій, які загрожують життю та здоров'ю дітей.*

Серед таких онлайн-ризиків слід виділити:

- *ризики, пов'язані з контентом: сприйняття неточної або неповної інформації, невідповідного або навіть забороненого контенту, наприклад контенту, призначеного для дорослих/екстремістського/насильницького/експліцитно-насильницького контенту, контенту, пов'язаного з самоприниженням та самокатуванням, контенту, пов'язаного з деструктивною і насильницькою поведінкою, радикалізацією чи підтримкою ідей расистського та дискримінаційного характеру;*

- *ризики, пов'язані з контактами з боку дорослих або однолітків: домагання, виключення, дискримінація, наклеп та шкода репутації, а також сексуальні зловживання та сексуальна експлуатація. Це може включати здирництво, грумінг у сексуальних цілях, матеріали, пов'язані з сексуальними зловживаннями щодо дітей, торгівля дітьми та сексуальна експлуатація дітей у подорожах та туризмі, а також вербування екстремістськими угрупованнями;*
- *ризики, пов'язані з контрактами: невідповідні договірні відносини, питання згоди дітей в онлайн-середовищі, прихований маркетинг, азартні ігри в онлайн-середовищі, а також порушення та неправомірне використання особистих даних. Це може включати злом, шахрайство, крадіжку особистих даних та упереджене ставлення, засноване на профілюванні;*
- *ризики, пов'язані з поведінкою: обмін сексуальним контентом, створеним самостійно, а також ризики, пов'язані з ворожою та насильницькою поведінкою однолітків, такі як кібербулінг, переслідування, виключення та домагання.*

Всі ці негативні явища, пов'язані з онлайн-ризиками та насильством в кіберпросторі, сприяли впровадженню нової термінології, яка позначає різні їх види».

До уваги тренера/тренерки!

Для забезпечення наочності та кращого сприйняття інформації доцільно підготувати мультимедійні слайди.

2. Мозковий штурм «Нові виклики – нові терміни»

Мета: оцінити рівень поінформованості учасників щодо наявної термінології, пов'язаної зі сферою онлайн-ризиків та насильства в кіберпросторі.

Час: 15 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери.

Хід проведення:

Тренер/тренерка звертається до аудиторії з пропозицією назвати відомі їм терміни, які позначають різні види онлайн-ризиків та насильства в кіберпросторі. Всі запропоновані аудиторією терміни фіксуються на аркуші для фліпчарту. За необхідності, тренер/тренерка доповнює перелік названих термінів.

До уваги тренера/тренерки!

Для проведення цієї вправи можна використати інтерактивні платформи Mentimetr, Slido для побудови хмаринки думок.

3. Робота в групах «Пазли»

Мета: оцінити рівень обізнаності учасників щодо основних термінів, пов'язаних зі сферою онлайн-ризиків та насильства в кіберпросторі, та розуміння їх змісту.

Час: 35 хв.

Необхідні матеріали: аркуші паперу для фліпчарту, маркери, клей, конверти, в яких на окремих аркушах знаходяться назви основних термінів, а їх визначення розбиваються на словосполучення по 3-5 слів (Додаток 1.2.1.1).

Хід проведення:

Тренер/тренерка об'єднує учасників у чотири групи та забезпечує кожну групу аркушем паперу для фліпчарту, маркерами, клеєм, конвертами, в яких на окремих аркушах знаходяться назви основних термінів, а їх визначення розбито на словосполучення по 3-5 слів (Додаток 1.2.1.1).

Кожна група учасників отримує завдання: враховуючи наявні в учасників знання (або асоціації), протягом 15 хвилин необхідно відтворити визначення основних понять, використовуючи наявні словосполучення в конвертах, приклеївши їх на аркуш для фліпчарту (так би мовити, зібрати «пазли»). Після завершення виконання завдання групи по черзі презентують своє бачення щодо розуміння основних термінів, пов'язаних зі сферою онлайн-ризиків та насильства в кіберпросторі.

До уваги тренера/тренерки!

Залежно від наявного часу на виконання вправи, можна роздати кожній команді елементи всіх термінів або декількох з них. Якщо команди опрацювали всі терміни, презентацію результатів роботи в групах доцільно організувати по черзі по одному поняттю, не повторюючи їх.

Доцільно підготувати мультимедійні слайди з правильними визначеннями термінів та після презентації командою одного з них, а також коментарів інших груп, виводити правильну відповідь на екран.

Запитання для обговорення:

- *Чи складно було сформулювати поняття? В чому саме полягала складність?*
- *Чи всі терміни були вам знайомі? Чи чули ви їх раніше?*
- *Чи важливим є єдине розуміння понять? Чому?*

4. Інформаційне повідомлення «Визначення понять»

Мета: систематизувати знання учасників щодо понятійного апарату у сфері онлайн-ризиків та насильства в кіберпросторі, надати інформацію щодо основних термінів.

Час: 20 хв.

Необхідні матеріали: мультимедійне обладнання, Додаток 1.2.1.2.

Хід проведення:

Тренер/тренерка презентує інформацію з Додатка 1.2.1.2, після чого пропонує учасникам порівняти презентовану інформацію із виконаними вправами 2 та 3.

Запитання для обговорення:

- *Чи вважають учасники за потрібне закріплення презентованих понять у національному законодавстві?*
- *Чому важливим є закріплення визначення понять в нормативно-правових актах?*

Тестові питання до заняття:

1. Характеристику якого онлайн-ризику в кіберпросторі визначено помилково?

А) сексторшен – налагодження довірливих стосунків із дитиною в інтернеті з метою отримання приватних матеріалів (інтимні фото або відео) для подальшого шантажування дитини, вимагання додаткових матеріалів або грошей;

Б) фішинг – це одна з форм шахрайства, що проявляється у вигляді певних різновидів атак з використанням соціальної інженерії, який часто використовується для крадіжки персональних даних користувачів, зокрема даних для входу в облікові записи та номерів кредитних карток, для подальшого їх використання із злочинною метою;

В) тролінг – надсилання, отримання власноруч створеного сексуального контенту, зокрема зображення, повідомлення або відео, чи обмін ними за допомогою сучасних засобів зв'язку: мобільних телефонів, електронної пошти, соціальних мереж тощо;

Г) грумінг – налагодження/побудова взаємин із дитиною особисто або за допомогою інтернету чи інших цифрових технологій, з метою домогтися сексуальних зв'язків із цією особою в цифровому середовищі або в реальному житті, схиливши дитину вступити в сексуальний зв'язок.

2. До якої групи онлайн-ризиків належить обмін сексуальним контентом, створеним самостійно, або ризики, що характеризуються ворожою та насильницькою діяльністю однолітків, такі як кібербулінг, переслідування, виключення та домагання?

А) ризики, пов'язані з контентом;

Б) ризики, пов'язані з поведінкою;

В) ризики, пов'язані з контактами з боку дорослих або однолітків;

Г) ризики, пов'язані з контрактами.

3. Надсилання, отримання власноруч створеного сексуального контенту, зокрема зображення, повідомлення або відео, чи обмін ними за допомогою сучасних засобів зв'язку: мобільних телефонів, електронної пошти, соціальних мереж – це...

А) сексторшен;

Б) фішинг;

В) секстинг;

Г) порнографічний контент.

4. Дії, спрямовані на поширення інформації, яка не відповідає дійсності або викладена неправдиво, тобто містить відомості про події та явища, яких не існувало взагалі або які існували, але відомості про них не відповідають дійсності (неповні або перекручені) – це...

А) кіберсталкінг;

Б) онлайн-грумінг (кібергрумінг);

В) розповсюдження шкідливого (небажаного) контенту в кіберпросторі;

Г) розповсюдження неправдивої недостовірної інформації в кіберпросторі.

5. Яким умовам повинні відповідати матеріальні об'єкти, предмети, друкована, аудіо- та відеопродукція, зокрема реклама, повідомлення та матеріали, продукція засобів масової інформації, електронних засобів масової інформації для віднесення до таких, що мають порнографічний характер?

А) основний зміст продукції або її значну частину становить демонстрація великим планом статевих органів у збудженому стані або деталізований опис чи демонстрація статевого акту;

Б) продукція містить натуралістичне зображення, максимально наближене до реальної анатомії і фізіології людини та її статевого акту;

В) продукція створена виключно з метою статевого збудження її споживачів;

Г) повинні відповідати всім перерахованим умовам.

Ключі-відповіді: 1. В; 2. Б; 3. В; 4. Г; 5. Г.

Додаток 1.2.1.1

КІБЕРБУЛІНГ –

навмисні агресивні дії,

що неодноразово вчиняються

групою осіб або окремою особою

за допомогою цифрових технологій

та спрямовані проти особи, якій

важко захиститися.

СЕКСТИНГ –

надсилання, отримання власноруч

створеного сексуального контенту

зокрема зображення, повідомлення або відео

чи обмін ними за допомогою

сучасних засобів зв'язку.

ОНЛАЙН-ГРУМІНГ –

процес налагодження/побудови взаємин

із дитиною особисто або

за допомогою інтернету чи

інших цифрових технологій,

з метою домогтися сексуальних зв'язків

із цією особою в цифровому середовищі

або в реальному житті,

схиливши дитину вступити в сексуальний зв'язок.

СЕКСТОРШЕН –

налагодження довірливих стосунків

із дитиною в інтернеті

з метою отримання приватних матеріалів

(інтимні фото або відео)

для подальшого шантажування дитини,

вимагання додаткових матеріалів або грошей.

ПОРНОГРАФІЧНИЙ КОНТЕНТ –

це інформаційні матеріали (зображення, відео, аудіо, тексти),

наповнення (склад) певного інформаційного ресурсу,

що містить вульгарно-натуралістичну,

цинічну, непристойну фіксацію статевих актів,

самоцільну, спеціальну демонстрацію геніталій,

антиетичних сцен статевого акту,

сексуальних збочень, зарисовок з натури,

які не відповідають моральним критеріям,

ображають честь і гідність людини,

спонукаючи негідні інстинкти.

ШКІДЛИВИЙ (НЕБАЖАНИЙ) КОНТЕНТ –

це інформаційні матеріали (зображення, відео, аудіо, тексти),

наповнення (склад) певного інформаційного ресурсу,

що заохочують до небезпечної або незаконної діяльності,

може загрожувати серйозною психологічною травмою,

фізичною шкодою або смертю.

РОЗПОВСЮДЖЕННЯ НЕДОСТОВІРНОЇ ІНФОРМАЦІЇ –

це дії, спрямовані на поширення інформації,

яка не відповідає дійсності або викладена неправдиво,

тобто містить відомості про події та явища,

яких не існувало взагалі або які існували,

але відомості про них

не відповідають дійсності (неповні або перекручені).

ФІШИНГ –

це одна з форм шахрайства,

що проявляється у вигляді

певних різновидів атак

з використанням соціальної інженерії,

яке часто використовується для

крадіжки персональних даних користувачів,

зокрема даних для входу в облікові записи

та номерів кредитних карток,

для подальшого їх використання із злочинною метою.

ТРОЛІНГ –

це глузування

з метою

спровокувати

конфлікт.

КІБЕРСТАЛКІНГ –

це переслідування

в інтернеті.

Додаток 1.2.1.2

Під **кібербулінгом** зазвичай розуміють навмисні агресивні дії, що неодноразово вчиняються групою осіб або окремою особою за допомогою цифрових технологій та спрямовані проти постраждалої, якій важко захиститися. Зазвичай це передбачає використання цифрових технологій та інтернету для розміщення чутливої інформації про будь-кого, навмисне поширення відомостей особистого характеру, небажаних світлин або відео, надсилання повідомлень із погрозами чи образами (електронною поштою, у форматі миттєвого обміну повідомленнями, в чатах і текстових повідомленнях), поширення пліток та неправдивої інформації про постраждалу особу або навмисне виключення її з онлайн-спілкування. Кібербулінг може відбуватися безпосередньо (в чатах або текстових повідомленнях), у межах спільноти з обмеженим доступом (розсилання постів та дратівливих повідомлень за списком електронних адрес) або ж у громадському доступі (наприклад створення сайтів з метою знущань). Сучасні американські дослідники Робін Ковальскі, С'юзан Лімбер і Патріція Агатстон виокремлюють вісім типів поведінки, що характеризують кібербулінг і відображають переважну більшість різновидів негативного впливу в інтернет-просторі:

1. *Суперечки або флеймінг* (від англ. *flaming* – пекучий, гарячий, полум'яний) – обмін короткими гнівними й запальними репліками між двома чи більше учасниками за допомогою комунікаційних технологій. Найчастіше розгортається в «публічних» місцях інтернету, таких як чати, форуми, дискусійні групи, а іноді перетворюється на затяжну війну. На перший погляд, флеймінг виглядає як боротьба між рівними, але в певних умовах він може стати формою нерівноправного психологічного терору. Неочікуваний випад може призвести до сильних емоційних переживань, особливо тоді, коли особа не знає, хто серед учасників яку займе позицію, наскільки його/її власна позиція буде підтримана значущими учасниками.

2. *Нападки, постійні виснажливі атаки* (англ. *harassment*) – повторювані образливі дії, спрямовані на особу, які найчастіше виявляються у формі численних атак у вигляді повідомлень (наприклад сотні смс-повідомлень на мобільний телефон або постійні дзвінки), що перевантажують персональні канали комунікації. На відміну від перепалки, атаки є більш тривалими й односторонніми. Нападки можуть відбуватися в чатах чи на форумах (місця розмов в інтернеті). В онлайн-іграх атак найчастіше зазнають гравці, які стають постраждалими від гріферів (*grieffers*) – груп учасників, що ставлять собі за мету перемогти в певній грі, руйнуючи ігровий досвід інших учасників.

3. *Обмовлення, зведення наклепів* (*denigration*) – розповсюдження принизливої неправдивої інформації з використанням комп'ютерних технологій. Це можуть бути текстові повідомлення, фото або пісні, які змальовують постраждалу особу в негативному, іноді сексуальному контексті. Об'єктами обмовлення можуть ставати не тільки окремі підлітки, але й групи: відбувається розсилка списків, наприклад «хто є хто», або «хто з ким перебуває у стосунках» у класі чи школі. Створюються також спеціальні «книги для критики» (*slam books*), у яких розміщуються жарти про однокласників, що можуть містити наклепи. Це перетворює гумор на техніку «списку ненависті», з якого вибираються мішені для вивільнення агресії, зливу роздратування, тренування власної злоби.

4. *Самозванство, втілення в певну особу* (*impersonation*) – форма переслідування, за якої зловмисник позиціонує себе як постраждала особа, використовуючи її пароль доступу до її акаунту в соціальних мережах, блогах, пошті, системах миттєвих повідомлень тощо. Після цього він/вона здійснює негативну комунікацію від її імені. Організація «хвилі зворотних зв'язків» відбувається, коли з адреси постраждалої особи, без її відома, надсилають ганебні провокаційні листи її друзям і близьким за адресною книгою. Постраждала особа потім от-

римує несподівано гнівні відповіді. Особливо небезпечним є використання імперсоналізації щодо людей, включених до «списку ненависті», адже це наражає їхнє життя на реальну небезпеку.

5. *Ошуканство, видурювання конфіденційної інформації та її розповсюдження (outing & trickery)* – процес отримання персональної інформації під час міжособової комунікації та її подальше передавання (текстів, фото, відео) в публічну зону інтернету або поштою тим, кому ця інформація не призначена.

6. *Відчуження (остракізм), ізоляція*. Кожній людині, особливо в дитинстві, властиво сприймати себе як частину групи або поза нею. Бажання бути включеним у групу є мотивом багатьох вчинків підлітків. Виключення з групи сприймається як соціальна смерть. Чим більше людина виключається з взаємодії, наприклад у грі, тим гірше вона почувається, і тим більше знижується її самооцінка. У віртуальному середовищі виключення також спричиняє серйозні емоційні негаразди, аж до повного емоційного руйнування дитини. Онлайн-відчуження можливе в будь-яких типах середовищ, де використовується захист паролями, формується список небажаної пошти або список друзів. Кібероствракізм проявляється також через відсутність швидкої відповіді на миттєві повідомлення чи електронні листи.

7. *Кіберпереслідування* – це дії з прихованого спостереження за переслідуваними особами або тими, хто, вештаючись, перебуває поблизу. Зазвичай такі дії здійснюються нишком, анонімно, з метою організації злочинних дій, таких як спроби зґвалтування, фізичне насильство або побиття. Відстежуючи необережних користувачів через інтернет, злочинець отримує інформацію про час, місце та всі необхідні умови здійснення майбутнього нападу.

8. *Хепіслепінг* (від англ. *happy slapping* – щасливе ляскання) – зйомка та поширення відеороликів, в яких зафіксовані реальні напади. Відеоролики нападів з метою ґвалтування чи його імітації інколи ще називають «хопінг» (від англ. *hopping* – «наскок»), що особливо поширено в США. Ці відеоролики розміщують в інтернеті, де його можуть переглядати тисячі людей, зазвичай без жодної згоди постраждалої особи. Інша форма хепіслепінгу – це передавання сюжетів через мобільні телефони.

Секстинг зазвичай визначається як надсилання та отримання власноруч створеного сексуального контенту, зокрема зображення, повідомлення або відео, а також обмін ними за допомогою сучасних засобів зв'язку: мобільних телефонів, електронної пошти, соціальних мереж тощо.

У більшості країн створення, поширення та зберігання зображень сексуального характеру, що стосуються дітей, є незаконним. У разі поширення таких зображень, дорослі не повинні їх переглядати. Демонстрація зображень сексуального характеру дитині дорослим завжди є злочинним діянням. Поширення таких зображень між дітьми може завдати серйозної шкоди, і про подібні інциденти слід обов'язково повідомляти. Також може знадобитися допомога для усунення поширених зображень.

Грумінг в цифровому середовищі, згідно з Люксембурзькими керівними настановами, означає процес налагодження взаємин із дитиною особисто або за допомогою інтернету чи інших цифрових технологій з метою домогтися сексуальних зв'язків із цією особою як у цифровому середовищі, так і в реальному житті. Це включає спроби схилити дитину вступити до сексуального контакту. Процес онлайн-грумінгу спрямований на заманювання дітей до дій або бесід сексуального характеру як з їхнього відома, так і без нього, а також встановлення взаємин між порушником і дитиною, щоб зробити останню вразливішою до сексуальних зловживань. Термін «грумінг» не передбачений у міжнародному праві; в деяких юридичних системах, зокрема в Канаді, використовується термін «заманювання».

Сексторшен – налагодження довірливих стосунків із дитиною в інтернеті з метою отримання приватних матеріалів (інтимні фото або відео) для подальшого шантажування дитини, вимагання додаткових матеріалів або грошей.

Порнографічний контент – інформаційні матеріали (зображення, відео, аудіо, тексти), що містять вульгарно-натуралістичну, цинічну або неприйстойну фіксацію статевих актів, а також спеціальну демонстрацію геніталій і антиетичних сцен статевого акту, сексуальних збочень, або натуралістичні зарисовки, які не відповідають моральним критеріям і ображають честь та гідність людини, спонукаючи до негідних інстинктів.

Слід зазначити, що відповідно до положень чинного законодавства, матеріальні об'єкти, предмети, друкована, аудіо-, відеопродукція, зокрема реклама, повідомлення та матеріали засобів масової інформації, електронних засобів масової інформації належать до продуктів з порнографічним характером, за умови, якщо вони відповідають таким критеріям:

1) основний зміст продукції або її значну частину становить демонстрація великим планом статевих органів у збудженому стані або деталізований опис чи демонстрація статевого акту;

2) продукція містить натуралістичні зображення, максимально наближені до реальної анатомії і фізіології людини та її статевого акту;

3) продукція створена виключно з метою статевого збудження її споживачів.

Шкідливий (небажаний) контент – інформаційні матеріали (зображення, відео, аудіо, тексти), які заохочують до небезпечної або незаконної діяльності та можуть загрожувати серйозною психологічною травмою, фізичною шкодою або смертю.

Розповсюдження недостовірної інформації в кіберпросторі – дії, спрямовані на поширення інформації, яка не відповідає дійсності або викладена неправдиво. Ця інформація може містити відомості про події та явища, яких не існувало взагалі, або які існували, але інформація про них є неповною чи перекрученою.

Фішинг – одна з форм шахрайства, що проявляється у вигляді певних різновидів атак з використанням соціальної інженерії. Фішинг часто використовується для крадіжки персональних даних користувачів, зокрема даних для входу в облікові записи та номерів кредитних карток, з метою їх подальшого використання у злочинних намірах.

Тролінг – глузування або провокація з метою спровокувати конфлікт.

Кіберсталкінг – це переслідування в інтернеті. Сталкер, тобто переслідувач, може стежити за постраждалою особою через соціальні мережі, створювати для цього фейкові акаунти, писати в різні месенджери, а також створювати нові сторінки і профілі, якщо попередні заблокують. Сталкінг згадується у Конвенції Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу із цими явищами (Стамбульській конвенції), яка передбачає, що сторони зобов'язані вжити необхідні законодавчі або інші заходи для забезпечення того, щоб умисна поведінка, що полягає в повторному вчиненні загрозливої поведінки, спрямованої на іншу особу та змушує її боятися за свою безпеку, була криміналізована.

Заняття 1.2.2. Онлайн-ризики та насильство в кіберпросторі: секстинг, онлайн-грумінг, сексторшен

Мета: ознайомити учасників із поняттями «секстинг», «онлайн-грумінг» та «сексторшен», причинами та наслідками зазначених онлайн-ризиків для дітей, а також алгоритмом дій, за допомогою якого можна захистити дітей онлайн.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Поговоримо про секстинг, онлайн-грумінг та сексторшен	Інформаційне повідомлення	25 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.2.2.1
2.	Причини та наслідки секстингу	Робота у парах	25 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.2.2.2
3.	Працюємо з реальними ситуаціями	Робота у групах	40 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.2.2.3, посилання на відео «Як відбувається грумінг в інтернеті? Історія української родини», «Online сексуальне насильство над дітьми (кібергрумінг)»

ХІД ЗАНЯТТЯ

1. Інформаційне повідомлення «Поговоримо про секстинг, онлайн-грумінг та сексторшн»

Мета: ознайомити учасників із дефініціями секстингу, онлайн-грумінгу та сексторшену, а також основними причинами та наслідками цих онлайн-ризиків.

Час: 25 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.2.2.1.

Хід проведення:

Тренер/тренерка, попередньо ознайомившись із Додатком 1.2.2.1, повідомляє учасникам про те, що таке секстинг, онлайн-грумінг та сексторшен, причинно-наслідковий характер вищезазначених онлайн-ризиків. Потрібно фіксувати на фліпчарті ключові аспекти своєї доповіді (який саме матеріал фіксувати, визначає тренер/тренерка) або підготувати мультимедійну презентацію.

Запитання для обговорення:

- *Чи чули ви щось про секстинг, онлайн-грумінг чи сексторшен до заняття?*
- *Які причини дають змогу маніпулювати зловмиснику дитиною?*
- *Як пережите в дитинстві онлайн-насильство може вплинути на майбутнє доросле життя?*

2. Робота у парах «Причини та наслідки секстингу»

Мета: сформувати в учасників розуміння причин та наслідків секстингу, а також визначити рекомендації для дітей щодо надсилання своїх фото та відео в інтернет.

Час: 25 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.2.2.2.

Хід проведення:

Тренер/тренерка об'єднує учасників по двоє (за бажання, вони можуть самі обрати, з ким будуть працювати) та просить кожну пару зазначити на аркуші причини та наслідки секстингу для дитини. Після роботи в парах тренер/тренерка ініціює загальне обговорення та формує загальний перелік із озвучених по черзі парами варіантів причин та наслідків на окремому аркуші фліпчарту.

Запитання для обговорення:

- *Які б ви дали рекомендації дітям щодо надсилання своїх фото та відео в інтернеті?*
- *Чи можна видалити фото з мережі, які вже були надіслані?*

До уваги тренера/тренерки!

Під час обговорення доцільно використовувати інформацію, наведену в Додатку 1.2.2.2.

3. Робота у групах «Працюємо з реальними ситуаціями»

Мета: проаналізувати та дізнатися більше про онлайн-грумінг та сексторшен на прикладах, що трапилися у реальному житті з дітьми.

Час: 40 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.2.2.3, посилання на відео «Як відбувається грумінг в інтернеті? Історія української родини», «Online сексуальне насильство над дітьми».

Хід проведення:

Тренер/тренерка об'єднує учасників у три групи. Кожна із груп отримує для перегляду та аналізу посилання на відео із реальними ситуаціями, що трапилися з дітьми в інтернеті.

Група 1 – *відео* «Як відбувається грумінг в інтернеті? Історія української родини» (https://youtu.be/yGYKGa6J9eY?si=s_lLtg3UaFZAqVmM);

Група 2 та група 3 – *відео* «Online сексуальне насильство над дітьми». Це відео містить у собі дві історії: одна – про хлопчика, інша – про дівчинку. Одна група переглядає та аналізує історію хлопчика, а інша, відповідно, – дівчинки (https://youtu.be/b-gaa9ZI2JE?si=5JDkFqFaOop2ORTK).

Потрібно переглянути відео, проаналізувати його та відповісти на питання:

- *Як ви вважаєте, який це онлайн-ризик? Чому?*
- *Чому діти погоджуються поширювати свої інтимні фото чи відео, або роблять онлайн-трансляції сексуального характеру?*
- *Які емоції у вас виникали під час перегляду відеоматеріалів?*
- *Сформулюйте порядок дій для дитини, якщо вона потрапила у таку ситуацію.*
- *Що важливо знати дорослим, які знаходяться поруч із постраждалою дитиною, зокрема батькам та вчителям?*

Час на перегляд відео – 10 хвилин, на підготовку відповідей – 15 хвилин, решта часу – на обговорення.

До уваги тренера/тренерки!

Під час загального обговорення доцільно використовувати інформацію, наведену в Додатку 1.2.2.3.

Тестові питання до заняття:

1. Згідно зі статистикою, чи зупиниться шантаж дитини після того, як зловмисник отримає бажане?

А) зазвичай зупиняється, лише 2% злочинців продовжують шантаж;

Б) ймовірніше, що ні, 68% дітей і далі страждають від злочинця;

В) зупиняється, бо злочинець отримав усе, що хотів;

Г) не зупиняється у 100% випадків.

2. Обмін власними фото-, відео- , текстовими матеріалами та/або дій сексуального характеру із застосуванням сучасних засобів зв'язку: мобільних телефонів, електронної пошти, соціальних мереж. Про який ризик йдеться?

А) секстинг;

Б) кіберсталкінг;

В) онлайн-грумінг;

Г) сексторшен.

3. Наслідки сексторшену? (оберіть декілька варіантів)

А) більшість дітей, які мали досвід сексторшену, заподіювали собі шкоду, вчиняли спроби самогубства через отриману психологічну травму;

Б) психологічна травма;

В) ризик збільшення ваги тіла;

Г) нездорові очікування від статевих стосунків.

4. Чи є в Україні відповідальність за онлайн-грумінг?

А) так, кримінальна;

Б) так, адміністративна;

В) питання про обговорення внесення змін до законодавства на розгляді у Верховній Раді України;

Г) ні.

5. Чому важливо вчити дітей правилам поводження в інтернеті?

А) щоб діти знали, як обрати інтернет-провайдера;

Б) діти повинні уміти приховувати інформацію від дорослих;

В) бо видалити контент із мережі неможливо;

Г) це не важливо, діти можуть робити все, що хочуть в інтернеті.

Ключі-відповіді:

1. Б; 2. А; 3. А,Б; 4. А; 5. В.

Додаток 1.2.2.1

Секстинг

Секстинг – це обмін власними фото, відео, текстовими матеріалами та/або діями сексуального характеру із застосуванням сучасних засобів зв'язку: мобільних телефонів, електронної пошти, соціальних мереж, а також дії приватного характеру сексуального формату на камеру. Світова статистика свідчить, що секстинг – це явище, яке поширене серед 22% дівчат та 18% хлопців до 18 років.

Причини:

1. Підлітки вбачають у цьому цікавий і безпечний спосіб пізнати свою сексуальність, сприймаючи це як веселу гру або невинний флірт.
2. Це спосіб отримати увагу та схвальні коментарі, лайки, що допомагають підняти їхню самооцінку.
3. Обмін такими матеріалами може бути способом виразити довіру та симпатію до того, кому ці фото (відео чи повідомлення) надсилаються.
4. Це може бути наслідком примусу або шантажу (наприклад від хлопця/дівчини: «Якщо ти не надішлеш своє фото – значить, у нас все несерйозно. Ти мені не довіряєш, і ми припиняємо наші стосунки»).

Наслідки:

1. Шантаж, вимагання та маніпуляції зловмисником над постраждалою особою. Це може призвести до посилення залежності через страх опублікування матеріалів.
2. Якщо фото, відео, інші матеріали були поширені третім особам, дитина часто відчуває страх, сором, приниження, почуття провини, ганьби, злість та самозвинувачення. Це може призвести до емоційного дистресу, самовіддалення від інших, суїцидальних думок.
3. Дитина може зіткнутися з кібербулінгом в мережі та булінгом у закладі освіти, а також іншими принизливими діями.
4. Загроза психічному здоров'ю дитини.

Відео про секстинг: https://www.youtube.com/watch?v=Qv506wMWrZA.

Сексторшен

Сексторшен – це налагодження довірливих стосунків з дитиною в інтернеті незнайомцями з метою отримання приватних матеріалів, інтимних фото чи відео, а також їх шантажування та вимагання грошей або додаткових матеріалів. Це може також включати дії сексуального формату на камеру. Згідно з дослідженнями організації «Центру дослідження кібербулінгу» (https://cyberbullying.org/sextortion-michigan-teen), щонайменше 5% підлітків стали постраждалими від сексторшену. До того ж ФБР (https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/sextortion/sextortion) фіксує значний сплеск ситуацій, які пов'язані із сексторшеном.

Для ознайомлення пропонуємо відеоролики про це:

- Online сексуальне насильство над дітьми: https://www.youtube.com/watch?v=b-gaa9ZI2JE.
- Злочинці шукають дітей в інтернеті. Соціальна реклама про небезпеки в мережі: https://www.youtube.com/watch?v=e-vsl2Xr5Cw.
- Соціальна реклама. Переконайтеся, що у вашому домі зачинені двері від сексуальних насильників: https://www.youtube.com/watch?v=OmFEo6NQDYA&t=19s.

Причини, які дають змогу зловмиснику маніпулювати дитиною:

1) довіра до незнайомця. Злочинці часто використовують фейкові профілі підлітків для налагодження контакту й завоювання довіри;
2) брак уваги в реальному житті. Недостатня кількість соціальних контактів призводить до того, що діти та підлітки намагаються знайти друзів або романтичні стосунки в інтернеті;
3) погрози завдати шкоди. Зловмисники можуть погрожувати заподіяти шкоду дитині чи членам її родини, якщо вона не надішле фото;
4) залякують створити неіснуючий сексуалізований контент. Злочинці можуть поєднувати обличчя дитини з тілом іншої людини через спеціальні застосунки, якщо дитина не зробить те, що злочинці вимагають;
5) залякують вчинити суїцид, якщо дитина чи підліток не надішле оголене фото;
6) обмін грошей чи подарунків за контент.

Наслідки:

1. Наслідки сексторшену мають однаковий вплив на дівчат та хлопців будь-якого віку. Згідно з дослідженнями Transparency International, 1 з 3 дітей, які постраждали від сексторшену, заподіювали собі шкоду або вчиняли спроби самогубства через отриману психологічну травму. Більшість з тих, хто зіткнувся з цим явищем, повідомляють про відчуття самотності, високої тривоги та депресивні думки.
2. Психологічна травма, спричинена цим ризиком, впливає на всі сфери життя постраждалої особи. Це може включати зниження продуктивності, відмову від відвідування навчання, а також уникання місць, де потенційно можна зустрітись зі злочинцем. Дитина знаходиться в постійній тривозі та страху.
3. Постраждалі від сексторшену можуть відчувати стигму суспільства, що проявляється у неприйнятті, приниженні, ізоляції та звинуваченнях у тому, що сталося.

Онлайн-грумінг

Відео з мамою дівчинки-постраждалої на цю тему, за закритим посиланням: https://youtu.be/yGYKGa6J9eY?si=CP86Z43_PLxcFHqg.

Онлайн-грумінг – це процес, в якому дорослі або група дорослих налагоджують довірливі стосунки з дитиною (підлітком) з метою сексуального насильства в онлайн-середовищі чи у реальному житті, а також проводять дії приватного характеру сексуального формату на камеру. Це іноді переростає до вимагання офлайн секс-зустрічей, внаслідок чого діти стають постраждалими від зґвалтувань, або використання їх у виготовленні матеріалів сексуального насильства. Одна з причин цього полягає в тому, що, спілкуючись онлайн із незнайомцем, діти втрачають обережність і перестають дотримуватися правил поведінки з незнайомими людьми. Дослідження організації THORN показало, що серед опитаних постраждалих дітей від онлайн-грумінгу кожна четверта дитина була віком 12 років або менше. 62% дітей погоджувалися на вимоги злочинців, а для 68% з них погрози, вимоги та шантаж не зменшувалися навіть після надсилання матеріалів. Відповідальність за онлайн-грумінг встановлена частиною 2 статті 156 ККУ.

Причини, які дають змогу зловмиснику маніпулювати дитиною:

1. постраждалими можуть ставати діти, які відчувають труднощі в спілкуванні з однолітками, зокрема соціальні та комунікаційні проблеми, а також брак уваги в реальному житті. Вони намагаються знайти друзів чи романтичні стосунки в інтернеті;
2. діти з низькою самооцінкою часто мають обмежене розуміння ризиків в інтернеті й можуть сприймати всіх онлайн-знайомих як вірних друзів;

3. відсутність контролю за часом, проведеним онлайн, з боку дорослих;
4. більше довіряють незнайомцям в інтернеті, оскільки зловмисники часто використовують фейкові профілі підлітків для налагодження контакту;
5. зловмисники погрожують заподіяти шкоду дитині чи членам її родини, якщо вона не надішле фото;
6. зловмисники залякують дітей створити неіснуючий сексуалізований контент, поєднуючи обличчя дитини з тілом іншої людини через спеціальні застосунки, якщо дитина не виконає їхні вимоги;
7. зловмисники можуть залякувати дітей, погрожуючи вчинити суїцид, якщо дитина чи підліток не надішле оголене фото;
8. обмін грошей чи подарунків на контент, що зображає сексуальну експлуатацію або насильство над дитиною, наприклад, отримані фото, відео або записи прямих етерів з оголеними дітьми чи підлітками (своїми або друзів/подруг/братів/сестер).

Британська організація Internet Watch Foundation виділила найпоширеніші види злочинів в інтернеті проти дітей за останній рік:

- самостійно створений контент сексуального характеру (селфі), який діти були змушені робити на вимогу злочинців вдома у своїх кімнатах. За даними IWF, 73% зазначеного контенту належить саме до цієї категорії;
- вебстріми, які діти під примусом проводять з дому;
- втягування в прямі етери або стріми своїх молодших братів і сестер, які навіть не усвідомлюють, що це може бути записано. Ця тенденція спостерігалася у 57% контенту.

Наслідки:

1) самотність, відчай та безвихідь – діти погоджуються на всі умови кривдників;
2) відчуття провини за те, що сталося, або думка, що дитина на це заслуговує;
3) порушення довіри з боку злочинця, яке негативно впливає на подальшу побудову стосунків дитини з оточенням;
4) суїцид – як крайній прояв безвиході;
5) однаковий вплив на дівчат та хлопців будь-якого віку;
6) психологічна травма, спричинена цим ризиком, впливає на всі сфери життя: зниження продуктивності, відмова від відвідування навчання та уникання місць, де потенційно можна зустрітися зі злочинцем. Дитина постійно перебуває в тривозі та переживає страх;
7) постраждалі від грумінгу можуть відчувати стигму суспільства через неприйняття, приниження, ізоляцію та звинувачення у тому, що сталося.

Додаток 1.2.2.2

Чому важливо навчати дітей правилам захисту від сексуального насильства в інтернеті?

Пам'ятайте, що видалити фото та відео з мережі майже неможливо!

1. Діти повинні слідкувати за тим, з ким спілкуються в інтернеті.
2. Діти мають усвідомлювати, що якщо вони не знають, як учинити в певній ситуації, їм слід повідомити дорослих.
3. Дітям важливо не довіряти незнайомцям та НЕ поширювати свої інтимні зображення.
4. Діти повинні розуміти, що потрібно ігнорувати прохання надіслати своє інтимне фото. Якщо людина справді цінує стосунки, то зрозуміє і більше не проситиме.
5. Діти мають знати «Правило білборду» – перш ніж натиснути «опублікувати» або «надіслати», уявіть, що це фото, відео, текст буде надруковано на величезному білборді поруч зі школою, і його побачать всі, хто буде йти повз нього. Варто задуматися, чи ви хочете, щоб це бачили всі. Якщо ні, то краще не відправляти такий контент.
6. Діти повинні знати, як блокувати користувачів, які змушують почуватися некомфортно.
7. Діти мають розуміти, що секстинг – це не норма і не частина здорових романтичних стосунків.
8. Діти повинні знати, що якщо хтось показав їм інтимне фото знайомої людини, вони мають розповісти про це цій людині, не критикуючи і не образивши її, а просто поінформувати, що такий матеріал став доступний.
9. Якщо матеріали є у вільному доступі в інтернеті, варто звернутись на портал для видалення такого контенту, щоб він не поширювався далі: https://stop-sexting.in.ua/send/.

Додаток 1.2.2.3

Що важливо знати дорослим (не поліцейським), які знаходяться поруч із постраждалою дитиною, зокрема батькам та вчителям?

Орієнтовний алгоритм дій для секстингу, онлайн-грумінгу та сексторшену

1. Підтримайте дитину. Пам'ятайте, що в таких ситуаціях дитина відчуває сором і може перебувати під тиском.
2. Не вимагайте від дитини, яка причетна до інциденту, розкривати інформацію про зображення (що саме на ньому зображено).
3. Не просіть показати фото чи відео, які зробила дитина, але попросіть її зробити знімок або запис екрану власного гаджета, щоб зафіксувати матеріали листування, фото, відео чи аудіо. Ці дані стануть частиною доказової бази для поліції.
4. Не розголошуйте деталі інциденту іншим співробітникам закладу освіти чи однокласникам дитини. Попередьте їх, що за перегляд та поширення таких матеріалів передбачена кримінальна відповідальність.
5. Поговоріть з батьками дитини. Наголошуйте на тому, щоб вони не звинувачували дитину та не корили себе за те, що сталося. Згідно з дослідженням американської організації THORN, серед опитаних 2 100 дітей, які постраждали від онлайн-грумінгу, кожній четвертій дитині було 12 років або менше. 62% дітей погоджувалися на вимоги злочинців, а для 68% з них погрози та вимоги не зменшувалися навіть після надсилання матеріалів. Секстинг поширений серед 22% дівчат-підлітків і 18% хлопців-підлітків, що становить 20% підлітків всього світу.
6. Дорослі мають сприяти видаленню контенту. Можливо, цей контент є в однокласників, в чатах, хмаросховищах, інших приватних сторінках, платформах чи сайтах. За потреби, донесіть інформацію щодо кримінальної відповідальності (стаття 301-1 ККУ).
7. Заблокуйте цей контент, якщо він в інтернеті, подавши скарги адміністрації соцмережі, месенджера тощо.
8. Якщо матеріали знаходяться у вільному доступі в інтернеті, то варто звернутись на портал для видалення такого контенту, щоб він не поширювався далі: https://stop-sexting.in.ua/send/.
9. Зверніться по допомогу:
   - «Гаряча лінія» допомоги – Урядова консультаційна лінія з питань безпеки дітей в інтернеті – 1545 (далі 3).
   - Чат-бот «ГО стопсекстинг» – чат для дітей та їхніх батьків, який допоможе отримати психологічну допомогу і повідомити про насильство над дитиною онлайн.
   - Портал повідомлень про контент, який зображає сексуальне насильство над дітьми на сайті: https://report.iwf.org.uk/ua.
   - Чат-не-бот Unsee, якому можна анонімно поскаржитися на небажаний контент у мережі: @Unsee_nebot.
   - Платформи безоплатної психологічної допомоги громадських організацій (проєкти «Ла Страда» «Teenergizer», «Дівчата», «ПОРУЧ»). Це спеціальні проєкти, які були створені психологами для дорослих та підлітків, які можуть потребувати анонімної психологічної, безоплатної консультації з різних причин та максимально швидко.

До уваги тренера/тренерки!

Для кращого розуміння слухачами ситуації щодо онлайн-ризиків доцільно запропонувати для індивідуального перегляду тематичні фільми:

1. «Зв'язку немає» (англ. *Disconnect*), 2012, Генрі Алекс Рубін, драматичний трилер, 16+.

2. «Довіра» (*Trust*), 18+, 2010 р., режисер – Енгус Бенфілд.

3. «Чоловіки, жінки і діти», 2014, Джейсон Райтман, комедія, драма, 18+.

Увага! Вікові обмеження. Фільми можуть містити сцени насильства та експлуатації.

Заняття 1.2.3. Онлайн-ризики та насильство в кіберпросторі: порнографічний та інший шкідливий контент для дітей

Мета: ознайомити слухачів із основними видами шкідливого контенту для дітей, його впливом та наслідками для дітей; сформувати розуміння важливості комунікації з дітьми щодо такого контенту та правил поводження в інтернеті із неналежним та порнографічним контентом.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Про що сьогодні говоримо?	Інформаційне повідомлення	35 хв	Фліпчарт, аркуші для фліпчарту, маркери, Додаток 1.2.3.1
2.	Пишемо пост	Робота у групах	35 хв	Аркуші із зошита, паперу, блокнота – для фіксації своїх думок, ручка, Додаток 1.2.3.1, Додаток 1.2.3.2, Додаток 1.2.3.3
3.	План дій	Обговорення	20 хв	Фліпчарт, аркуші для фліпчарту, маркери, стикери за необхідності, Додаток 1.2.3.2, Додаток 1.2.3.3

ХІД ЗАНЯТТЯ

1. Інформаційне повідомлення «Про що сьогодні говоримо?»

Мета: ознайомити слухачів із основними дефініціями та причинами перегляду дітьми неналежного контенту, а також розкрити наслідки та вплив зазначених матеріалів на психіку та дії дитини.

Час: 35 хв.

Необхідні матеріали: фліпчарт, аркуші для фліпчарту, маркери.

Хід проведення:

Тренер/тренерка, попередньо ознайомившись із Додатком 1.2.3.1, повідомляє учасникам про особливості неналежного та порнографічного контенту та його вплив на дітей. Потрібно фіксувати на фліпчарті ключові аспекти своєї доповіді (який саме матеріал фіксувати, визначає тренер/тренерка) або завчасно підготувати мультимедійну презентацію.

Запитання для обговорення:

- *Яким може бути шкідливий контент для дітей в інтернеті?*
- *Як ви вважаєте, чому неналежний контент нормалізується серед дітей?*
- *Про що може свідчити статистика, яка стосується перегляду дітьми порнографічного і неналежного контенту?*
- *Чому діти дивляться порнографічний контент?*
- *Який вплив такий контент має на дітей?*
- *Як можна вберегти дітей від впливу неналежного контенту?*

2. Робота у групах «Пишемо пост»

Мета: докладно обговорити із учасниками вплив та наслідки неналежного та порнографічного контенту на дітей.

Час: 35 хв.

Необхідні матеріали: аркуші із зошита, паперу, блокнота – для фіксації своїх думок, ручка, Додаток 1.2.3.1, Додаток 1.2.3.2, Додаток 1.2.3.3.

Хід проведення:

Тренер/тренерка об'єднує учасників у групи, залежно від кількості учасників. Максимальна кількість груп – п'ять. Завдання для кожної групи – створити інформаційний пост для соціальних мереж на тему, яку отримає група під час розподілу.

Теми для опрацювання:

- види шкідливого контенту для дітей в інтернеті;
- які наслідки має неналежний контент для дітей;
- причини перегляду дітьми шкідливого контенту;
- як перегляд порнографічного контенту дітьми впливає на вразливість дітей до сексуального насильства в інтернеті;
- як діти та батьки можуть обмежити доступ до неналежного контенту.

До уваги тренера/тренерки!

Інформаційний пост – це невеликий за обсягом унікальний текст на задану тему, який коротко розкриває суть питання.

Час на підготовку – 10 хвилин. Обсяг – половина листа із зошита. Можна використовувати для підготовки всі матеріали, що є у наявності.

Після закінчення підготовки, кожна група обирає спікера/спікерку, який/яка представить свій пост для широкого загалу. На презентацію кожній групі дається 2-5 хвилин. Решта часу – на обговорення.

Далі тренер/тренерка пропонує учасникам обговорити їхні напрацювання та зробити висновки про вплив неналежного та порнографічного контенту на дітей, а також запропонувати свій алгоритм, що робити, аби захистити дітей від такого контенту. За потреби, після кожної доповіді тренер/тренерка коригує відповіді, згідно з Додатком 1.2.3.1, Додатком 1.2.3.2, Додатком 1.2.3.3.

3. Обговорення «План дій»

Мета: сформувати у слухачів розуміння важливості обговорення тем щодо впливу неналежного та порнографічного контенту на дітей та створення правил спілкування з дітьми.

Час: 20 хв.

Необхідні матеріали: фліпчарт, аркуші для фліпчарту, маркери, Додаток 1.2.3.2, Додаток 1.2.3.3.

Хід проведення:

Тренер/тренерка пропонує учасникам заходу разом обговорити питання, що подані нижче. Основні положення під час обговорення доцільно фіксувати на аркуші для фліпчарту.

Запитання для обговорення:

- *Чи може дитина самостійно вберегти себе від впливу шкідливого контенту?*
- *Кого ще потрібно залучати для обговорення тем впливу неналежного та порнографічного контенту на дітей?*
- *Запропонуйте алгоритм дій для обмеження впливу такого контенту на дітей.*

До уваги тренера/тренерки!

Під час обговорення доцільно використовувати інформацію, викладену у Додатку 1.2.3.2, Додатку 1.2.3.3.

Тестові питання до заняття:

1. Що таке неналежний контент?

А) неконтрольоване батьками використання сімейних коштів на дитячі потреби: онлайн-ігри, покупки перків, бустів, скінів, кейсів, лутбоксів;

Б) матеріали, що зображають або спонукають до поведінки, яка може фізично/психічно нашкодити дитині та призвести до каліцтв;

В) надання фото/відео/геолокації, для отримання інформації про розташування українських військових, місць скупчення людей;

Г) публікація свідомо неправдивої інформації, для маніпуляції суспільною думкою.

2. Яке визначення ви дасте предметам, друкованим, аудіо-, відеопродукції, зокрема рекламі, повідомленням та матеріалам, продукції засобів масової інформації, електронних засобів масової інформації, змістом яких є детальне зображення анатомічних чи фізіологічних деталей сексуальних дій, чи які містять інформацію еротичного характеру?

А) порнографічні матеріали;

Б) неналежний контент;

В) секстинг;

Г) онлайн-грумінг.

3. Вкажіть причини перегляду дітьми порнографічних матеріалів? (оберіть декілька варіантів)

А) помилкове введення запиту в пошуковій системі;

Б) почули про порнографічний контент у компанії друзів чи від старших людей, і це їх зацікавило;

В) бажання відірватися від надмірного батьківського контролю;

Г) це єдина можливість для них побачити, що таке секс.

4. Чому перегляд порнографічних матеріалів нормалізує секстинг?

А) тому, що перегляд порнографічних матеріалів створює нереальні уявлення про те, яким має бути статевий акт;

Б) бо перегляд порнографічних матеріалів спонукає відірватися від батьківського контролю;

В) бо перегляд порнографічних матеріалів стирає здорові сексуальні кордони, заохочує до поведінки, яка там зображається;

Г) перегляд порнографічних матеріалів ніяк не впливає на це.

5. Які наслідки для дитини перегляду неналежного контенту? (оберіть декілька варіантів)

А) психологічна травматизація побаченого;

Б) дитина бажає заробити на такому контенті гроші;

В) ніяких негативних наслідків від цього контенту немає. Це норма, дитина це переросте;

Г) нормалізація насильства, ранніх статевих відносин, ризикованої поведінки.

Ключі-відповіді:

1. Б; 2. А; 3. А,Б,В,Г; 4. В; 5. А,Г.

Додаток 1.2.3.1

Неналежний контент

Дослідження організації ОФКОМ (https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/children-parents-nov16/children-parents-media-use-attitudes-report-2016.pdf?v=335496) показало, що кожна десята дитина віком від 8 до 11 років, яка користується інтернетом, повідомила, що бачила що-небуть неприємне або тривожне. Третина британських дітей віком 12-15 років стикалися з сексистським, расистським або дискримінаційним контентом.

До розповсюдженого шкідливого контенту в онлайн-середовищі належать матеріали, що зображують:

- удушення – ігри з задухою, утопленням або підвішуванням;
- використання зброї;
- вживання небезпечних предметів і речовин, які не є продуктами харчування і можуть спричиняти отруєння або іншим способом завдати шкоди здоров'ю;
- дії, які можуть призвести до обморожень, опіків чи ударів струмом;
- нанесення собі травм або каліцтв;
- нанесення травм або каліцтв іншим, наприклад раптовий удар;
- небезпечні ситуації без завдання фізичної шкоди – погрози зброєю або вибухівкою, інсценування дзвінка в поліцію, пограбування або інсценування викрадення;
- розіграші, що спричиняють серйозні емоційні потрясіння, зокрема інсценування смерті або самогубства, насильства, наміри батьків (опікуна) залишити дитину, а також психологічне насильство (образи, приниження) стосовно дитини;
- інструкції, як створити вибуховий пристрій;
- насильство – зображення справжніх бійок або інших епізодів насильства (в тому числі і воєнна тематика);
- реклама вживання, виготовлення наркотичних речовин;
- позитивне ставлення до харчових розладів;
- порнографічні матеріали.

Причини перегляду неналежного контенту:

- випадкове виникнення матеріалів у стрічці соціальних мереж;
- неналежні матеріали, які містяться в рекламі;
- перегляд новин, у яких можуть міститися згадані матеріали;
- інтерес до певної тематики, наприклад використання зброї, що призводить до пошуку матеріалів через пошукові системи;
- розсилки у месенджерах (Телеграм, Вайбер, Вотсап, електронна пошта) від незнайомців;
- алгоритми інтернет-пошуку: якщо дитина щось шукала, то схожий контент буде знову з'являтися в її стрічці, внаслідок чого онлайн-середовище заповниться цією темою.

Наслідки:

- психологічна травматизація від побаченого;
- нав'язливе переживання страху;
- нормалізація насильства, ранніх статевих відносин, ризикованої поведінки;
- виникнення суїцидальних намірів – особливо якщо хтось надсилає дитині неналежний контент, який може спонукати до суїцидальних думок, і вимагає його перегляду.

Ознаки виникнення суїцидальних намірів:

- розміщення фраз на сторінках соціальних мереж та в месенджерах, що ілюструють самоприниження;
- завдання собі ушкоджень;
- матеріали, зроблені з висоти (дахи, горища) з неоднозначними написами;
- надмірне захоплення цитатами, присвяченими темі смерті, чи з містичної літератури;
- група друзів, які викликають підозри у дорослих, і з'явились у дитини за короткий час;
- прослуховування музики на тему смутку чи смерті.

Порнографічний контент (перегляд матеріалів)

Перегляд порнографії у дитячому віці нормалізує раннє сексуальне експериментування та заохочує сексуальну активність задовго до того, як діти будуть емоційно, соціально чи інтелектуально готові до цього. Часто такі матеріали зображують секс як випадковий, незахищений і насильницький. Згідно з дослідженням (https://drive.google.com/file/d/1qPWJZ140hv24dZJcClmJv7yVwbrMVIEK/view), більшість дітей в Україні (83%) побачили вперше сексуальний контент у віці 7-13 років. 59,8% побачили його випадково самостійно. 12,6% – хтось показав неочікувано, і лише 7,8% самостійно шукали подібний контент. Найбільш поширеними емоційними реакціями дітей на сексуальний контент були: здивування (35,2%), байдужість (33,6%) та відраза (30,8%).

Причини перегляду порнографічного контенту дітьми:

- помилкове введення запиту у пошуковій системі;
- чутки про порнографічний контент від друзів або старших людей, які зацікавили дітей;
- реклама такого контенту, що може з'явитися на екрані під час пошуку інформації в інтернеті;
- підлітки часом вивчають порнографічний матеріал для того, щоб більше дізнатись про статеві стосунки;
- для дітей це може бути способом боротьби зі стресом та життєвими негараздами;
- бажання відірватися від надмірного батьківського контролю;
- перегляд таких матеріалів однокласниками;
- цікавість до теми;
- демонстрація бунтарської поведінки.

Наслідки перегляду порнографічного контенту:

- нездорові очікування щодо інтимних стосунків;
- хибні уявлення про «норми» того, як має виглядати тіло жінки чи чоловіка та рання сексуалізація;
- неправильні уявлення про дорослі стосунки (наприклад більшість таких матеріалів зображують принизливі статеві відносини, які уявляють задоволення тих, хто бере участь. Найчастіше такий контент зображує приниження жінок і насильницькі дії щодо них. У тих, хто систематично переглядає такий матеріал, може сформуватися враження, що жінці повинно подобатись таке ставлення і в реальному житті);
- у підлітків формується бажання неконтрольованого та частого перегляду таких матеріалів набагато швидше;
- перегляд порнографії робить підлітків більш лояльними до вчинення сексуальних злочинів, зокрема й щодо себе;
- стирання здорових сексуальних кордонів через перегляд порнографії може призвести до залученення дитини до нездорової сексуальної поведінки, наприклад до надсилання чи публікування своїх оголених фото.

Додаток 1.2.3.2

Чи можна захистити дітей від впливу неналежного та порнографічного контенту?

Серед підлітків 53% хлопців і 39% дівчат вважають, що порнографія – це реальне зображення того, як має відбуватись статевий акт.

Для дорослих важливо зрозуміти, що вони можуть зробити для уникнення негативних наслідків перегляду порнографічного контенту:

1. Встановлення батьківського контролю та регулярна перевірка його функціонування на пристроях дитини.
2. Використання спеціальних додатків (наприклад YouTube Kids, Google Kids).
3. Встановлення додаткових налаштувань на телефонах та браузерах, якими користуються діти.
4. Спостерігати за історією браузера та активністю в інтернеті.
5. Спілкуватися з дитиною про статевий розвиток та цікавитися її життям.
6. Варто пояснювати, що не все, що вони бачать в інтернеті, є правдою.
7. Пояснювати дітям, що вони мають звертатися до дорослих щоразу, коли діти не знають, як їм вчинити в інтернеті.

Додаток 1.2.3.3

Що робити дорослим для обмеження впливу неналежного та порнографічного контенту на дітей

Перегляд неналежного контенту

Якщо ви помітили, що дитина переглядає матеріали, що зображають неналежний контент, то потрібно:

1. Поговорити з дитиною та пояснити, що такий контент може їй зашкодити, спонукати до дій, які становлять загрозу для життя та здоров'я.
2. Наголосити, що краще не переглядати цей контент, оскільки він може сформувати нереальні очікування щодо статевого життя та створити неправильне ставлення до людей.
3. Повідомити батьків дитини з метою залучення додаткової уваги до ситуації (розібратися у причинах – можливо, залучити психолога).

Перегляд порнографічного контенту

- Запевніть дітей, що це нормально – відчувати цікавість до сексу.
- Поясніть, що зображення у порнографії викривляють сприйняття реальності й відрізняються від того, як це відбувається в реальному житті.
- Поговоріть про те, як будувати здорові стосунки, засновані на довірі та повазі.
- Навчайте дітей здоровій сексуальності та знанням про секс раніше, ніж це зробить хтось інший. Говоріть з ними відкрито, але відповідно до віку дитини.
- Своєчасне навчання дітей відповідно до віку зменшить ймовірність того, що вона буде шукати відповіді у Google через цікавість. Дайте їм зрозуміти, що, якщо виникатимуть запитання чи занепокоєння, вони можуть звернутися до вас, і ви приймете їхні запитання із розумінням та повагою.
- Поясність дітям, що порнографія – це не те, що повинен подивитися кожен, і вони не повинні відчувати тиску, щоб дивитися це. Скажіть, що зображення чи відео сексуального характеру є неналежними в онлайн-просторі.
- Переконайтеся, що на всіх пристроях налаштовано батьківський контроль (якщо ви батьки), або поговоріть про це з ними.
- Дізнайтеся, які вебсайти відвідують діти, з ким спілкуються.
- Усвідомте, що кривдники можуть використовувати порнографію, щоб зацікавити постраждалу особу.

До уваги тренера/тренерки!

Для кращого розуміння слухачами ситуації щодо онлайн-ризиків доцільно запропонувати для індивідуального перегляду тематичний фільм:
«Нерв», 2016, Генрі Джуст, Еріел Шульман, трилер, 16+.

Увага! Вікові обмеження. Фільм може містити сцени насильства та експлуатації.

ТЕМА 1.3. Стратегії вчинення онлайн-насильства щодо дитини. Ознаки (індикатори), що дитина потрапила в небезпечну ситуацію онлайн

Мета: визначити ризики та небезпеки, з якими може стикнутися дитина в інтернеті; надати інформацію щодо особливостей вчинення насильства щодо дитини; сформувати розуміння учасників про ознаки (індикатори) того, що дитина потрапила в небезпечну ситуацію в онлайн-просторі.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Види онлайн-небезпек	Робота в групах	30 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.3.1
2.	Як вчиняється насильство щодо дитини в онлайн-середовищі	Інтерактивна лекція	30 хв	Аркуші паперу для фліпчарту, маркери, аркуші паперу, мультимедійне обладнання, відео: https://youtu.be/b-gaa9ZI2JE
3.	Ознаки того, що дитина зазнає онлайн-насильства	Вправа	30 хв	2 аркуші для фліпчарту із намальованою дитиною, 2 пари карток до вправи (Додаток 1.3.2), скотч

ХІД ЗАНЯТТЯ

1. Робота в групах «Види онлайн-небезпек»

Мета: актуалізувати знання щодо ризиків та переваг користування дітьми інтернетом.

Час: 30 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.3.1.

Хід проведення:

Тренер/тренерка зазначає: *«Напевно, в сучасному світі ніхто з нас не уявляє життя без інтернету, адже він відкриває перед нами безліч можливостей. Тож спробуймо спочатку сформувати перелік можливостей в інтернеті, які можуть отримати діти».*

Тренер/тренерка об'єднує учасників у дві групи:

Група 1 повинна записати, які можливості отримує дитина в інтернеті;

Група 2 – визначити, з якими ризиками або видами насильства в онлайн-середовищі може стикнутися дитина.

Кожна група працює 10 хвилин, після сигналу тренера/тренерки групи міняються місцями та доопрацьовують результати іншої групи протягом п'яти хвилин.

Після завершення роботи в групах кожна група презентує свої напрацювання, а тренер/тренерка підбиває підсумки, використовуючи інформацію із Додатка 1.3.1.

Наприкінці вправи тренер/тренерка зазначає: *«Ми маємо безліч можливостей в онлайн-просторі, однак, щоб користуватися ним безпечно, важливо знати про ризики. З іншого боку,*

лише усвідомлення ризиків не є достатнім для того, щоб обмежити використання інтернету та убезпечити дитину від цих небезпек».

Запитання для обговорення:

- *З якого віку дитина починає користуватися інтернетом без контролю батьків?*
- *Чи усвідомлюють діти ризики, з якими можуть стикнутись під час користування інтернетом?*

2. Інтерактивна лекція «Як вчиняється насильство щодо дитини в онлайн-середовищі»

Мета: надати інформацію щодо особливостей вчинення насильства щодо дитини в онлайн-середовищі.

Час: 30 хв.

Необхідні матеріали: аркуші паперу для фліпчарту, маркери, аркуші паперу, мультимедійне обладнання, відео «Online сексуальне насильство над дітьми (кібергрумінг)»: https://youtu.be/b-gaa9ZI2JE.

Хід проведення:

Тренер/тренерка ставить учасникам запитання для обговорення:

- *Як злочинцям вдається вчиняти насильство у кіберпросторі?*
- *Як дитина сприймає таку людину (злочинця)?*
- *Як вдається вийти на контакт з дитиною?*

Тренер/тренерка фіксує результати на фліпчарті, після чого розповідає:

«Частіше за все злочинці реєструються в соціальних мережах під виглядом молодих людей, налагоджують контакт в онлайн-іграх або створюють сторінки, розміщуючи інформацію, яка може зацікавити дітей. Використовуючи фейкові акаунти та фотографії, вони маскуються під однолітків, розповідають про ті самі хобі та інтереси, актуальні для дітей, або видають себе за впливових чи знаменитих особистостей. На початку спілкування все виглядає дуже доброзичливо: злочинці приділяють багато уваги, роблять компліменти, хвалять за досягнення тощо, а згодом настає момент, коли вони починають висувати вимоги.

Розгляньмо, як це реалізується на прикладі онлайн-грумінгу. Щоб досягти своєї мети, онлайн-грумери вдаються до маніпуляцій, шантажу чи контролю, потенційно ізолюючи дитину від друзів та сім'ї. Онлайн-грумінг може тривати від одного вечора до декількох тижнів, перш ніж буде отриманий перший матеріал, а згодом починається вимагання грошей, більш інтимного матеріалу або примушування до особистих зустрічей. Через брак досвіду та наївність молоді користувачі можуть піддаватися на такі провокації з боку дорослих.

Основною метою онлайн-грумінгу є аморальні, протиправні дії інтелектуального характеру щодо дитини (натяки, цинічні розмови, демонстрація порнографічної продукції, спокуси, маніпуляції, отримання фото- або відеоматеріалів) або зустріч у реальному світі з метою вчинення дій сексуального характеру, спрямованих на задоволення статевої пристрасті зловмисника.

Грумери вміло маніпулюють дитиною, її сім'єю та колом спілкування, аби приховати свої наміри і уникнути викриття. Вони дотримуються певних стратегій, таких як: вибір

вразливої дитини, отримання доступу до неї, розвиток довірчих стосунків і зниження чутливості до сексуального підтексту. Найчастіше грумер представляється ровесником дитини і починає розмову із загальних питань про вік, інтереси, школу, стосунки з батьками та переходить до питань сексуального досвіду.

Отже, тепер попрошу вас знову повернутися до наших напрацювань, зафіксованих на фліпчарті. Проаналізувавши його, визначте, що можливо треба ще сюди додати, аби ми з вами повністю впорались із завданням?

Зараз я попрошу уважно подивитись відео та визначити/занотувати фази онлайн-грумінгу, який використовує злочинець».

Тренер/тренерка пропонує учасникам переглянути відео за лінком:

https://youtu.be/b-gaa9ZI2JE та відповісти на питання: «Які фази ви виокремили?»

Учасники презентують свої бачення, після чого тренер/тренерка продовжує:

«Зазвичай можна виокремити такі фази онлайн-грумінгу:

1. *Фаза формування дружби – це стадія початкового контакту. Зазвичай це випадкова розмова між користувачами інтернет-сайту на визначену дорослим тему або питання про профіль дитини.*
2. *Наступна фаза – на цьому етапі розмова зазвичай набуває більш індивідуального характеру, але сексуальний підтекст не є обов'язковим.*
3. *Фаза оцінки ризику – реалізація злочинного наміру. На цій стадії онлайн-грумер може ініціювати розмову про секс, алкоголь, наркотики, надіслати фото чи спробувати зателефонувати.*
4. *Фаза ізолювання – тут онлайн-грумер намагається відвернути постраждалу особу від її друзів. Він/вона маніпулює почуттям провини дитини, наголошуючи на тому, що вона забула про нього/неї, коли не в мережі, або приділяє йому/їй недостатньо уваги. Підвищена «потреба» дитини бути онлайн може бути показником її залучення у цю фазу.*
5. *Інтимна фаза – це кінцева фаза, яка може настати внаслідок примусу, обману, загрози викриття або відносин, які досягають рівня почуття любові грумера.*

Сам процес онлайн-грумінгу може відбуватися стрімко, проте негативний психологічний вплив на дитину може бути довгостроковим».

3. Вправа «Ознаки того, що дитина зазнає онлайн-насильства»

Мета: формувати вміння виявляти ознаки наявності онлайн-насильства над дитиною.

Час: 30 хв.

Необхідні матеріали: 2 аркуші для фліпчарту із намальованої дитиною, 2 пари карток до вправи (Додаток 1.3.2), скотч.

Хід проведення:

Тренер/тренерка об'єднує учасників у дві групи, роздає кожній групі аркуші для фліпчарту із намальованою дитиною, картки та скотч. Завдання кожної групи – проаналізувати отримані картки, з них обрати та наклеїти на аркуші для фліпчарту ті індикатори, які будуть свідчити про те, що дитина зазнає онлайн-насильства.

Після завершення виконання вправи кожна група презентує свої результати, після чого відбувається загальне обговорення.

Далі тренер/тренерка підбиває підсумок:

«Отже, ознаками того, що дитина потрапила у небезпечну ситуацію, можуть бути:

- *Постійне приховування телефону.*
- *Перегорнутий телефон екраном донизу.*
- *Встановлення паролів на всі месенджери.*
- *Зміна поведінки або емоційних реакцій після користування телефоном або гаджетами.*
- *Зниження навчальної успішності.*
- *Погіршення стосунків з батьками, вчителями та друзями.*
- *Уникання розмов про те, чим дитина займається в телефоні або на комп'ютері.*
- *Замкненість.*
- *Бажання припинити користування телефоном або гаджетом.*
- *Постійна збентеженість, страх або тривожність.*
- *Проблеми зі сном або апетитом.*
- *Спроби суїциду.*
- *Фіксація на спілкуванні в онлайні з певною особою (надмірна значущість цього спілкування) та ізоляція від спілкування офлайн.*

Заклопотаним дорослим, як батькам, так і вчителям, може бути складно зрозуміти, що зміни в поведінці дитини спричиненні онлайн-насильством. Важливо бути уважними до дитини, помічати та аналізувати можливі причини змін у її поведінці».

Запитання для обговорення:

- *Чим корисна ця вправа?*
- *Які висновки ви можете зробити за результатами виконання цієї вправи?*
- *Що важливо враховувати у разі виявлення дітей, які зазнали насильства в онлайн-середовищі?*

Тестові питання до теми:

1. Які є фази вчинення онлайн-насильства кривдником?

А) фаза формування дружби, фаза формування взаємин, фаза оцінки ризику, фаза ізолювання, інтимна фаза;

Б) фаза фантазування, фаза вибору ізолювання, фаза акту насильства, фаза збереження секретності;

В) фаза виникнення суперечностей, фаза наростання напруги, фаза розрядки, фаза налагодження стосунків.

2. Що НЕ належить до ознак того, що дитина зазнає онлайн-насильства?

А) дитина постійно ховає телефон та перегортає телефон екраном донизу;

Б) дитина має бажання припинити користування телефоном або гаджетом;

В) дитина має акаунт, який не відповідає її реальному життю.

3. Що належить до ризиків, з якими може стикнутися дитина в інтернеті?

А) швидкий доступ до інформації;

Б) відсутність цензури;

В) можливість спілкуватися з друзями та близькими.

4. Що належить до переваг користування інтернетом?

А) дитина може отримати безперешкодно доступ до будь-якої інформації;

Б) можливість отримувати послуги спеціалістів онлайн;

В) заміна живого спілкування.

5. Чи правильне твердження: «Діти самі винні у тому, що можуть втрапити у небезпечну ситуацію онлайн»?

А) твердження правильне, бо дитина сама має розуміти небезпеки в інтернеті;

Б) твердження неправильне, бо відповідальність завжди буде на кривднику;

В) твердження неправильне, бо, окрім дитини, також відповідальність несуть батьки.

Ключі-відповіді:

1. А; 2. В; 3. Б; 4. Б; 5. Б.

Додаток 1.3.1

Інформація для підбиття підсумків до вправи

Можливості, які отримує дитина в інтернеті:

- Швидке спілкування з однолітками та батьками.
- Доступ до нових знайомств без фізичного контакту.
- Доступ до великої кількості інформації.
- Дистанційне навчання.
- Опанування різних навичок за допомогою різних каналів (малювання, ліплення, автомеханіка тощо).
- Ігри та розваги.
- Працювати віддалено (за згодою батьків).
- Ведення блогів.
- Отримання послуг (наприклад психолога).
- Придбання товарів.

Ризики кіберпростору:

- Віруси.
- Шахрайство (пропозиції товарів або збір коштів).
- Відсутність цензури (ненормативна лексика, пропаганда культу жорстокості та насильства тощо).
- Шкідливий контент (акти насильства, порнографія, висвітлення суїцидів, виготовлення наркотичних засобів тощо).
- Залежності (наприклад інтернет-залежність, порнографічна залежність, ігроманія тощо).
- Заміна живого спілкування віртуальним.
- Хепі-слепінг (створення насильницького контенту та його розміщення в інтернеті заради розваг).
- Тролінг (розміщення провокативних повідомлень з метою спричинення конфлікту або цькувань).
- Флеймінг (обмін гнівними повідомленнями із запальними репліками між двома або більше особами у чатах, в коментарях або на форумах).
- Секстинг (пересилання особистих фотографій, повідомлень інтимного змісту).
- Ошуканство (наприклад виманювання персональної інформації з метою її розповсюдження у мережі).
- Відчуження або ізоляція (наприклад видалення учасника із чату класу).
- Самозванство (створення аналогічного акаунту з метою шахрайства або реалізації насильницьких дій).

Додаток 1.3.2

Картки до вправи

Дитина весела
Дитина просить батьків допомогти знімати відео для TikTok
Постійно ховає телефон
Має багато друзів
Перегортає телефон екраном донизу
Постійно бере активну участь у шкільному житті
Встановлює паролі на всі месенджери
Гарно навчається
Зміна поведінки або емоційних реакцій після використання телефону або гаджету
Зниження навчальної успішності
Уникання розмов про те, що дитина робить в телефоні або на комп'ютері
Погіршення стосунків з батьками, вчителями, друзями
Замкненість
Відвідує гуртки
Бажання припинити користування телефоном або гаджетом
Наявність адекватної самооцінки
Наявність планів на майбутнє
Розвиток різних навичок
Моє добрі та близькі стосунки з батьками
Постійна збентеженість, страх або тривожність
Проблеми зі сном або апетитом
Наявність фізичної активності
Спроби суїциду
Ділиться та обговорює з батьками інформацію, отриману з інтернету
Відкритість у спілкуванні з іншими
Навчає батьків користуватися різними застосунками у телефоні або гаджеті
Наявність великої кількості підписників у соціальних мережах
Фіксація на спілкуванні онлайн з певною особою (надмірна значущість цього спілкування) та ізоляція від спілкування офлайн

ТЕМА 1.4. Базові правила та підходи до кібергігієни (цифрової безпеки)

Мета: сформувати розуміння змісту кібергігієни та засвоїти окремі інструменти її забезпечення.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Що таке кібергігієна?	Інформаційне повідомлення	10 хв	Комп'ютер, мультимедійне обладнання.
2.	Налаштування доступу в мережу через VPN	Індивідуальна робота	20 хв	Комп'ютери для учасників з доступом до мережі інтернет, Додаток 1.4.1
3.	Безпечний перегляд вебсторінок	Індивідуальна робота	20 хв	Комп'ютери для учасників з доступом до мережі інтернет
4.	Парольний менеджер	Індивідуальна робота	30 хв	Комп'ютери для учасників з доступом до мережі інтернет, Додаток 1.4.2
5.	Висновки	Мозковий штурм	10 хв	

ХІД ЗАНЯТТЯ

1. Інформаційне повідомлення «Що таке кібергігієна?»

Мета: розглянути зміст поняття «кібергігієна».

Час: 10 хв.

Необхідні матеріали: комп'ютер, мультимедійне обладнання.

Хід проведення:

Тренер/тренерка звертається до учасників:

«Сьогодні безпека роботи з інформацією є актуальною як ніколи. Зростаючі кібератаки на державні та приватні підприємства, установи й організації тільки посилюють цей тренд. Окрема категорія загроз стосується громадян, які дедалі частіше стають об'єктом прискіпливої уваги правопорушників. Враховуючи це, поступово набуває поширення концепція необхідності самостійного дотримання елементарних правил безпеки користувачами. Такий підхід значно посилює систему колективної безпеки суспільства та держави загалом. Агентство Європейського Союзу з мережної та інформаційної безпеки (European Union Agency for Network and Information Security) зазначає, що кібергігієна повинна розглядатися так само, як особиста гігієна. Після належної інтеграції в організацію кібергігієна має стати простою повсякденною процедурою, яка забезпечить оптимальний стан кіберздоров'я організації.

Порушення правил кібергігієни може призвести до згубних наслідків не лише для окремої людини. Часто від дій зловмисників страждає й роботодавець. Навіть великі держави можуть зазнати значної шкоди через необачне ставлення до вимог безпеки з боку одного з працівників. Порушники часто використовують окрему особу як шлях для проникнення на об'єкти критичної інфраструктури, викрадення чутливих державних даних і створення умов для скоординованих повномасштабних атак.

Отже, недотримання вимог кібергігієни може завдати значної матеріальної та моральної шкоди, а також суттєво вплинути на особисту репутацію.

У світі існує багато тлумачень слова «кібергігієна», які зазвичай відображають найбільш значущі аспекти цього терміну, важливі для конкретної галузі знань. Серед останніх оприлюднених визначень можна навести такі:

- *правила кібербезпеки, яких мають дотримуватися онлайн-користувачі для забезпечення цілісності та безпеки своїх персональних даних на мережевих пристроях від компрометації у разі кібератаки;*
- *сукупність практик, спрямованих на захист від негативного впливу ризиків, пов'язаних з кібербезпекою;*
- *способи заохочення користувачів комп'ютерних технологій до безпечної поведінки в інтернеті.*

Більш спрощена інтерпретація терміна «кібергігієна» представляє його як дотримання правил безпечної поведінки у кіберсфері. Ця поведінка обумовлена наявністю загроз, які виникають під час роботи користувачів з інформацією в електронному вигляді. Спроби реалізації загроз називаються атаками.

Як і на рибаловлі чи полюванні, зловмисники можуть заздалегідь обирати цілі, які вважають цікавими для себе, або ж розставити пастки, чекаючи, поки постраждала особа потрапить в них. Це саме стосується ситуацій, коли порушники випадково обирають особу, стосовно якої намагаються реалізувати свої наміри.

Виділяють декілька типів інформаційних атак: соціальна інженерія, отримання віддаленого доступу за допомогою вірусів, вплив на інфраструктуру стільникового зв'язку, маніпуляція через медіа, атаки відмови в обслуговуванні, атаки на енергетичні системи та комунікації, політичний спамінг, атаки на системи управління та провайдерів тощо.

Перед нападом зловмисники часто здійснюють підготовчі дії, які можуть включати підшукування працездатних схем нападу, збирання інформації про постраждалу особу різними способами, створення умов для реалізації атаки.

Для мінімізації ризику успішної реалізації таких атак і потрібна кібергігієна. Фактично це рутинний процес. Щоб полегшити його, необхідно використовувати спеціальний інструментарій. Якщо в класичній гігієні такими інструментами є мило, шампунь, зубні щітки тощо, то для забезпечення її кібернетичного аналогу використовуються спеціальні програми, такі як антивіруси, фаєрволи, захищені браузери та багато інших застосунків і сервісів.

Важливим моментом в роботі з інструментами кібергігієни є їх правильне застосування. Це можна порівняти з правильним підрізанням нігтів ножицями чи зачісування волосся гребінцем. З одного боку, все здається простим, але з іншого – необхідно чітко визначити для себе елементарний порядок дій з певними програмами, щоб уникнути проблем. Просте озброєння купою застосунків для захисту інформації зазвичай не приносить користі. Без знання правил роботи з такими програмами вони стають просто набором коду, який малоймовірно зможе забезпечити захист.

Також важливо пам'ятати, що чим меншою буде кількість інформації, яку ви хочете вберегти, тим менше вам потрібно буде вживати дій для її убезпечення. Тому під час створення фотознімків, написання повідомлень в мережі або спілкування телефоном з незнайомими та навіть знайомими людьми, задумайтеся про необхідність і можливі ризики використання певної інформації проти вас.

Саме тому рекомендується використовувати переваги інтернету щодо забезпечення анонімності та застосуванні вигаданих даних, особливо на мережевих ресурсах, безпеки

яких не можна бути впевненим. У разі атаки на вас, зловмисники зможуть отримати доступ лише до вигаданих даних, що створить додатковий захист від протиправних дій.

Не менш важливим принципом забезпечення кібергігієни є періодичне резервування даних. Ви можете використовувати мережеве резервування або дублювання даних на фізичних запам'ятовувальних пристроях. Це залежить від чутливості даних, які потрібно зберегти, та від ваших знань у цій сфері. Наприклад, другорядні дані цілком можуть бути перенесені у хмару, що дасть змогу скоротити обсяг інформації, яка потребує захисту на локальних пристроях, і так зберегти їх у безпеці.

Найкращий варіант – зробити кібергігієну своєю повсякденною звичкою. Цей процес не потребує значних витрат коштів і часу. Згодом ви звикнете до виконання відповідних процедур і відчуєте їх корисність як в особистих, так і в службових справах».

2. Індивідуальна робота «Налаштування доступу в мережу через VPN»

Мета: відпрацювати навички організації безпечного з'єднання в мережі.

Час: 20 хв.

Ресурси: комп'ютери для учасників з доступом до інтернету (зокрема сайтів vpnbook.com, protonvpn.com), Додаток 1.4.1.

Хід проведення:

Тренер/тренерка звертається до учасників:

«Для налагодження безпечного з'єднання з віддаленими ресурсами може бути застосовано проміжні захисні механізми, такі як VPN-сервери. VPN-сервери надають організації повноцінне захищене з'єднання між користувачем та відповідними ресурсами. Для користування VPN-сервером потрібно знати його налаштування та відповідні автентифікаційні дані».

Тренер/тренерка презентує учасникам інформацію із Додатка 1.4.1.

Після демонстрації учасники повинні самостійно відпрацювати щонайменше два способи налаштування VPN-з'єднання:

1) через налаштування параметрів мережевого підключення операційної системи;

2) за допомогою VPN Client.

Після встановлення з'єднання слід переконатися у зміні параметрів виходу в мережу (наприклад скориставшись сайтом 2ip.ua).

3. Індивідуальна робота «Безпечний перегляд вебсторінок»

Мета: відпрацювати навички організації безпечного з'єднання в мережі.

Час: 20 хв.

Ресурси: комп'ютери для учасників з доступом до мережі інтернету (зокрема сайтів vpnbook.com, protonvpn.com).

Хід проведення:

Тренер/тренерка звертається до учасників:

«Перегляд вебсторінок зазвичай здійснюється за допомогою програм-браузерів, найпоширенішими серед яких є Chrome та Firefox. В усіх сучасних браузерах є меню налаштувань, де можна обрати безпеку та конфіденційність (Рис. 1).

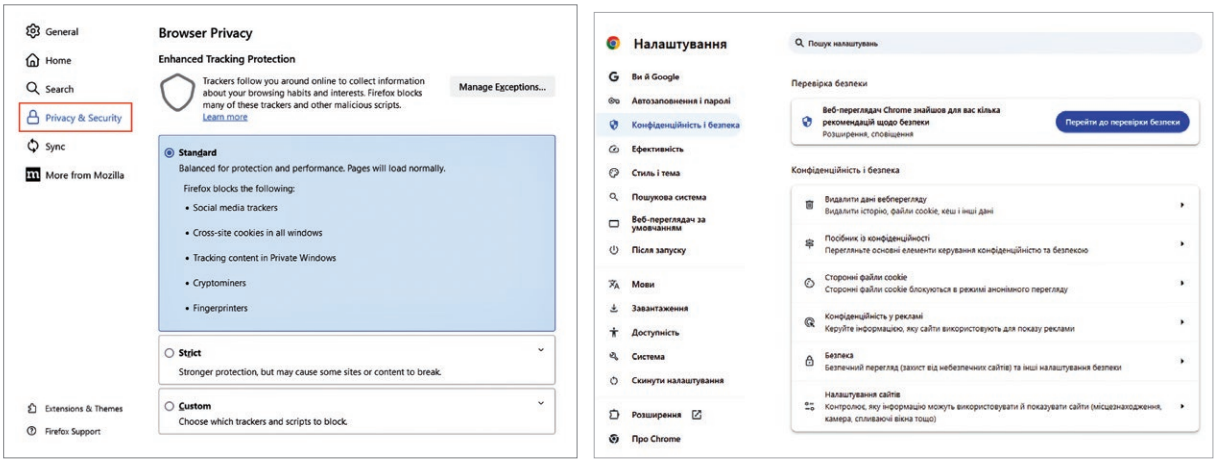


Рис. 1. Зліва направо налаштування безпеки у браузерах Firefox та Chrome

Якщо налаштування безпеки не повною мірою влаштовують користувача, можна встановити плагіни (застосунки), підключені до основної програми. Популярними такими плагінами є:

- *AdBlock для блокування спливаючих вікон (https://adblockplus.org/ru/download);*
- *uBlock Origin для фільтрації контенту, зокрема блокування спливаючих вікон (https://github.com/gorhill/uBlock/);*
- *Cookie AutoDelete для контролю кукі-файлів (https://github.com/Cookie-AutoDelete/Cookie-AutoDelete);*
- *User-Agent Switcher для зміни параметру User-Agent браузера (https://addon.com/useragent-switcher.html);*
- *RequestPolicy для блокування міжсайтових запитів (https://www.requestpolicy.com/);*
- *RequestPolicy для блокування міжсайтових запитів (https://www.requestpolicy.com/);*
- *Click&Clean для видалення тимчасових файлів у браузері* (https://www.hotcleaner.com/).

Після демонстрації учасникам потрібно самостійно налаштувати параметри безпеки та конфіденційності браузера, пояснити свій вибір налаштувань, встановити додаткові плагіни, описані в матеріалах до заняття».

4. Індивідуальна робота «Парольний менеджер»

Мета: навчитися безпечно зберігати складні паролі для різних ресурсів.

Час: 30 хв.

Ресурси: комп'ютери для учасників з доступом до інтернету, Додаток 1.4.2.

Хід проведення:

Тренер/тренерка звертається до учасників із питанням: *«Які ви знаєте правила до створення надійного паролю?»* Слід наголосити, що паролі є першою лінією захисту облікових записів, які можуть містити особисту, фінансову або корпоративну інформацію. Створення надійних паролів та використання парольного менеджера допомагають захистити дані від несанкціонованого доступу. Надійні паролі перешкоджають зломам, а парольні менеджери

забезпечують зручне і безпечне керування ними, що значно підвищує загальний рівень кібербезпеки.

На наступному етапі тренер/тренерка звертається до учасників із питанням: «*Де ви зберігаєте свої паролі?*» Після відповідей учасників тренер/тренерка розповідає учасникам про парольний менеджер як інструмент для безпечного зберігання та генерування паролей. Далі учасникам потрібно індивідуально здійснити послідовність дій, зазначених у Додатку 1.4.2.

Запитання для обговорення:

- *Які існують вимоги до створення надійного паролю?*
- *Чи знали ви про існування парольного менеджеру?*
- *Які, на вашу думку, є переваги та недоліки використання парольного менеджера?*

5. Мозковий штурм «Висновки»

Мета: сформулювати основні правила кібергігієни.

Час: 10 хв.

Хід проведення:

Тренер/тренерка просить кожного учасника сформулювати одне правило кібергігієни.

Приклад підсумкового переліку:

1. Завжди критично ставтеся до відомостей, отриманих з інтернету.
2. Регулярно здійснюйте резервування важливих даних і не зберігайте все в одному місці.
3. Користуйтеся останніми версіями програмного забезпечення та регулярно проводьте оновлення.
4. Залишайте якомога менше персональних даних в інтернеті.
5. Дотримуйтесь вимог парольного захисту та використовуйте двофакторну автентифікацію.
6. Використовуйте антивірусне програмне забезпеченням та інші засоби захисту.
7. У разі компрометації чутливих даних, повідомте про це уповноважену особу та вживайте заходів убезпечення решти відомостей.
8. Максимально обмежте доступ сторонніх осіб до терміналів, за якими ви працюєте.
9. Використовуйте лише перевірені носії інформації.
10. Регулярно оновлюйте свої знання у сфері кібергігієни.

Тестові питання до теми:

1. Що таке кібергігієна?

А) резервування даних;

Б) забезпечення анонімності та використання вигаданих даних;

В) дотримання правил безпечної поведінки у кіберсфері;

Г) одержання віддаленого доступу за допомогою вірусів.

2. Яке (які) поняття стосуються кібергігієни?

А) кібербезпека;

Б) кібербезпека та інформаційна безпека;

В) інформаційна безпека;

Г) жодне не стосується.

3. Який з наведених паролів є найбільш безпечним?

А) 123456123;

Б) password;

В) mfjie@#&HHjdf!!mI&8@##43;

Г) Salenko_2001_06_01.

4. Як доцільно організовувати парольний захист?

А) окремий пароль для кожного ресурсу;

Б) дуже складний пароль, який використовувати для всіх ресурсів;

В) завжди використовувати складний набір символів і знаків, який слід запам'ятати, із додаванням певного символу в пароль для кожного ресурсу в мережі;

Г) занотовувати паролі у блокноті, який зберігати на робочому місці.

5. Що відбудеться, якщо натиснути комбінацію клавіш Ctrl+Shift+N у браузері Chrome або Ctrl+Shift+P у браузері Firefox?

А) відкриється нове анонімне вікно;

Б) відкриється вікно друку поточної сторінки;

В) відкриється вікно очищення історії;

Г) відкриється гра «Динозаврик».

Ключі-відповіді:

1. В; 2. Б; 3. В; 4. А; 5. А.

Додаток 1.4.1

Налаштування доступу в мережу через VPN

Зазвичай налаштування відповідного підключення можливе і без встановлення додаткового програмного забезпечення. Для цього, наприклад, у системі Windows 10 слід відкрити «Центр управління мережами та спільним доступом», створивши нове з'єднання (Рис. 1).

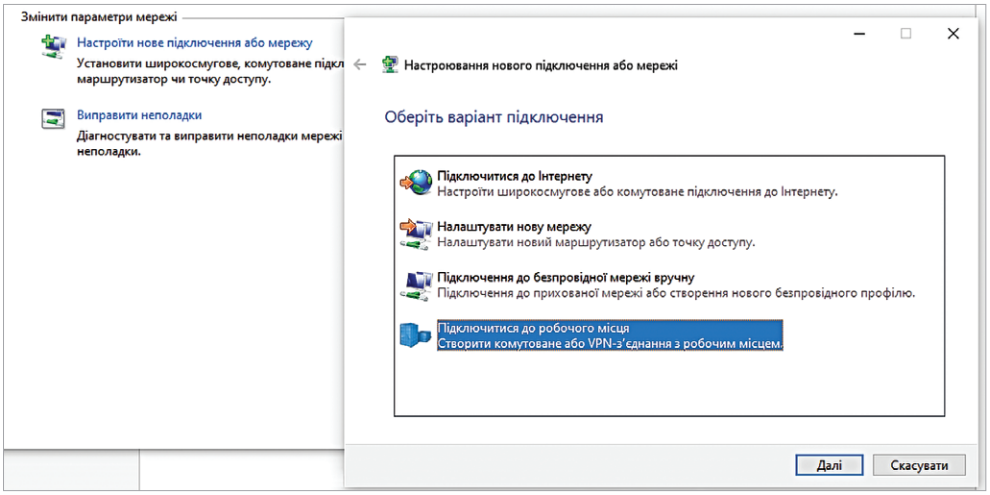


Рис. 1. Налаштування нового з'єднання в операційній системі

Потім вказати адресу VPN-сервера та перейти до розділу «Зміна параметрів адаптера», двічі клацнувши на ліву кнопку миші, ввести ім'я користувача, складний пароль і дочекатися з'єднання.

Універсальним способом налаштування VPN-з'єднання є використання спеціальних програм для організації такої діяльності. З цією метою може бути використано, наприклад, безоплатний застосунок OpenVPN
(https://openvpn.net/community-downloads/)
або Proton VPN (https://protonvpn.com/).

Розглянемо схему підключення Proton VPN. У застосунку на сайті (protonvpn.com) слід завести обліковий запис, завантажити відповідний застосунок операційної системи (account.protonvpn.com/downloads) та авторизуватися в ньому. Далі потрібно авторизуватися у завантаженому застосунку та просто обрати потрібний спосіб підключення (Рис. 2).

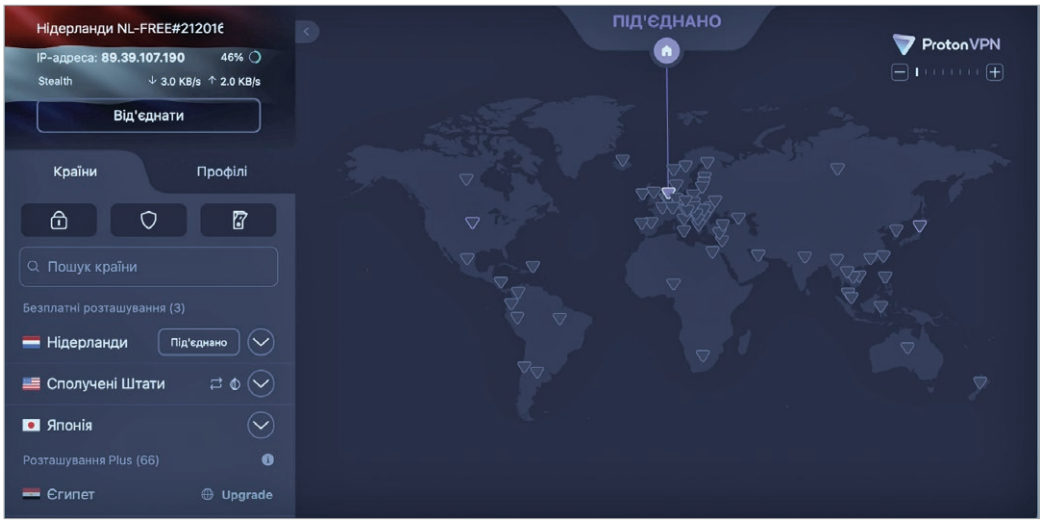


Рис. 2. Зовнішній вигляд клієнта Proton VPN

Додаток 1.4.2

Парольний менеджер

Завантажити (https://keepass.info/index.html), встановити та запустити парольний менеджер KeePass Password Safe (Рис. 1).

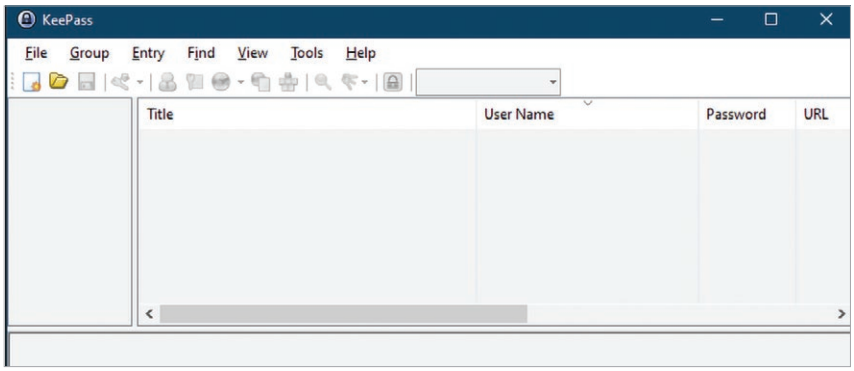


Рис. 1. Головне вікно KeePass

Комбінацією клавіш (Ctrl+N) створити та вказати місце зберігання файлу нової бази паролів (Рис. 2).

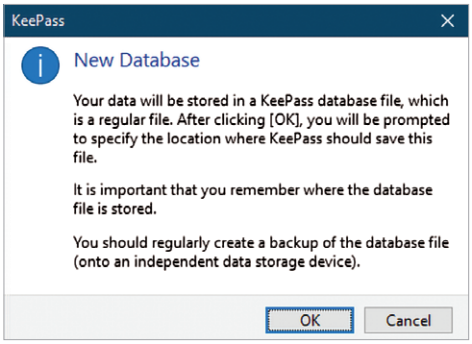


Рис. 2. Повідомлення щодо створення нової бази паролів

Придумати та запам'ятати майстер-пароль (парольну фразу) довжиною не менше десяти символів із використанням маленьких та великих літер, цифр та спеціальних символів. Ввести майстер-пароль (парольну фразу) та вибрати ім'я для бази паролів (Рис. 3). Додатково можна роздрукувати основні дані щодо місця зберігання основної бази паролів, її резервної копії та підказки щодо майстер-пароля (Рис. 4).

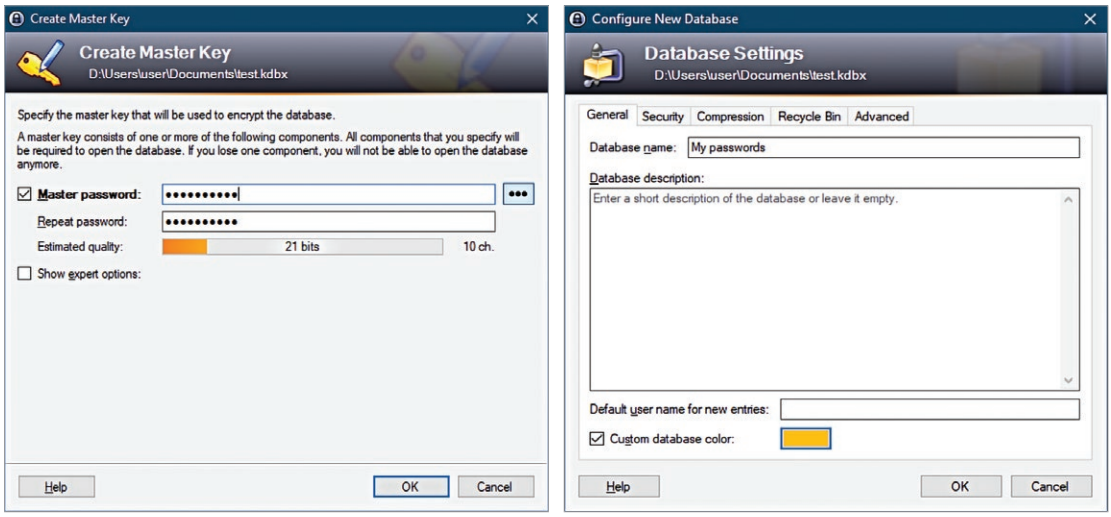


Рис. 3. Створення майстер-паролю та налаштування бази

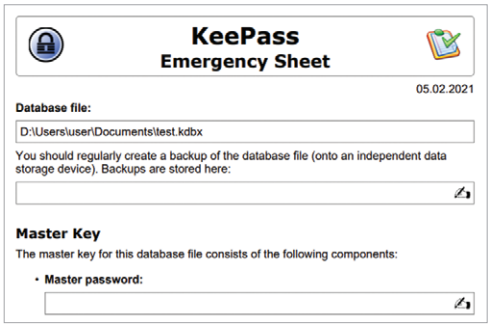


Рис. 4. Пам'ятка щодо місця зберігання основної бази паролів, її резервної копії та підказки щодо майстер-пароля

В основному вікні KeePass зліва обрати папку «eMail», створити новий запис (комбінація клавіш Ctrl+I), заповнити поля для свого поштового облікового запису, перейти у налаштування Генератора паролів і обрати довжину пароля та абетку символів, з яких буде генеруватися пароль (Рис. 5). Завершити редагування, зберегти зміни (комбінація клавіш Ctrl+S) і переглянути створений запис (Рис. 6).

Зверніть увагу, що деякі вебсервіси забороняють наявність у паролі спеціальних символів. У такому разі потрібно після генерації паролю вручну видалити спеціальні символи або виключити їх із абетки налаштувань Генератора паролів.

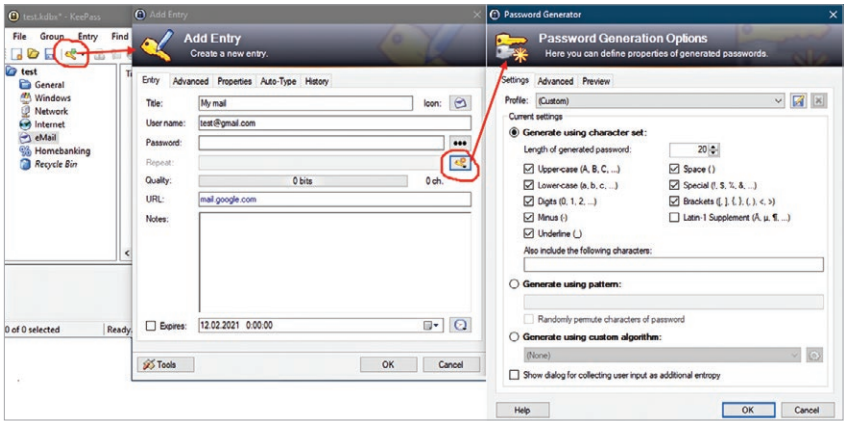


Рис. 5. Створення і налаштування параметрів нового запису у базі паролів

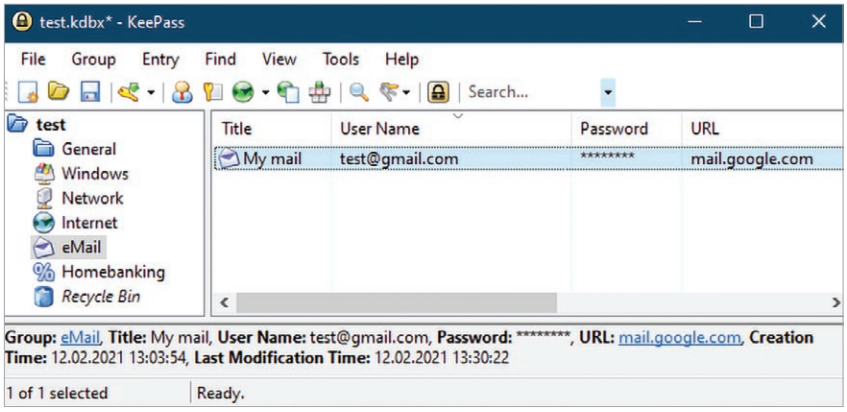


Рис. 6. Створений запис у базі паролів

Пройти автентифікацію в поштовому сервісі, використовуючи менеджер паролів. Для цього в KeePass обирається відповідний запис та почергово копіюється у буфер логін (комбінація клавіш Ctrl+B) та пароль (комбінація клавіш Ctrl+C), які почергово вставляються у відповідні поля форми автентифікації поштового сервісу.

ТЕМА 1.5. Безпека мобільних пристроїв, електронної пошти, акаунту в соціальних мережах

Мета: навчити базовим навичкам щодо безпеки мобільних пристроїв, електронної пошти, акаунту в соціальних мережах.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Асоціації	Обговорення	20 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери
2.	Перевірка паролів	Індивідуальна робота	10 хв	Мультимедійне обладнання, інтернет
3.	Перевірка електронних пошт щодо витоку даних	Індивідуальна робота	20 хв	Мультимедійне обладнання, інтернет
4.	Перевірка та встановлення двоетапної перевірки	Індивідуальна робота	20 хв	Мультимедійне обладнання, інтернет, Додаток 1.5.1
5.	Перевірка мобільних додатків на трекери	Індивідуальна робота	20 хв	Мультимедійне обладнання, інтернет

ХІД ЗАНЯТТЯ

1. Обговорення «Асоціації»

Мета: визначення рівня інформованості учасників щодо загроз, пов'язаних із безпекою мобільних пристроїв, електронної пошти, акаунту в соціальних мережах.

Час: 20 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери.

Хід проведення:

Тренер/тренерка на аркуші фліпчарту пише: «*Загрози для мобільних пристроїв, електронної пошти, акаунту в соціальних мережах*» і пропонує учасникам озвучити асоціації, які виникають у них.

До уваги тренера/тренерки!

Важливо спонукати учасників називати абсолютно всі асоціації, які виникають у них, як позитивні, так і негативні.

Тренер/тренерка записує всі відповіді, які надають учасники.

Запитання для обговорення:

- *Чи складно було знайти відповідну асоціацію?*
- *Чи пов'язані якісь із цих асоціацій з вашим власним досвідом?*

Після обговорення тренер/тренерка зазначає: «*Для того, щоб мінімізувати наявні ризики, необхідно володіти базовими навичками, про які ми будемо говорити далі*».

2. Індивідуальна робота «Перевірка паролів»

Мета: посилити парольну безпеку учасників.

Час: 10 хв.

Необхідні матеріали: мультимедійне обладнання, інтернет.

Хід проведення:

Тренер/тренерка пропонує перевірити рівень безпеки паролів учасників, скориставшись своїми смартфонами:

- *«зайдіть за лінком https://www.security.org/how-secure-is-my-password/;*
- *у графу «enter password» введіть один із паролів, яким ви користуєтеся в особистих цілях або в роботі, й одразу побачите, скільки часу потрібно для його зламу.*

Порівняйте ваші паролі, наприклад з такими: 1111, 1234567, 12345qaz, qwerty, кіт#16Портрет. Якщо пароль, яким ви зараз користуєтеся, можна легко зламати, то змініть його, скориставшись порадами нижче.

- ***Створюйте для кожного облікового запису окремий пароль.*** Не використовуйте всюди однакові та найпростіші паролі. Пароль 1111 є найпоширенішим у світі, тож зламати його можна миттєво. Рік народження, як пароль, також є небезпечним, тож надійним можна вважати той, що містить щонайменше 16 та більше знаків. Зазначимо, що деякі системи можуть вимагати мінімум 6–10 знаків, зокрема певну кількість великих та малих літер, цифр, позначок.
- ***Тримайте паролі в таємниці.*** Не залишайте записки з паролями соцмереж, електронної пошти, робочих ресурсів поруч із комп'ютером або в шухляді робочого столу. Запам'ятовуйте їх або зберігайте зашифрованими в непередбачених шахраями місцях. Чим складніші будуть паролі, тим складніше їх буде зламати, наприклад, «Фіолетовий сніг#48Кандидат$table+sobaka=>(T@8l3+S0ba4ka) та подібні. Підвищить цифрову безпеку вихід з пошти чи з інших акаунтів на завершення робочого дня.
- ***Періодично змінюйте паролі.*** Оновлюйте їх хоча б щопівроку, а найкраще – кожні три місяці. Не вводьте логіни й паролі в громадських місцях з відеоспостереженням. А якщо заходили у свій акаунт з чужого пристрою – змініть пароль.

*Створити надійний пароль допоможе генератор паролів на сайті Департаменту кіберполіції Національної поліції України (*https://cyberpolice.gov.ua/generate-password/*), коли ви визначите необхідну кількість символів, додаткові знаки й цифри та зробите позначки на відповідних полях. Якщо переймаєтеся безпекою створеного пароля, то можете взяти за основу запропонований генератором, змінивши в ньому деякі символи».*

3. Індивідуальна робота «Перевірка електронних пошт щодо витоку даних»

Мета: перевірити та убезпечити електронні пошти від витоку даних.

Час: 20 хв.

Необхідні матеріали: мультимедійне обладнання, інтернет.

Хід проведення:

«Своєчасно виявляти, реагувати та уникнути потенційних загроз допомагає також перевірка ресурсів на витік даних. Пропонуємо перевірити, чи відбувались витоки з вашої електронної пошти:

- *перейдіть на спеціалізований сайт https://haveibeenpwned.com/?utm_source=canva&utm_medium=iframely;*

- *у графі «email address» введіть адресу електронної пошти, якою ви користуєтеся в особистому житті або в роботі, клацніть на «pawnd?» і побачите, чи був витік даних».*

Після перевірки запитайте в учасників про їхні результати. Якщо виявлено злами, обов'язково змініть пароль та підпишіться на оновлення інформації про витік даних.

4. Індивідуальна робота «Перевірка та встановлення двоетапної перевірки»

Мета: перевірити та убезпечити усі акаунти від зламів та витоку даних.

Час: 20 хв.

Необхідні матеріали: мультимедійне обладнання, інтернет, Додаток 1.5.1.

Хід проведення:

Тренер/тренерка пояснює учасникам, що таке двоетапна перевірка:

«Двофакторна автентифікація також є важливим інструментом у захисті онлайн-акаунтів від несанкціонованого доступу, що значно підвищує рівень безпеки, вимагаючи від користувача кілька доказів автентифікації.

Це можуть бути:

- *інформація, відома лише одній особі (наприклад пароль чи пін-код);*
- *прилад, що належить конкретній людині (наприклад електронна або магнітна карта, токен, флеш-пам'ять);*
- *властивість (наприклад біометрія – природні відмінності обличчя, відбитки пальців, райдужна оболонка очей).*

Використання двофакторної автентифікації є рекомендованою практикою для всіх користувачів, особливо для тих, хто зберігає конфіденційну інформацію або має доступ до важливих онлайн-ресурсів. Налаштувати її можна у всіх месенджерах та соціальних мережах. Це буде додатковим захистом доступу до комп'ютера чи гаджета».

Далі тренер/тренерка ознайомлює учасників із інструкцією щодо двофакторної автентифікації, яка міститься у Додатку 1.5.1.

Після презентації тренера/тренерки учасники індивідуально налаштовують двофакторну автентифікацію згідно з інструкцією у тих месенджерах, які вони використовують.

5. Індивідуальна робота «Перевірка мобільних додатків на трекери»

Мета: навчити учасників перевірці програм та застосунків щодо «стеження».

Час: 20 хв.

Необхідні матеріали: мультимедійне обладнання, інтернет.

Хід проведення:

Тренер/тренерка пропонує перевірити 5-10 додатків на спеціалізованому сайті https://reports.exodus-privacy.eu.org/en/ щодо стеження. Наприклад Вайбер, Дія, Телеграм, Фейсбук.

Після перевірки доцільно запитати в учасників про їхні результати і попросити зайти в налаштування цих застосунків і, наприклад, забрати доступ програм до геолокацій чи мікрофону.

Також поясніть, що якщо мобільний застосунок відстежує багато даних, його можна видалити, або використовувати цю програму через браузер.

Тестові питання до теми:

1. Чи можна перевірити на спеціалізованих сайтах, наскільки безпечний ваш пароль?

А) так;

Б) ні.

2. Як ви охарактеризуєте такі паролі: 1111, 1234567, 12345qaz, qwerty?

А) слабкі;

Б) міцні;

В) звичайні.

3. Міцний пароль має містити:

А) не менше 16 знаків;

Б) великі та малі літери;

В) цифри та знаки;

Г) усі відповіді правильні.

4. Чи можна перевірити на спеціалізованому сайті, чи траплялись витоки або злами електронних пошт?

А) так;

Б) ні

5. Двофакторну аутентифікацію можна налаштувати:

А) лише у месенджерах;

Б) лише у соціальних мережах;

В) у всіх месенджерах та соціальних мережах.

Ключі-відповіді:

1. А; 2. А; 3. Г; 4. А; 5. В.

Додаток 1.5.1

Перевірка та встановлення двофакторної автентифікації

ТЕЛЕГРАМ:

Відеопояснення: https://youtu.be/uoX2qs0-xY4.

Пояснення: https://yak.dslua.org/services/telegram/2fa/.

1 крок. Відкриваємо застосунок Телеграм.

2 крок. Заходимо в налаштування застосунку.

3 крок. Обираємо розділ «Приватність та безпека».

4 крок. Клацаємо на «Двоетапна перевірка» та на «Встановити додатковий пароль».

5 крок. Придумуємо складний пароль та клацаємо на відповідну позначку.

6 крок. Встановлюємо підказку на випадок, якщо пароль забули.

7 крок. Вводимо електронну пошту, якщо бажаєте змінити або скинути пароль для відновлення акаунту.

Вітаємо, ви встановили двофакторну автентифікацію в Телеграм! Тепер ваші дані під надійним захистом.

INSTAGRAM:

Пояснення: https://yak.dslua.org/services/instagram/2fa.

Відеопояснення: https://youtu.be/Y7kVPQzJK5M.

1 крок. Заходимо в застосунок Інстаграм.

2 крок. Заходимо в налаштування застосунку.

3 крок. Обираємо розділ «Безпека».

4 крок. Клацаємо на «Двоетапна перевірка».

5 крок. Клацаємо на «Почати».

6 крок. Вибираємо або встановлюємо для автентифікації застосунок (серед найпопулярніших: Google Authenticator або та Authenticator App (iOS), що можна скачати в Play Market (Android) або App store (iOS). Якщо автентифікатор встановлено – застосунки синхронізуються та з'являється код для Instagram.

7 крок. Копіюємо в застосунку обраний код та повертаємось в Instagram.

8 крок. Вставляємо код та клацаємо на «Готово».

Вітаємо, ви встановили двофакторну автентифікацію в Instagram! Тепер ваші дані під надійним захистом.

SIGNAL:

Відеопояснення: https://youtu.be/M5fgb3eS310.

Пояснення: https://yak.dslua.org/services/signal/avtovydalennya/.

1 крок. Заходимо в застосунок Signal.

2 крок. Заходимо в налаштування застосунку.

3 крок. Обираємо розділ «Конфіденційність».

4 крок. Обираємо із переліку позицію «Блокування реєстрації».

5 крок. Придумуємо пароль та підтверджуємо пароль.

Вітаємо, ви встановили двофакторну автентифікацію в Signal! Тепер ваші дані під надійним захистом.

ТІК ТОК:

Відеопояснення: https://www.youtube.com/watch?v=JuW7cN2h22k.

1 крок. Заходимо в застосунок Тік Ток.

2 крок. Заходимо в налаштування застосунку.

3 крок. Обираємо розділ «Безпека».

4 крок. Обираємо із переліку позицію «Двоетапна перевірка».

5 крок. Оберіть бажаний спосіб для активації двофакторної автентифікації: SMS або електронна пошта.

6 крок. Дочекайтеся повідомлення з кодом на ваш телефон або листа на вказану електронну пошту і введіть отриманий код у застосунку для завершення налаштування.

Вітаємо, ви встановили двофакторну автентифікацію в Тік Току! Тепер ваші дані під надійним захистом.

GMAIL:

Відеопояснення: httpss://youtu.be/ldof5C8Ls5c.

Пояснення: https://yak.dslua.org/services/gmail/2fa/.

Активний лінк для встановлення двофакторної автентифікації:
https://safety.google/authentication/?fbclid=IwAR3SOplrJT2-.

1 крок. Заходимо до налаштування облікового запису. У «вікні» Gmail клацаємо на фото або ініціали користувача, розміщені у верхньому правому куті. Коли з'явиться наступне «вікно», обираємо кнопку «Обліковий запис Google».

2 крок. Далі обираємо вкладку «Безпека».

3 крок. «Вікно» налаштувань безпеки гортаємо вниз до розділу «Вхід в обліковий запис Google». Знаходимо нижче напис «Двоетапна перевірка» та клацаємо на нього.

4 крок. Далі клацаємо на кнопку «Розпочати» та на запит Google вводимо пароль свого облікового запису.

5 крок. Так потрапляємо до «вікна» налаштування двофакторної автентифікації. Якщо ви вже використовуєте цей обліковий запис на мобільному пристрої, Google запропонує вам другий фактор – «Отримувати сповіщення від Google».

Вітаємо, ви встановили двофакторну автентифікацію в Gmail! Тепер ваші дані під надійним захистом.

UKR.NET. Покрокова інструкція:

1 крок. Із сайту Ukr.net входимо до особистого поштового акаунту за своїм логіном та паролем.

2 крок. У верхньому правому куті екрану клацаємо на свій профіль (ім'я або аватар).

3 крок. Залежно від інтерфейсу, обираємо «Налаштування» або «Безпека».

4 крок. Шукаємо опцію увімкнення двофакторної автентифікації (може бути розміщена під розділом «Додаткова безпека» або подібним).

5 крок. Клацаємо на «Увімкнення двофакторної автентифікації». Реагуємо на пропозицію зробити це через SMS або через застосунок (Google Authenticator, Authy тощо) для генерації одноразового коду на підтвердження особи користувача під час входу в обліковий запис. Якщо обрано метод SMS, відправляємо номер свого телефону та чекаємо код підтвердження, який вводимо у відповідне поле. Якщо обрано застосунок – скануємо QR-код за допомогою застосунку, встановленого на смартфоні (наприклад Google Authenticator). Вводимо код у відповідне поле на сайті.

Вітаємо, ви встановили двофакторну автентифікацію в Ukr.net! Тепер ваші дані під надійним захистом.

ФЕЙСБУК:

Відеопояснення: https://youtu.be/DxwGczekFqc.

Пояснення: https://yak.dslua.org/services/facebook/2fa/.

Активний лінк для встановлення двофакторної автентифікації:
https://www.facebook.com/security/2fac/factors/recovery-code/.

1 крок. Заходимо в застосунок Фейсбук.

2 крок. Заходимо в налаштування застосунку.

3 крок. Обираємо розділ «Налаштування та конфіденційність».

4 крок. Обираємо вкладку «Безпека й авторизація». Гортаємо сторінку вниз, поки не побачимо напис «Використання двоетапної перевірки». Клацаємо на кнопку «Редагувати».

5 крок. Шукаємо вікно з поясненням двофакторної автентифікації. Обираємо один із запропонованих засобів захисту (sms або застосунок). Фейсбук може попросити ввести пароль для переконання, що дієте ви, а не зловмисник.

6 крок. Щоб отримати другий фактор за допомогою sms, обираємо цю опцію та клацаємо на «Далі». Якщо у **вашому обліковому записі** є номер вашого телефону, ви можете вказати його або інший для отримання коду підтвердження. Вводимо номер в наступне вікно.

Вітаємо, ви встановили двофакторну автентифікацію в Фейсбуці! Тепер ваші дані під надійним захистом.

X (Твіттер):

Пояснення: https://yak.dslua.org/services/twitter/2fa/.

Активний лінк для встановлення двофакторної автентифікації: https://twitter.com/settings/account.

1 крок. Заходимо в застосунок X (Твіттер).

2 крок. Заходимо в налаштування застосунку.

3 крок. Обираємо «Налаштування та конфіденційність».

4 крок. Обираємо вкладку «Профіль» (відкривається першою).

5 крок. У розділі «Безпека» знаходимо пункт «Підтвердження входу». Клацаємо на «Налаштуйте підтвердження входу».

6 крок. У «вікні» з поясненням, як працює двофакторна автентифікація, клацаємо на «Почати». X (Твіттер) надішле код на телефон, прив'язаний до вашого акаунта, який маємо ввести в наступне вікно.

Вітаємо, ви встановили двофакторну автентифікацію в X (Твіттер). Тепер ваші дані під надійним захистом.

ВОТСАП. Покрокова інструкція:

1 крок. Заходимо в застосунок Вотсап.

2 крок. Знаходимо налаштування (параметри) застосунку в нижньому правому кутку для iOS або у верхньому правому кутку – для Android.

3 крок. Обираємо «Обліковий запис».

4 крок. Обираємо «Двоетапна перевірка» та клацаємо на «Увімкнути».

5 крок. Застосунок запропонує створити 6-значний PIN-код, який слід запам'ятати. Потім клацаємо «Далі» та підтверджуємо створений PIN-код.

6 крок. Застосунок запропонує додати електронну пошту, щоб скористатися нею, якщо забудете PIN-код. Потім клацаємо на «Далі».

7 крок. Підтверджуємо адресу електронної пошти. Обираємо «Зберегти» або «Готово».

Вітаємо, ви встановили двофакторну автентифікацію у Вотсапі! Тепер ваші дані під надійним захистом.

ТЕМА 1.6. Персональні дані та особиста інформація в мережі: поняття, види інформації, способи отримання інформації в мережі. Способи захисту персональних даних в кіберпросторі

Мета: навчитися поводитись з персональними даними у кіберсфері.

Загальна тривалість: 4 академічні години (180 астрономічних хвилин).

План:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Що таке персональні дані та як з ними поводитись?	Інформаційне повідомлення	30 хв	Мультимедійне обладнання, Додаток 1.6.1
2.	Розв'язання задач	Робота в групах	30 хв	Комп'ютери для учасників з доступом до мережі інтернет, Додаток 1.6.2
3.	Чи скомпрометовані ваші персональні дані?	Індивідуальна робота	15 хв	Комп'ютери для учасників з доступом до мережі інтернет
4.	Пошук інформації про осіб	Індивідуальна робота	90 хв	Комп'ютери для учасників з доступом до мережі інтернет, Додаток 1.6.3
5.	Висновки	Вікторина	15 хв	Мультимедійне обладнання, доступ до мережі інтернет, Додаток 1.6.4

ХІД ЗАНЯТТЯ

1. Інформаційне повідомлення «Що таке персональні дані та як з ними поводитись?»

Мета: розглянути види, порядок поводження та захисту персональних даних.

Час: 30 хв.

Необхідні матеріали: мультимедійне обладнання, Додаток 1.6.1.

Хід проведення:

Тренер/тренерка презентує учасникам інформацію із Додатка 1.6.1 та відповідає на їхні запитання (у разі наявності).

До уваги тренера/тренерки!

Доцільно завчасно підготувати презентацію, використовуючи інформацію, яка міститься у Додатку 1.6.1 або під час інформаційного повідомлення занотовувати основні дані на аркуші паперу для фліпчарту.

2. Робота в групах «Розв'язання задач»

Мета: сформувати навички дій у ситуаціях, пов'язаних із роботою з персональними даними.

Час: 30 хв.

Необхідні матеріали: комп'ютери для учасників з доступом до інтернету, Додаток 1.6.2.

Хід проведення:

Тренер/тренерка об'єднує учасників у три групи, які будуть спільно працювати над розв'язанням задач.

Тренер/тренерка виводить на екран проєктора першу задачу, яка міститься в Додатку 1.6.2. На розв'язання задачі групам відводиться п'ять хвилин, після чого тренер/тренерка заслуховує відповіді команд та корегує їх (до п'яти хвилин).

Після обговорення тренер/тренерка зазначає: «*А тепер розглянемо більш цікаву задачу*» та виводить на екран другу задачу із Додатка 1.6.2. На розв'язання другої задачі групам відводиться 5 хвилин, після чого тренер/тренерка заслуховує відповіді команд та корегує їх (до п'яти хвилин).

3. Індивідуальна робота «Чи скомпрометовані ваші персональні дані?»

Мета: перевірити, чи не сталося витоку власних автентифікаційних даних.

Час: 15 хв.

Необхідні матеріали: комп'ютери для учасників з доступом до інтернету.

Хід проведення:

Тренер/тренерка звертається до учасників: «*Проведіть перевірку своїх поштових облікових записів на наявність витоку даних за допомогою сайтів https://haveibeenpwned.com та https://monitor.firefox.com. Якщо виявлено ваші дані у витоках, негайно змініть паролі на відповідних ресурсах та налаштуйте двофакторну автентифікацію, якщо це можливо».*

4. Індивідуальна робота «Пошук інформації про осіб»

Мета: здобути навички пошуку інформації з відкритих джерел.

Час: 90 хв.

Необхідні матеріали: комп'ютери для учасників з доступом до інтернету, Додаток 1.6.3.

Хід проведення:

Тренер/тренерка послідовно виводить на екран (або надає посилання в мережі) на завдання для пошуку із Додатка 1.6.3.

До уваги тренера/тренерки!

Виконання цієї вправи передбачає оволодіння тренером/тренеркою інструментами OSINT. В інакшому випадку можливе проведення заняття з теми без цієї вправи.

Для виконання першого завдання можна застосувати сервіс https://epieos.com/.

Для вирішення другої задачі можна використати інструменти пошуку за зображенням, зокрема: images.google.com; bing.com/images; images.yahoo.com; tineye.com; searchbyimages.com; prepostseo.com/reverse-image-search; intelx.io/tools?tab=image; berify.com.

Виконання третього завдання потребує використання винятково google.com. Слід відшукати за номером термінату зображення, встановити аеропорт, встановити за зображеннями логотипів авіакомпанію, зайти на сайт аеропорту та подивитись розклад, визначити час прибуття та рейс.

Запитання для обговорення:

- *Чи складно було виконати завдання?*
- *Чи важливо поліцейським володіти навичками пошуку інформації?*

5. Вікторина «Висновки»

Мета: перевірити рівень засвоєння учасниками теми заняття, а також закріпити отримані знання.

Час: 15 хв.

Необхідні матеріали: мультимедійне обладнання, доступ до інтернету, Додаток 1.6.4.

Хід проведення:

Тренер/тренерка просить кожного учасника перейти за посиланням та взяти участь у підсумковій вікторині. Орієнтовні питання вікторини містяться у Додатку 1.6.4.

До уваги тренера/тренерки!

Доцільно завчасно підготувати вікторину у Kahoot або Quizizz. Питання вікторини доцільно супроводжувати тематичними ілюстраціями.

Тестові питання до теми:

1. Що таке «інформація про фізичну особу (персональні дані)», відповідно до Закону України «Про інформацію»?

А) інформація, що визнана конфіденційною, відповідно до Закону України «Про державну таємницю»;

Б) відомості у сфері банківської, особистої та комерційної таємниць, передбачені відповідними нормативними актами;

В) відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

Г) інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень.

2. Який гриф має надаватися документам, що містять персональні дані, в державних органах?

А) «Не для друку»;

Б) «Для службового користування»;

В) «Опублікуванню не підлягає»;

Г) «Конфіденційно».

3. Що з наведеного є первинним джерелом відомостей про фізичну особу?

А) дані з персональної сторінки в соціальній мережі;

Б) задокументовані відомості, які надали про особу її близькі та/або члени родини;

В) видані на її ім'я документи;

Г) створений органом державної влади реєстр інформації про фізичних осіб.

4. Які дані про особу допускається використовувати без її згоди, з метою висвітлення діяльності особи або діяльності організації, в якій вона працює чи навчається, що ґрунтується на відповідних документах (звітах, стенограмах, протоколах, аудіо-, відеозаписах, архівних матеріалах тощо)? (оберіть декілька варіантів відповідей)

А) ім'я;

Б) телефон;

В) місце проживання;

Г) дані про нерухоме майно.

5. Хто НЕ може бути розпорядником бази персональних даних, якою володіє орган державної влади чи орган місцевого самоврядування?

А) оператор мобільного зв'язку;

Б) орган державної влади;

В) орган місцевого самоврядування;

Г) підприємство державної або комунальної форми власності, що належить до сфери управління цього органу.

Ключі-відповіді:

1. В; 2. Б; 3. В; 4. А; 5. А.

Додаток 1.6.1

Захист персональних даних, які містять інформацію про особу, є одним із найважливіших аспектів побудови громадянського суспільства.

Як і в Україні (2010 р.), спеціальні закони про захист персональної інформації були ухвалені в більшості європейських країн: Австрії (1978 р.), ФРН (1977 р.), Великобританії (1984 р.), Франції (1987 р.), Норвегії (1988 р.), Португалії (1991 р.), Бельгії (1992 р.), Іспанії (1993 р.) тощо.

Радою Європи ухвалено Конвенцію про захист особи у зв'язку з автоматизованою обробкою персональних даних (1981 р.), 15 директив і рекомендацій у галузі захисту даних, зокрема про захист: персональних даних у приватному (1973 р.) та державному (1974 р.) секторах; даних, що використовуються у медичних цілях (1981 р.), наукових дослідженнях та статистиці (1983 р.), прямому маркетингу (1985 р.), соціальному забезпеченні (1986 р.), правоохоронній сфері (1987 р.); даних у галузях зайнятості (1981 р.), платежів (1990 р.) тощо. Нормативні акти та рекомендації у вказаній сфері ухвалені також Європейським Союзом (95/46/CE), Організацією економічного співробітництва та розвитку.

Наразі в Україні є чинним Закон України «Про захист персональних даних» від 01.06.2010. Відповідно до п. 2 ст. 5 цього закону персональні дані, крім знеособлених персональних даних, за порядком доступу є інформацією з обмеженим доступом. Водночас ***персональні дані*** – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Таке саме визначення наведено у ст. 11 Закону України «Про інформацію» від 02.10.1992. Основними даними про особу (персональними даними) є: національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження.

Джерелами документованої інформації про особу є видані на її ім'я документи, підписані нею документи, а також відомості про особу, зібрані державними органами влади та органами місцевого і регіонального самоврядування в межах своїх повноважень.

Інформацію про особу можна поділити на:

загальну, яка є відкритою і може використовуватися іншими особами. Це, наприклад, ім'я фізичної особи, право на використання якого відповідно до п. 3 ст. 296 Цивільного кодексу України допускається без її згоди, з метою висвітлення діяльності особи або діяльності організації, в якій вона працює чи навчається, що ґрунтується на відповідних документах (звітах, стенограмах, протоколах, аудіо-, відеозаписах, архівних матеріалах тощо);

вразливі персональні дані (конфіденційна інформація про особу), що є інформацією з обмеженим доступом. Саме про такі дані йдеться у ст. 32 Конституції України та у ст. 302 Цивільного кодексу України: «Збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини». До таких даних належать, зокрема, персональні дані, що свідчать про расову належність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, засудження до кримінального покарання. Також згідно з Рішенням Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К. Г. Устименка) від 30.10.1997 *до конфіденційної інформації про особу*, зокрема, належать свідчення про особу: освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані.

У 2012 році Конституційний суд України додатково розтлумачив, що інформація про особисте та сімейне життя особи (персональні дані про неї) – це будь-які відомості чи сукупність

відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адреса, дата і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка обіймає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування. Така інформація про фізичну особу та членів її сім'ї є конфіденційною і може бути поширена тільки за їх згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Оскільки персональні дані є інформацією, вимога щодо захисту якої встановлена законом «Про захист персональних даних», то відповідно до п. 4 Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету Міністрів України від 29.03.2006 №373, вона підлягає захисту в системі.

Враховуючи викладене, відповідно до Закону України «Про захист персональних даних», Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету Міністрів України від 29.03.2006 № 373 та інших нормативних актів у сфері захисту інформації **загальна інформація про особу**, що зберігається в інформаційних системах держави, повинна бути захищена як відкрита інформація, а **вразливі персональні дані –** як службова інформація відповідно до вимог чинного законодавства у державних органах, або як окремий вид інформації згідно з вимогами Закону України «Про захист персональних даних» від 01.06.2010.

Дія цього закону *не поширюється* на діяльність з обробки персональних даних, яка здійснюється повністю або частково *із застосуванням автоматизованих засобів*, а також на обробку персональних даних, що містяться в *картотеці* (будь-які структуровані персональні дані, доступні за визначеними критеріями, незалежно від того, чи такі дані централізовані, децентралізовані або розділені за функціональними чи географічними принципами) чи призначені до внесення до картотеки, із застосуванням *неавтоматизованих засобів*.

Відповідно до ст. 3 Закону України «Про захист персональних даних» ***база персональних даних*** – іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних.

Суб'єктами відносин, пов'язаних із персональними даними, є:

- суб'єкт персональних даних;
- володілець бази персональних даних;
- розпорядник бази персональних даних;
- третя особа;
- Уповноважений Верховної Ради України з прав людини.

Володілець чи розпорядником бази персональних даних можуть бути *підприємства, установи й організації* ***всіх форм власності****, органи державної влади чи органи місцевого самоврядування, фізичні особи – підприємці*, які обробляють персональні дані відповідно до законодавства.

Розпорядником бази персональних даних, володільцем якої є орган державної влади чи орган місцевого самоврядування, крім цих органів, може бути лише *підприємство державної або комунальної форми власності*, що належить до сфери управління цього органу.

Персональні дані, крім знеособлених персональних даних, за порядком доступу **є інформацією з обмеженим доступом**.

Законом може бути заборонено віднесення окремих персональних даних до інформації з обмеженим доступом. Наприклад, згідно з ч. 6 ст. 6 Закону України «Про доступ до публічної інформації» не належать до інформації з обмеженим доступом відомості, зазначені в декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, поданій відповідно до Закону України «Про запобігання корупції», крім відомостей, зазначених в абз. 4 ч. 1 ст. 47 вказаного закону.

Склад і зміст персональних даних мають бути **відповідними та ненадмірними** стосовно визначеної мети їх обробки.

Первинними джерелами відомостей про фізичну особу є: *видані на її ім'я документи; підписані нею документи; відомості, які особа надає про себе.*

Не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, **без її згоди**, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Для обробки персональних даних суб'єктом персональних даних має бути надана **згода на обробку його даних**.

Сьогодні збирати, обробляти, зберігати та використовувати персональні дані дозволено лише після отримання попередньої згоди особи. Згідно із законом, така згода повинна бути задокументованою, зокрема письмово, або в окремих випадках в електронному вигляді.

У загальному випадку **забороняється** обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях і професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних.

Суб'єкта персональних даних наділено низкою прав, зокрема на доступ до своїх персональних даних, що містяться у відповідній базі персональних даних. Водночас відомості про особисте життя фізичної особи не можуть використовуватися як чинник, що підтверджує чи спростовує її ділові якості.

Порядок доступу до персональних даних третіх осіб визначається умовами згоди суб'єкта персональних даних, наданої володільцю бази персональних даних на обробку цих даних, або відповідно до вимог закону. Для отримання доступу складається запит.

Суб'єкти відносин, пов'язаних із персональними даними, зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, зокрема незаконного знищення чи доступу до персональних даних.

В органах державної влади та органах місцевого самоврядування, організаціях, установах і на підприємствах усіх форм власності створюється *структурний підрозділ або відповідальна особа, яка організовує роботу, пов'язану із захистом персональних даних* під час їх обробки відповідно до закону.

За незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконну зміну такої інформації передбачено кримінальну відповідальність згідно зі ст. 182 Кримінального кодексу України.

Додаток 1.6.2

Завдання 1

До підрозділу Національної поліції надійшов запит про доступ до публічної інформації, у якому просять надати інформацію про дітей, які перебувають на обліку:

- ПІБ;
- дата народження;
- адреса проживання;
- контактні дані;
- з якого року перебуває на обліку.

Вам доручили підготувати відповідь на цей запит. Складіть проєкт відповіді.

Завдання 2

До підрозділу Національної поліції надійшов запит про доступ до публічної інформації, у якому просять надати інформацію про знеособлені паролі доступу до інформаційної системи підрозділу:

- назва системи;
- список паролів.

Вам доручили підготувати відповідь на цей запит. Складіть проєкт відповіді.

Додаток 1.6.3

Завдання 1

Підозрюваний у розбещенні неповнолітніх залишив контактну адресу cyberhygieneukraine@gmail.com. Знайдіть фото, прив'язане до облікового запису та місця, які володілець облікового запису відмітив на карті. Знайдіть принаймні три ресурси, на яких під час реєстрації використовувалася встановлена електронна пошта.

Встановіть, чи справжнє фото використав порушник у своєму профілі.

Завдання 2

У результаті аналізу вмісту облікового запису адміністратора деструктивної молодіжної групи в соціальній мережі було знайдено фотографію (Рис. 1), яка може вказувати на місце перебування особи, яка становить оперативний інтерес.

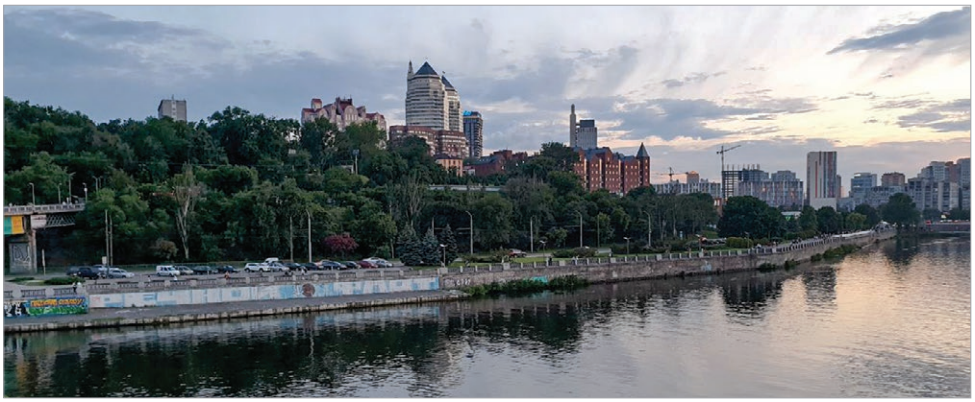


Рис. 1. Місто та водойма

Визначте приблизні координати місця, де було зроблено цю фотографію.

Завдання 3

Особа, яка перебуває у розшуку за викрадення дитини, розмістила у своєму обліковому записі в соціальних мережах повідомлення, що вона нарешті прибула додому та долучила відповідне фото (Рис. 2). Фото розміщено в Instagram о 12:30.

Рис. 2. Літак в аеропорту

Визначити:

- авіакомпанію;
- назву аеропорту;
- напрям рейсу;
- час прибуття.

Додаток 1.6.4

Вікторина

1. З яким видом інформації вам найчастіше доводиться мати справу?

А) відкрита;

Б) службова;

В) конфіденційна;

Г) таємна.

2. Чи потребує захисту відкрита інформація в державних органах?

А) так;

Б) ні.

3. Порядок роботи з якою інформацією регулює Наказ Національної поліції України № 65 від 26.01.2017?

А) таємна;

Б) конфіденційна;

В) службова;

Г) немає правильних відповідей.

4. Який гриф надається відомостям, що містять службову інформацію?

А) «Не для друку»;

Б) «Для службового користування»;

В) «Опублікуванню не підлягає»;

Г) «Конфіденційно».

5. Які з наведених персональних даних є відкритими?

А) прізвище та ім'я;

Б) прізвище, ім'я та номер телефону;

В) номер телефону, паспортні дані;

Г) немає правильних відповідей.

6. Що з наведеного не належить до персональних даних про особу?

А) національність;

Б) освіта;

В) дата і місце народження;

Г) немає правильних відповідей.

7. Хто з наведених осіб здійснює контроль за додержанням законодавства про захист персональних даних?

А) Уповноважений Верховної Ради України з прав людини;

Б) Директор Національної поліції України;

В) Міністр юстиції України;

Г) Голова Державної служби статистики України.

8. У якій справі ЄСПЛ дійшов висновку про порушення приватності під час збирання правоохоронцями даних з відкритих джерел?

А) Фінляндія проти Куусеніна;

Б) Угорщина проти Куна;

В) Франція проти Бомарше;

Г) немає правильних відповідей.

9. Вам цікаво вивчати, як захищати персональні дані?

А) так;

Б) ні.

10. Коли я повернусь на роботу, то обов'язково перевірю стан захисту персональних даних у своєму підрозділі:

А) так;

Б) ні;

В) «У мене вже все перевірено»;

Г) «Я заплутався».

Ключі-відповіді:

1. Б; 2. А; 3. В; 4. Б; 5.А; 6.Г; 7. А; 8.А; 9.А; 10.В.

ТЕМА 1.7. Убезпечення дітей від неправдивих повідомлень в мережі інтернет. Види маніпуляцій з інформацією та правила реагування на них

Заняття 1.7.1. Види маніпуляцій з інформацією та їх ознаки

Мета: надати учасникам інформацію про види маніпуляцій з інформацією та сприяти усвідомленню ними шкідливого впливу неправдивої інформації на дітей.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Вплив інформації на людину	Інформаційне повідомлення	5 хв	Мультимедійне обладнання або фліпчарт, аркуші для фліпчарту, маркери
2.	Два пілоти	Рольова гра	20 хв	Додаток 1.7.1.1
3.	Факт чи судження?	Вправа	15 хв	Додаток 1.7.1.2, фліпчарт та аркуші для фліпчарту, маркери, мультимедійне обладнання.
4.	Трихвилинний тест	Вправа	10 хв	Роздруківка Додатка 1.7.1.3 та кулькові ручки за кількістю учасників
5.	Види маніпуляцій з інформацією	Вправа	40 хв	Додатки 1.7.1.4, 1.7.1.5, мультимедійне обладнання

ХІД ЗАНЯТТЯ

1. Інформаційне повідомлення «Вплив інформації на людину»

Мета: сприяти усвідомленню учасниками впливу інформації на людину та її поведінку, актуалізувати важливість розвитку медіаграмотності.

Час: 5 хв.

Необхідні матеріали: мультимедійне обладнання або фліпчарт, аркуші для фліпчарту, маркери**.**

Хід проведення:

Тренер/тренерка зазначає: *«Щодня ми споживаємо величезні обсяги інформації. Телебачення, соціальні мережі, газети, реклама – інформаційні повідомлення надходять з усіх боків. Проте за таку доступність інформації ми платимо певну ціну: стикаємося з маніпуляціями, які можуть бути як усвідомленими, так і ненавмисними, як онлайн, так і офлайн. Не слід недооцінювати їх вплив на наше життя, зокрема на пізнання, впевненість, ставлення, настрої, поведінку та навіть фізіологічний стан. Наприклад, новини про війну викликають у нас страх, що може призвести до пришвидшеного серцебиття та сильнішого потовиділення. Стандарти краси, нав'язані медіа, можуть спонукати деяких підлітків експериментувати з харчуванням, що в результаті може призвести до анорексії або булімії. Медіа здатні мотивувати до дії або бездіяльності. Часто саме через соціальні мережі розповсюджуються челенджі, які можуть становити небезпеку для дітей, або дітей втягують у молодіжні субкультури, які безпосередньо впливають на поведінку дітей. Важливо навчитися відрізняти якісну інформацію від маніпулятивної чи неправдивої.*

У 1977 році група вчених виявила, що люди схильні сприймати інформацію як правдиву, якщо вже чули її кілька разів. Це явище назвали ***ефектом ілюзії правди або ефектом повторення****: ч****им більше інформаційного шуму створено, тим вища ймовірність, що люди в це повірять.***

У межах інформаційного впливу використовується певний набір характеристик: видовищність, порушення звичної моделі світу, пропаганда, «тролінг» (активна участь у багатьох дискусіях під вигаданими іменами), копіпастинг. Типові ознаки троля: емоційні меседжі, чіткі тези із закликами, одноманітний профіль у мережі, незначна кількість віртуальних друзів, відсутність власних постів, створена нещодавно сторінка.

Підвищення рівня медіаграмотності суспільства та протидія дезінформації є одними зі стратегічних цілей України. Відповідно до Закону України «Про медіа», ***медіаграмотність*** *– це навички та знання, які надають користувачам можливість ефективно і безпечно користуватися медіасервісами. Дотримання правил інформаційної та кібербезпеки на сьогодні актуальні для кожної людини, починаючи з самого дитинства».*

До уваги тренера/тренерки!

Доцільно фіксувати ключові повідомлення на аркуші для фліпчарту або завчасно підготувати презентацію.

Запитання для обговорення:

- *Чи замислювались ви раніше про те, який вплив має інформація на людину?*
- *Які категорії населення, на вашу думку, є більш вразливими щодо впливу інформації?*

Підсумовуючи, тренер/тренерка наголошує: *«Враховуючи особливу через вік уразливість дітей, вплив інформації на них в рази сильніший, ніж на дорослих. Тому вкрай важливо, починаючи з дитинства, формувати у дітей навички критичного мислення та аналізу інформації, яку вони споживають».*

2. Рольова гра «Два пілоти»

Мета: опанувати маркери інформування і впливу, ідентифікації фактів та суджень; з'ясувати для учасників, чим вони керуються в ситуації вибору інформації для прийняття рішення – фактами чи емоційними судженнями.

Час: 20 хв.

Необхідні матеріали: Додаток 1.7.1.1.

Хід проведення:

На початку вправи тренер/тренерка обирає двох добровольців і запрошує їх вийти із загального приміщення. Там учасники отримують інструкції пілотів із Додатка 1.7.1.1. Учасники мають прочитати інструкції, продумати свій текст, щоб говорити впевнено, і за командою тренера/тренерки повернутися в загальне приміщення.

Поки учасники готуються (до п'яти хвилин), тренер/тренерка повертається до групи і пояснює їм змодельовану ситуацію, в якій далі буде виконуватися вправа. Завдання для групи міститься у Додатку 1.7.1.1.

Повернувшись з кімнати, «пілоти» виступають перед учасниками групи. Після виступів учасників тренер/тренерка просить зробити вибір одночасно на «раз-два-три».

До уваги тренера/тренерки!

Можна запропонувати різні моделі виявлення голосу учасників, наприклад, це можуть бути написи імен пілотів на завчасно розданих стікерах; або можна запропонувати тим учасникам, які голосують за «пілота» №1, встати, а ті, хто за «пілота» №2, – залишатися сидіти; або можна провести голосування за допомогою Mentimetr, Slido тощо.

Запитання для обговорення:

- *Чому ви обрали саме цього пілота?*
- *Що вас змусило повірити саме йому?*
- *Чи немає тут аналогії до тієї інформації, яку ми отримуємо щодня з різних джерел і каналів інформації?*
- *Якщо є учасники, які не зробили свій вибір, запитайте у них, чому вони не довірили життя жодному з пілотів та вирішили залишитися на планеті Земля?*

Підсумовуючи, тренер/тренерка наголошує: *«Емоційний компонент є характерною рисою інформаційно-психологічного впливу. Кожен з нас, приймаючи рішення, переважно керується або фактами, або емоціями. Інформування базується на фактах, але часто «програє» через емоційну нейтральність, відсутність прямих закликів, обіцянок простих рішень і яскравих емоцій. Натомість тиск на адресата, обіцянки, заклики, емоційні судження – все це дуже поширене в іншому типі контенту, який не лише інформує, а й чинить вплив на адресата з метою зміни його ставлення чи поведінки. Діти є особливо уразливими і чутливими до емоцій, тому важливо це враховувати всім фахівцям, які з ними працюють».*

3. Вправа «Факт чи судження?»

Мета: сформувати в учасників вміння відрізняти факти від суджень.

Час: 15 хв.

Необхідні матеріали: Додатки 1.7.1.2, фліпчарт та аркуші для фліпчарту, маркери, мультимедійне обладнання.

Хід проведення:

Тренер/тренерка зазначає: *«Переважно маніпуляції з інформацією розраховані на емоції споживачів, під впливом яких вони не завжди здійснюватимуть фактчекінг, тобто перевірку інформації. Важливо сформувати навичку відрізняти факти від суджень. Факт – це об'єктивна незмінна інформація, яку можна перевірити на правдивість. Судження – це чиясь думка, оцінка, припущення, вподобання, яке може змінюватися з часом»*.

Тренер/тренерка бере заздалегідь підготовлені картки із Додатка 1.7.1.2, на яких записані факти або судження. Учасникам пропонується «ногами» проголосувати за те, чим, на їхню думку, є це твердження – судження чи факт: якщо «Факт» – вони стають праворуч від тренера/тренерки, якщо «Судження» – ліворуч. На кожен приклад тренер/тренерка пропонує учасникам спільно сформулювати той маркер, за яким визначено факт чи судження. Якщо хтось із учасників помиляється з відповіддю, приклад доцільно обговорити більш детально.

До уваги тренера/тренерки!

Наведений у Додатку 1.7.1.2 перелік тверджень є орієнтовним. Для проведення вправи можна підготувати також інші твердження.

Інший варіант проведення вправи – голосування різнокольоровими картками, які потрібно попередньо роздати. Наприклад, зелений колір – факт, червоний – судження.

Також можна провести цю вправу з використанням Kahoot, Mentimetr, Quizizz і по черзі виводити твердження на екран.

Крім того, можна об'єднати учасників в групи та роздати кожній із них аркуші з твердженнями, на яких вони мають помітити, що є фактом, а що твердженням. Після закінчення часу на роботу групи по черзі коментують по одному твердженню, інші групи перевіряють, чи збігається відповідь з їхньою.

На наступному етапі вправи тренер/тренерка пропонує учасникам поміркувати, на основі чого вони визначали, фактом чи судженням є певне твердження та фіксує відповіді учасників на аркуші фліпчарту. Після того, як учасники висловилися, тренер/тренерка коментує та узагальнює їхні відповіді, а далі – пропонує порівняти їх із критеріями, які містяться у Додатку 1.7.1.2 (доцільно вивести на екран).

Запитання для обговорення:

- *Чи легко відрізнити факт від судження?*
- *Чому важливо вміти відрізняти факти від суджень?*

До уваги тренера/тренерки!

Слід наголосити учасникам, що вміння ідентифікувати, розрізняти факти й судження є базовим у компетентностях з медіаграмотності. На основі цих вмінь базуються наступні – враховувати вплив медіавласників на зміст повідомлення, розпізнавати маніпуляції тощо.

4. Вправа «Трихвилинний тест»

Мета: продемонструвати учасникам важливість вміння контролювати емоції і не втрачати пильність під впливом зовнішніх чинників.

Час: 10 хв.

Необхідні матеріали: роздруківка Додатка 1.7.1.3, та кулькові ручки за кількістю учасників.

Хід проведення:

Тренер/тренерка інструктує учасників про важливість дотримання під час виконання наступної вправи трьох умов:

1) час на виконання тесту – три хвилини (якщо хтось виконає раніше, не слід це жодним чином демонструвати);
2) виконувати вправу слід самостійно та
3) мовчки (можна порушити тільки якщо відповідно до завдання треба щось проголосити).

До уваги тренера/тренерки!

Доцільно вивести правила виконання вправи на екран.

Після інструктажу тренер/тренерка роздає кожному учаснику аркуш з Додатка 1.7.1.3, надрукований так, щоб п. 21 був на зворотному боці аркушу. Після того, як всі учасники отримали примірник Додатка 1.7.1.3, тренер/тренерка зазначає, що час на виконання вправи розпочався.

Під час виконання учасниками тесту тренер/тренерка має постійно проголошувати якісь фрази, нагадувати про те, скільки часу залишилось, про правила тощо, у такий спосіб відволікаючи учасників від виконання завдання.

Після закінчення часу на виконання вправи за командою тренера/тренерки учасники повинні відкласти кулькові ручки, після чого доцільно запитати в аудиторії, чи хто-небудь встиг

виконати весь тест. Зазвичай декілька осіб відповідають ствердно. Слід попросити їх пояснити іншим учасникам, як їм це вдалось.

До уваги тренера/тренерки!

Якщо уважно слідувати інструкції, зазначеній у п. 1, а саме – прочитати всі пункти, перш ніж будь-що робити, то достатньо виконати лише п. 1 та п. 2, про що зазначається у п. 21.

Підсумовуючи, тренер/тренерка наголошує: *«Важливо контролювати свої емоції, щоб вони не контролювали вас. Під впливом зовнішніх чинників (обмаль часу, поспіх, відволікання тощо) досить складно залишатись зосередженими та не втрачати пильність під час роботи з інформацією. Уважність до деталей та критичне мислення за будь-яких обставин – це також елемент медіаграмотності, якому слід привчати з дитинства».*

5. Вправа «Види маніпуляцій з інформацією»

Мета: сформувати в учасників розуміння існування різних видів маніпуляції з інформацією та оцінити їх рівень вміння відрізняти її різні види.

Час: 40 хв.

Необхідні матеріали: Додатки 1.7.1.4, 1.7.1.5, мультимедійне обладнання.

Хід проведення:

Тренер/тренерка зазначає: *«Як і будь-яка глобальна система, медіасередовище є забрудненим. У нашій інформаційній екосистемі є безліч неправдивої інформації, яка дестабілізує та поляризує суспільство. Іноді мета такого контенту – підвищити відвідуваність вебсайту, розпочати дискусію чи спровокувати конфлікт у коментарях. Ці коментарі використовують для формування громадської думки в соціальних мережах, тобто ставлення людей до певної події, особи чи країни. Деяка інформація в медіа може бути створена, щоб зашкодити, ввести в оману або просто задля розваги. Доцільно навчитись розрізняти типи маніпулятивного контенту у своєму медіапросторі. Здатність визначати та аналізувати неправдиву чи неточну інформацію є важливою навичкою у XXI столітті. Важливо не тільки знати про маніпуляції в медіа загалом, але й вміти ідентифікувати їх види. Якщо ми знаємо основні інструменти маніпуляції та розрізняємо види викривлення інформації, ми будемо менше підпадати під маніпулятивний вплив медіаповідомлень. Існує безліч підходів до класифікації маніпуляцій з інформацією. Так О. Юркова на підставі сучасного практичного досвіду представила кілька способів створення недостовірних новин. Серед них:*

1. *Маніпуляції з медіаданими: редагування; подання справжніх медіаданих в іншому контексті, зміна часу і місця їх створення; створення повністю недостовірного медіаконтенту.*
2. *Маніпулювання новинами: викривлення сенсу заголовків новин; подання окремої думки як факту; викривлення фактів; подання повністю недостовірної інформації як факту; ігнорування важливих деталей, які змінюють контекст.*
3. *Маніпулювання експертними оцінками: використання думок псевдоекспертів (несправжніх експертів, експертів в інших сферах тощо) та аналітичних центрів; перекручування заяв експертів або приписування видуманих заяв справжнім експертам; викривлення перекладу.*
4. *Маніпулювання повідомленнями: використання повідомлень маргінальних суб'єктів; перекручування реальних повідомлень з авторитетних джерел; посилання на неіснуючі повідомлення з авторитетних джерел.*

5. *Маніпуляції з результатами досліджень: використання слабкої або несправжньої методології; неправильна інтерпретація результатів; неправильні порівняння*[1]***».***

Тренер/тренерка презентує на екрані вікторину із Додатка 1.7.1.4, розроблену в межах проєкту «Вивчай та розрізняй: інфомедійна грамотність», що виконується Радою міжнародних наукових досліджень та обмінів (IREX) за підтримки Посольств США та Великої Британії, у партнерстві з Міністерством освіти і науки України та Академією Української преси. Учасникам необхідно ознайомитись із твердженням, яке було утворено із першопочаткового факту: «Курка знесла яйце» та обрати, який вид маніпуляції із запропонованих на слайді був використаний водночас.

До уваги тренера/тренерки!

За необхідності, тренер/тренерка після відповідей учасників щодо кожного із тверджень може більш детально роз'яснити окремі види маніпуляцій, використавши інформацію із Додатка 1.7.1.5.

Доцільно звернути увагу учасників на можливість використання цієї вікторини під час проведення інформаційно-просвітницьких заходів з дітьми, спрямованих на розвиток їхньої медіаграмотності та убезпечення від неправдивих повідомлень.

Запитання для обговорення:

- *Про які способи викривлення інформації ви знали, а про які дізнались вперше?*
- *Який спосіб викривлення інформації, на вашу думку, трапляється частіше за інші в інформаційному просторі сьогодні?*
- *Який найдивніший заголовок, який ви бачили в інтернеті? Що ви зробили, коли побачили це?*
- *Чи вважаєте ви влучною цитату Черчиля: «Неправда встигає обійти півсвіту, поки правда одягає штани»?*

До уваги тренера/тренерки!

Після проведення вправи, якщо дозволяє час, можна провести руханку «Зіпсований телефон» та звернути увагу учасників, що викривлення інформації – це звичне явище в суспільстві, яке може відбуватись як навмисно, так і випадково. Тому слід завжди мислити критично та перевіряти будь-яку інформацію.

[1] Yurkova O. Six Fake News Techniques and Simple Tools to Vet Them. URL: https://gijn.org/six-fake-news-techniques-and-simpletools-to-vet-them/.

Тестові питання до заняття:

1. Що таке дезінформація?

А) цілеспрямоване поширення ідей і моделей поведінки з метою впливу на суспільну думку;

Б) недостовірна інформація, поширена випадково та без злого наміру;

В) недостовірна інформація, навмисно поширена з метою заплутати, ввести в оману або вплинути;

Г) складно відповісти.

2. Факт має такі ознаки:

А) об'єктивна незмінна інформація, яку можна перевірити на правдивість;

Б) це висновки експерта щодо певного питання чи теми;

В) чиясь думка, оцінка, припущення, вподобання, які можуть змінюватися з часом;

Г) складно відповісти.

3. Чи впливають емоції на здатність сприймати та аналізувати інформацію?

А) так, звичайно, вони нам допомагають бути інфомедійно грамотними;

Б) емоції ніяк не впливають на ці процеси, бо почуття та емоції не пов'язані зі здатністю аналізувати та критично мислити;

В) так, звичайно, емоції заважають нам в аналізі та критичному сприйнятті інформації;

Г) складно відповісти.

4. Про що йдеться у твердженні: «Чим більше інформаційного шуму створено, тим вища ймовірність, що люди в це повірять»?

А) ілюзія правди;

Б) медіаграмотність;

В) прихована реклама;

Г) складно відповісти.

5. Що таке клікбейт?

А) суспільно важлива інформація;

Б) маніпулятивна інформація, поширена з метою «заманювання» на ресурс для отримання вигоди;

В) реклама товарів/послуг;

Г) складно відповісти.

Ключі-відповіді:

1. В; 2. А; 3. В; 4. А; 5. Б.

Додаток 1.7.1.1

ІНСТРУКЦІЯ

Завдання для пілотів

«На планеті Земля сталася жахлива катастрофа, кінець світу. Єдиний порятунок – політ на придатну до життя планету Марс. Ви – двоє з уцілілих, які мають досвід пілота. Але залишився лише один космічний корабель, і він уже заповнений людьми, які й будуть вибирати, ХТО з вас двох сяде за штурвал і «помчить» їх на планету життя».

Ваше завдання: відповідно до принципів вашого пілота (перший – інформування, оперування фактами; другий – пропаганда, маніпулювання, вплив на емоції) зробити свою презентацію так, щоб люди (пасажири) вибрали САМЕ ВАС. Інший пілот тоді залишиться на Землі.

ПІЛОТ № 1. Ви описуєте справжню ситуацію, якою вона є. Говорите всю правду. Без емоцій та прикрас. Говорите про те, що маєте 20 років досвіду. У вас були різні ситуації під час польотів, та ви вдало з них виходили. АЛЕ! Саме в цій ситуації сумніваєтеся, що за такої кількості пального ви зможете долетіти до кінцевого пункту. Ризик великий, але будете робити все можливе.

ПІЛОТ № 2. Ви прикрашаєте дійсність і жонглюєте емоціями. Хоча знаєте про те, що пального може не вистачити на таку далеку відстань. Ви запевняєте пасажирів, що тільки з вами вони можуть долетіти без проблем, і що їм нічого не загрожує. Все буде «ОК». Дарма, що ваш досвід роботи пілотом небагаторічний, проте саме ви, як суперпілот, молодий, амбітний професіонал, зможете долетіти до Марса і врятувати людей. Додайте емоційних прикрас, на кшталт гарний настрій, кава, легко тощо.

Завдання для учасників

Вихідна ситуація така: «На планеті Земля сталася жахлива катастрофа, наближається кінець світу. Єдиний порятунок – політ на придатну для життя планету Марс. Ви – ті, хто вцілів. Залишився лише один космічний корабель, який заповнений вами – людьми, які вціліли. Ваше завдання – вирішити, кому з двох пілотів довірити штурвал і своє життя. Зараз перед вами виступлять два капітани. Виберіть, з яким із них ви полетите на Марс».

Додаток 1.7.1.2

Можливі факти

1. Сьогодні +15.
2. Земля – третя планета від Сонця.
3. Цьогорічне літо спекотніше, ніж попереднє, – середня температура становила +35°C.
4. 65% випускників школи N цьогоріч склали ЗНО на 185+ балів, порівнюючи з минулорічними 48%.
5. Ріст найвищого українця Леоніда Стадника становив 2 метри 57 сантиметрів.
6. Володимир Зеленський переміг на виборах Президента України в 2019 році.
7. Населення України зменшилося з 52 мільйонів у 1991 році до 42 мільйонів у 2019.
8. Цей текст написаний українською мовою і містить дев'ять слів.

Можливі судження

1. На вулиці тепло.
2. Бразильська кава краща, ніж кава з Кенії.
3. Учні школи N почали вчитися краще.
4. Леонід Стадник був дуже високим.
5. Нерухомість у Києві дуже дорога.
6. Хороша кава – найкращий спосіб розпочати свій день.
7. Українці вимушені емігрувати, тому що вижити в країні – неможливо.
8. Наші викладачі найкращі.

ФАКТ	СУДЖЕННЯ
Цифри, дати, події, статистика тощо	Чиїсь думки, припущення, міркування з приводу чогось
Об'єктивний – існує сам по собі	Суб'єктивне – передає погляд людини
Можна перевірити	Не можна перевірити
Є незмінним після того, як відбувся	Може змінюватися залежно від настрою, мети або кількості нових фактів, на основі яких створено
Можуть бути основою для судження	Можуть базуватися або не базуватися на фактах
Для його повідомлення часто використовуються дієслова: є (було, буде), демонструвати, відкривати, доводити	Для його повідомлення часто використовуються дієслова: думати, вважати, припускати, відчувати, сподіватися, висловлювати (погляди) тощо
Розрізняють: 1) Доведені факти 2) Факти, які треба перевірити 3) Неправда, представлена як факт (фейк)	Розрізняють: 1) Думку – судження, базоване на фактах 2) Погляд або переконання – судження, засноване на вірі, моралі або цінностях 3) Упередження – думка на підставі недостатніх або не повністю досліджених доказах

Додаток 1.7.1.3

Трихвилинний тест

1. Прочитайте всі пункти, перш ніж будь-що робити.
2. Напишіть своє ім'я в правому верхньому куті аркуша після слова «ІМ'Я».
3. Обведіть колом слово «ІМ'Я» у пункті 2.
4. Намалюйте П'ЯТЬ МАЛЕНЬКИХ КВАДРАТІВ у верхньому лівому куті листа.
5. Поставте хрестик в кожному квадраті, описаному в пункті 4.
6. Обведіть кожен квадрат трьома концентричними колами.
7. Впишіть своє ПРІЗВИЩЕ _____.
8. Напишіть слово «ТАК» трьома різними мовами по одному разу або рідною мовою п'ять разів.
9. Обведіть колом пункти 7 та 8.
10. Поставте ХРЕСТИК в лівий нижній куток аркушу.
11. Намалюйте над цим хрестиком РІВНОСТОРОННІЙ ТРИКУТНИК.
12. Обведіть колом слово «ВЕРХНЬОМУ» в четвертому пункті.
13. Складіть у стовпчик на зворотному боці аркушу числа 896 та 472.
14. Якщо ви вже дійшли до цього пункту, чітко проголосіть своє повне ІМ'Я.
15. Якщо ви впевнені, що правильно виконали всі попередні інструкції, вимовте чітко і вголос «Я ТОЧНО ВИКОНАВ (-ЛА) ВСІ ІНСТРУКЦІЇ».
16. Поділіть на зворотному боці аркушу суму, отриману в п.13, на 12.
17. Обведіть колом результат розрахунку в п. 16 та помножте його на зворотному боці аркушу на 17.
18. Порахуйте пошепки до ДЕСЯТИ.
19. Зробіть ручкою ТРИ ОТВОРИ в правому нижньому куті аркушу.
20. Якщо ви виконали вправу раніше за інших, гучно скажіть вголос «Я ПЕРШИЙ (-А)!». Якщо другим (-ою), то – «Я ДРУГИЙ (-А)!», тощо.
21. Тепер, коли ви, згідно з п. 1, уважно прочитали весь текст, виконайте тільки те, що написано в пунктах 1 та 2.

Додаток 1.7.1.3

Подивимося, що можуть маніпулятори зробити з одного простого факту

ДЕЗІНФОРМАЦІЯ МАНІПУЛЯЦІЯ ФАКТАМИ ФЕЙК ПРОПАГАНДА ПРИХОВАНА РЕКЛАМА КЛІКБЕЙТ ЦЕНЗУРА УПЕРЕДЖЕННЯ	 *Курка-патріотка: курка знесла яйце на честь національного свята.*
ДЕЗІНФОРМАЦІЯ МАНІПУЛЯЦІЯ ФАКТАМИ ФЕЙК ПРОПАГАНДА ПРИХОВАНА РЕКЛАМА КЛІКБЕЙТ ЦЕНЗУРА УПЕРЕДЖЕННЯ	 *Кури, яких годують генетично модифікованою їжею, несуть корисніші для здоров'я яйця.*
ДЕЗІНФОРМАЦІЯ МАНІПУЛЯЦІЯ ФАКТАМИ ФЕЙК ПРОПАГАНДА ПРИХОВАНА РЕКЛАМА КЛІКБЕЙТ ЦЕНЗУРА УПЕРЕДЖЕННЯ	 *Курка знесла яйце – і з нього вилупилась ящірка.*
ДЕЗІНФОРМАЦІЯ МАНІПУЛЯЦІЯ ФАКТАМИ ФЕЙК ПРОПАГАНДА ПРИХОВАНА РЕКЛАМА КЛІКБЕЙТ ЦЕНЗУРА УПЕРЕДЖЕННЯ	 *Експерти розповідають, що кури з ферми "L2D" є найкращими та несуть найбільше яєць в Україні.*
ДЕЗІНФОРМАЦІЯ МАНІПУЛЯЦІЯ ФАКТАМИ ФЕЙК ПРОПАГАНДА ПРИХОВАНА РЕКЛАМА КЛІКБЕЙТ ЦЕНЗУРА УПЕРЕДЖЕННЯ	 *Ворожі іноземні господарства хочуть знищити наших курей! Підтримуй власного виробника і стань на захист рідних курей!*
ДЕЗІНФОРМАЦІЯ МАНІПУЛЯЦІЯ ФАКТАМИ ФЕЙК ПРОПАГАНДА ПРИХОВАНА РЕКЛАМА КЛІКБЕЙТ ЦЕНЗУРА УПЕРЕДЖЕННЯ	 *Українські кури несуть найкращі яйця у світі.*
ДЕЗІНФОРМАЦІЯ МАНІПУЛЯЦІЯ ФАКТАМИ ФЕЙК ПРОПАГАНДА ПРИХОВАНА РЕКЛАМА КЛІКБЕЙТ ЦЕНЗУРА УПЕРЕДЖЕННЯ	 *Сенсація! Шок! Ви ніколи не повірите, що зробила ця курка.*
ДЕЗІНФОРМАЦІЯ МАНІПУЛЯЦІЯ ФАКТАМИ ФЕЙК ПРОПАГАНДА ПРИХОВАНА РЕКЛАМА КЛІКБЕЙТ ЦЕНЗУРА УПЕРЕДЖЕННЯ	 *Курка, яку ми не можемо назвати, зробила те, про що ми не можемо розповісти, але ви про це від нас не чули.*

Відповіді на вікторину

ДЕЗІНФОРМАЦІЯ
МАНІПУЛЯЦІЯ ФАКТАМИ
ФЕЙК
ПРОПАГАНДА
ПРИХОВАНА РЕКЛАМА
КЛІКБЕЙТ
ЦЕНЗУРА
УПЕРЕДЖЕННЯ

МАНІПУЛЯЦІЯ ФАКТАМИ

Відома та правдива інформація, яка подана так, щоби ввести в оману.

Курка-патріотка: курка знесла яйце на честь національного свята.

ДЕЗІНФОРМАЦІЯ
МАНІПУЛЯЦІЯ ФАКТАМИ
ФЕЙК
ПРОПАГАНДА
ПРИХОВАНА РЕКЛАМА
КЛІКБЕЙТ
ЦЕНЗУРА
УПЕРЕДЖЕННЯ

ДЕЗІНФОРМАЦІЯ

Поєднання фактів, напівправди та неправди.

Кури, яких годують генетично модифікованою їжею, несуть корисніші для здоров'я яйця.

ДЕЗІНФОРМАЦІЯ
МАНІПУЛЯЦІЯ ФАКТАМИ
ФЕЙК
ПРОПАГАНДА
ПРИХОВАНА РЕКЛАМА
КЛІКБЕЙТ
ЦЕНЗУРА
УПЕРЕДЖЕННЯ

ФЕЙК

Неправдиве твердження, яке часто є повністю вигаданим. Створене для того, щоб ввести в оману громадськість та приховати правду.

Курка знесла яйце – і з нього вилупилась ящірка.

ДЕЗІНФОРМАЦІЯ
МАНІПУЛЯЦІЯ ФАКТАМИ
ФЕЙК
ПРОПАГАНДА
ПРИХОВАНА РЕКЛАМА
КЛІКБЕЙТ
ЦЕНЗУРА
УПЕРЕДЖЕННЯ

ПРИХОВАНА РЕКЛАМА

Реклама, замаскована у редакційний текст.

Експерти розповідають, що кури з ферми "L2D" є найкращими та несуть найбільше яєць в Україні.

ДЕЗІНФОРМАЦІЯ
МАНІПУЛЯЦІЯ ФАКТАМИ
ФЕЙК
ПРОПАГАНДА
ПРИХОВАНА РЕКЛАМА
КЛІКБЕЙТ
ЦЕНЗУРА
УПЕРЕДЖЕННЯ

ПРОПАГАНДА

Упереджена чи оманлива інформація, спрямована на поширення певної точки зору та зміни моделей поведінки.

Ворожі іноземні господарства хочуть знищити наших курей! Підтримуй власного виробника і стань на захист рідних курей!

ДЕЗІНФОРМАЦІЯ
МАНІПУЛЯЦІЯ ФАКТАМИ
ФЕЙК
ПРОПАГАНДА
ПРИХОВАНА РЕКЛАМА
КЛІКБЕЙТ
ЦЕНЗУРА
УПЕРЕДЖЕННЯ

УПЕРЕДЖЕННЯ

Медіаконтент надає перевагу одній точці зору і не показує інші.

Українські кури несуть найкращі яйця в світі.

ДЕЗІНФОРМАЦІЯ
МАНІПУЛЯЦІЯ ФАКТАМИ
ФЕЙК
ПРОПАГАНДА
ПРИХОВАНА РЕКЛАМА
КЛІКБЕЙТ
ЦЕНЗУРА
УПЕРЕДЖЕННЯ

КЛІКБЕЙТ

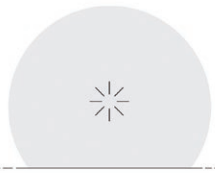
У статті використовують сенсаційний заголовок для привернення уваги.

Сенсація! Шок! Ви ніколи не повірите, що зробила ця курка.

ДЕЗІНФОРМАЦІЯ
МАНІПУЛЯЦІЯ ФАКТАМИ
ФЕЙК
ПРОПАГАНДА
ПРИХОВАНА РЕКЛАМА
КЛІКБЕЙТ
ЦЕНЗУРА
УПЕРЕДЖЕННЯ

ЦЕНЗУРА

Заборона повідомляти про певні події, людей чи теми. Редакція видаляє контент без очевидних причин.



Курка, яку ми не можемо назвати, зробила те, про що ми не можемо розповісти, але ви про це від нас не чули.

Додаток 1.7.1.5

Дезінформація

Цей тип неправдивої інформації створюється спеціально, щоб завдати шкоди особі, соціальній групі, організації чи країні. Коли люди поширюють неправдиву інформацію, вони часто вірять у те, що поширюють. Однак дезінформацію створюють і розповсюджують навмисно, з метою ввести в оману інших. Візуалізацію сутності дезінформації можна побачити на *зображенні.*

Іноді дезінформацію ретельно розробляють спеціалісти з метою схилити громадську думку на користь чогось чи когось або посіяти сумнів чи суперечки.

Дезінформація та **неправдива інформація** часто використовуються як синоніми. Проте їх слід розрізняти. Так дезінформація – це навмисне поширення неправдивої інформації з метою змінити погляд чи думку громадськості. **Неправдива інформація,** так само, часто поширюється людьми, яких ми знаємо, і часто з найкращими намірами. Вони не навмисно намагаються ввести в оману, але чим більше вмісту поширюється, тим більша ймовірність, що йому повірять.

Цензура

«Кожен запис було знищено або підроблено, кожну книжку – переписано, кожну картину – перемальовано, кожну статую та будівлю – переіменовано, кожну дату – змінено. І цей процес триває день за днем, хвилина за хвилиною. Історія зупинилася. Нічого не існує, крім безкінечного тепер, у якому Партія завжди має рацію». Так описує Міністерство правди Джордж Орвелл у своєму романі-антиутопії «1984». Незважаючи на назву, це Міністерство не має нічого спільного з правдою.

З 2002 року міжнародна організація «Репортери без кордонів» (Reporters Without Borders (RSF)) щорічно публікує рейтинг – «Індекс свободи преси». Для цього рейтингу організація використовує власну оцінку рівня свободи преси у різних країнах, яка ґрунтується на даних за рік. Серед країн з найвищим індексом свободи преси – Норвегія, Фінляндія та Швеція. Тут журналісти зазнають значно менше політичного тиску та цензури, ніж в інших країнах. Україна в 2022 році посіла 106 місце у цьому рейтингу. Найнижчі місця у рейтингу посідають Туркменістан, Північна Корея, Еритрея та Китай. У цих країнах існують

окремі закони, які забороняють поширювати ідеї та критикувати уряд. Наприклад, багато вебсайтів, зокрема Гугл, Фейсбук, Інстаграм та Ютуб, заблоковані у континентальному Китаї. Усі вони підлягають під політику інтернет-цензури, головна мета якої – попередити колективні дії, наприклад протести.

Клікбейт

Заголовок – найважливіший елемент будь-якої статті чи відео. Його головна мета – привернути увагу аудиторії та спонукати її прочитати чи проглянути матеріал. Саме тому журналісти та редактори часто використовують у своїх заголовках елементи драми та сенсації, наголошуючи на аспектах новин, які, на їхню думку, зацікавлять цільову аудиторію. Заголовок може також містити зображення, щоб підсилити емоційний вплив. «Сенсація дня», «Терміново» – ці слова привертають увагу читачів та змушують їх переходити за посиланням. Це називається **клікбейт** (англ. *clickbait*, від *click* «клацання» та *bait* «наживка»).

Сатиричне онлайн-видання *The Science Post* **опублікувало статтю з назвою «Дослідження: 70% користувачів Фейсбук читають лише заголовки наукових статей перед тим, як коментувати».** Перший абзац статті написаний англійською. Однак другий абзац – це стандартний текст lorem ipsum – варіант умовного беззмістовного тексту, який використовують графічні дизайнери у своїх макетах. Статтю поширили понад 194 400 користувачів. Сатирична стаття привернула увагу багатьох науковців, оскільки вона допомогла дослідити поведінку тих, хто читає новини в соціальних мережах. Науковці з багатьох дослідницьких центрів США проаналізували 2,8 мільйонів ретвітів та з'ясували, що 59% ставлять «подобається» та поширюють посилання, навіть якщо самі не переходили за ним.

Ознакою клікбейту може бути емоційність, інтрига, а також наявність однієї або кількох складових частин з формули «6С+1Г» (секс, смерть, страх, сміх, скандал, сенсація, гроші). Ймовірно, ви не раз помічали рекламні банери, з заголовками типу:

- *«Ти схуднеш на 10 кг за тиждень, якщо перед сном випиватимеш…»*
- *«Ви не повірите, але це…»*
- *«Те, що відбулося далі, ШОКУЄ вас…».*

Основні принципи, за якими можна визначити клікбейт заголовок, зокрема: залучення емоцій, обіцянки важливості та корисності інформації для читача, сенсаційність інформації, терміновість (обіцянка чогось надзвичайного тут і зараз), унікальність (завдяки чому досягається результат). Часто ці «гачки» уваги виявляються маніпуляціями, коли текст матеріалу й обіцяна інформація в заголовку не збігаються. Часто статті з такими заголовками містять ще й зображення, які суперечать змісту або заголовку.

Але навіщо все це вигадали? Онлайн-медіа отримують значну частину свого прибутку з реклами. Що більше користувачів вони мають на своїх вебсторінках, то більше рекламодавців хочуть розміщувати там свої оголошення. У такий спосіб прибуток власників медіа збільшується. Крім того, коли ви натискаєте на клікбейт, ви можете перейти на вебсайти, наповнені рекламою, шкідливим вмістом або неправдивими повідомленнями.

Фейк

Фейк – це:

- подання фактів у спотвореному вигляді;
- сфабрикована інформація, що не відповідає дійсності;
- повідомлення про щось, що ніколи не відбувалось.

Ознаки, які можуть вказувати на фейк, наведені у таблиці нижче

Джерела	Експерти
▶ відсутність джерел інформації ▶ анонімні джерела ▶ інформацію взято із неверифіковних акаунтів у соцмережах ▶ покликання на підозрілі або маловідомі джерела	▶ представники структур, яких насправді не існує ▶ експерти без вказування інституцій, які вони представляють ▶ анонімні експерти («вчені вважають ...») ▶ політично заангажовані експерти
Емоції	**Подання інформації**
▶ думку чи оцінку подано як факт ▶ заголовок занадто емоційний або не відповідає новині ▶ журналісти вживають слова, що викликають позитивні/негативні емоції ▶ навішування ярликів, поширення стереотипів	▶ соціологічні дані без вказання вибірки, замовника, географії тощо ▶ однобоке подання фактів, оцінок і коментарів, узагальнення ▶ викривлене подання новини: реальні факти подають з неправдою ▶ неправдиві фото чи відео подають як підтвердження інформації

Фейки бувають **невинними.** Їх створюють заради популярності та підписників.

Приклади:

1) у соцмережах просять поширити інформацію про перемогу на конкурсі чи змаганнях;
2) у маленькому українському містечку побачили нереально багато веселок.

Як швидко поширюються фейки? І які поширюються найкраще?

Фейки поширюються у **шість разів** швидше за правду. Про це йшлося в дослідженні, опублікованому в березні 2018 року в журналі Science. Дослідники взяли масив даних правдивих та фейкових повідомлень у Твіттері за період з 2006 по 2017 рік. А це – понад 100 000 історій, які були поширені 4,5 млн разів. Виявилось, що фейкові історії більше подобаються користувачам та краще поширюються. В результаті виявилося, що фейк може стати вірусним і без допомоги ботів. Головний висновок цього дослідження невтішний: **правда не може конкурувати з фейковими новинами.** Люди також схильні активніше поширювати інформацію, що містить емоцію злості. До такого висновку дійшли дослідники китайського аналогу Х (Твіттеру) – соцмережі Weibo. Вони виявили, що погане люблять поширювати більше, ніж хороше.

Фейкові фото. Наш мозок обробляє зображення значно швидше, ніж текст. Тому фотографії – ідеальне поле для маніпуляцій. Їх можна відредагувати або використати в іншому контексті. Як розпізнати маніпулятивне фото:

- «дивні» деталі, наприклад, людина тепло вдягнена, а в підписі вказано, що це літо;
- відсутність авторства/джерела фото;
- невідповідність змісту фото темі публікації;
- емоційність фото.

Сьогодні, із появою різних комп'ютерних технологій та інтернету, буквально кожен більш-менш обізнаний користувач може створювати фейкові повідомлення та поширювати їх. Згадайте, наприклад, як за допомогою фоторедакторів ви або ваші знайомі редагували зроблені фотознімки. Із появою штучного інтелекту проблема лише поглибилась. Зараз за допомогою відповідних програм досить легко зробити неправдиве фото. Серед іншого, почастішали випадки створення порнографічного контенту за допомогою штучного інтелекту з використанням фото певних осіб з метою їх подальшого шантажу або помсти (bleepingcomputer.com/news/security/sextortionists-are-making-ai-nudes-from-your-social-mediaimages/). Так, наприклад, для оголення осіб на фото може бути застосований Телеграм-бот @BodyScannerBot. У згаданому контексті однією з небезпечних тенденцій є генерування контенту, який містить зображення насильства, зокрема над дітьми, з використанням систем штучного інтелекту. Зокрема окремі користувачі використовують для генерування подібних зображень продукт stablediffusionweb.com. Так на теперішній час в мережі Даркнет можна знайти тисячі зображень, які містять сцени сексуального насильства над дітьми та оголених дітей, і це насправді є ще одним викликом для правоохоронної системи. Серед інших інструментів, за допомогою яких можна генерувати різноманітний контент, можна згадати Telegram @DeepPaintBot – для покращення якості фото, @qq_2d_ai_bot – для перетворення фото на аніме, @videotoanimebot – для анімації фото у різних стилях, сервіс www deepswap.ai – для заміни обличчя тощо.

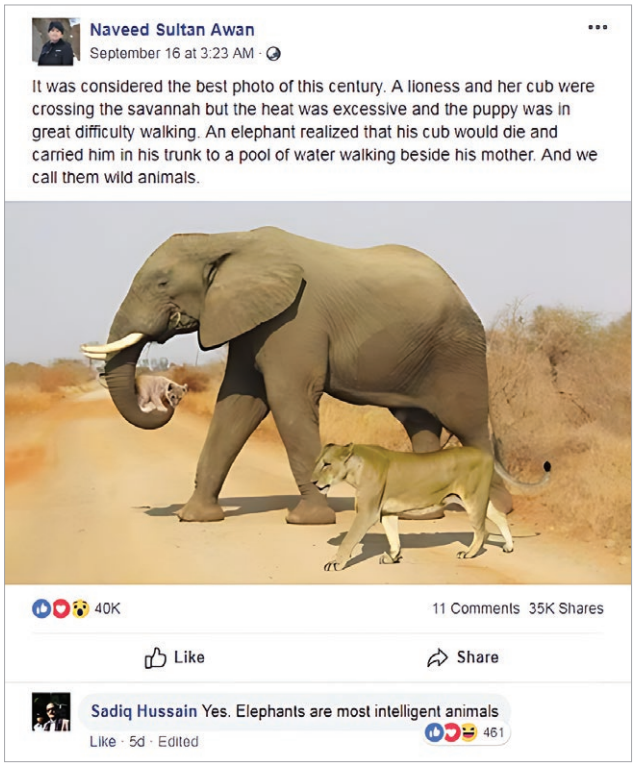
Виокремлюють 3 види маніпуляцій з фото:

- справжнє фото місця чи людини, яке використовують як зображення зовсім іншого місця чи особи, або для маніпуляції з підписом до фото;
- підроблені фото, змінені у графічних редакторах (наприклад Photoshop), щоб додати або прибрати певні елементи;
- обрізані фотографії, які показують лише частину зображення без контексту.

Справжнє фото місця чи людини, яке використовують як зображення зовсім іншого місця чи особи, або для маніпуляції з підписом до фото. Під час російсько української війни у соцмережах поширювалось фото та відео врятованих сиріт. Ці матеріали супроводжувались закликом «швидко всиновити» та про готовність влади України передавати дітей-сиріт у «добрі руки». Центр протидії дезінформації при РНБО України спростував цей фейк.

Підроблені фото, змінені у графічних редакторах (наприклад Photoshop), щоб додати або прибрати певні елементи.

На одному популярному фото зображений слон, який у своєму хоботі несе левеня, а левиця йде поруч. Це зображення з'явилося у мережі X (Твіттер) Національного парку Крюгера у Південній Африці. Як з'ясувалося, це колаж, створений у Photoshop. Фотографії, які використали для цього, можна легко знайти за допомогою зворотного пошуку зображень.



Обрізані фотографії, які показують лише частину зображення без контексту

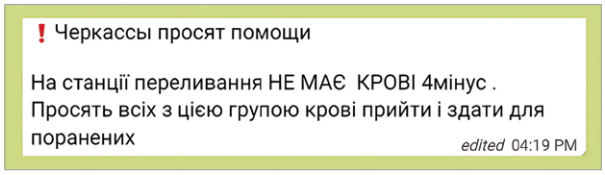
Приклад, як може вплинути на сприйняття та емоції обрізане фото: на першому слайді одинока дівчинка на коліях; на другому – дівчинка на коліях, за якою іде чоловік; на третьому – повна версія фото.

Фейковими можуть бути не лише текст, фото, а й **відео.** Якщо у вас виникли сумніви щодо правдивості відео, зверніть увагу на його **якість**. Варто звернути увагу й на **озвучку**. Адже текст, який супроводжує відео, може суттєво впливати на наше сприйняття. Уважно подивіться, чи відповідає картинка на екрані тому, що говорить тренер/тренерка. Чи застосовується музика або додаткові шуми, звуки? Також важливо дізнатися, хто **автор каналу**, на якому опубліковане відео. Краще не довіряти відео, якщо канал виглядає підозріло. Наприклад, немає аватарки конкретної людини або організації, опису каналу, посилань на офіційний сайт чи інші соціальні медіа. Якщо ви натрапили на популярне відео, але сумніваєтеся, що воно справжнє, **зверніть увагу на коментарі**. Цілком можливо, що хтось вже його спростував. Також можна пошукати ролик за ключовими словами і побачити, чи є інші варіанти відео. У липні 2017 року дослідники університету Вашингтону навчились створювати відео, у яких Барак Обама відкривав рот так, щоб відповідати вхідній звуковій доріжці. Тобто на відео Обама міг говорити будь-який запрограмований текст. Така технологія дозволяє штучному інтелекту вчитися на основі існуючих відео. А потім – замінювати практично будь-яке обличчя у відео на потрібне. Ці фальшиві відеоролики називаються **deepfakes** (глибокі фейки) та

є потужним інструментом дезінформації. Ця технологія може створювати відео чи аудіозаписи публічної особи, яка говорить або робить те, чого ніколи не було в реальному житті.

Проєктом «По той бік новин» розроблено алгоритм побудови фейків з месенджерів.

Наступний приклад фейкового повідомлення отримували мешканці багатьох міст України. Зверніть увагу на погану орфографію та написання міста російською мовою, водночас саме повідомлення написано українською. Також в повідомленні відсутні контакти станції переливання крові. Багато людей, прочитавши його, пішли до місцевих станцій переливання крові, так практично паралізувавши їх роботу.



Пропаганда

Зараз ми часто сприймаємо поняття «пропаганда» з негативним відтінком. Однак спочатку такої конотації не було. Поява терміну «пропаганда» пов'язана з буллою Папи Римського від 22 червня 1622 року, яка називалася Congregatio de Propaganda Fide. Пропаганда слово латинського походження і буквально означає «те, що підлягає поширенню». Це цілеспрямоване поширення ідей і моделей поведінки з метою впливу на суспільну думку. Від звичайного переконування її відрізняють такі риси, як однобокість, масовість, системність і маніпулятивність. Пропаганда небезпечна не лише масовим поширенням часто неправдивої інформації, а й спрямованістю на спонукання її споживачів до певних дій.

Пропаганда грає на тому, що: по-перше, люди – соціальні істоти, тобто ми завжди звертаємо увагу на те, як поводиться наше оточення; по-друге, легше наслідувати зразок, ніж прокла-

дати свій власний шлях, і це стосується моделей поведінки також; по-третє, люди схильні довіряти авторитетам, тому до будь-якої пропаганди неодмінно залучаються лідери думок.

Для поширення пропаганди застосовуються державні інструменти: державні органи, державні медіа, спецслужби, «зливні бачки», боти, тролі, групи у соцмережах тощо. Вплив пропаганди особливо посилюється у разі наявності цензури в країні, оскільки відсутні альтернативні джерела інформації.

Характерні ознаки пропаганди:

- частий повтор – у деталях ці тези можуть відрізнятися, але суть повідомлень одна й та сама;
- створення великої кількості майданчиків, які повторюють тези – однакові ідеї мають звучати з усіх можливих джерел, щоб створити ефект їх безальтернативності та очевидної правдивості;
- спрощення – пропаганда звернена до людей різного віку і з різним рівнем освіти, тому має бути зрозуміла всім (слогани, заклики);
- вплив на почуття, а не на розум. Емоції працюють швидше за логіку.

Пропаганда спрощує сприйняття світу до простої схеми: чорне/біле, вороги/друзі. Образ героя і образ ворога – обов'язкові елементи пропаганди. Впроваджуються як через інформаційні медіа, так і через масову культуру (кіно, серіали, мультфільми, меми), а також проведення заходів. Психологиня Елізабет Лофтус з Каліфорнійського університету досліджує формування фальшивої пам'яті. Вона – одна з авторів концепту **«ефекту хибної інформації»**. Цей ефект з'являється, коли людина намагається щось пригадати. Спогади стають менш точними, конкретні епізоди спотворюються, тому що з'являється інформація після події. Вона змінює наше сприйняття минулого, і, як наслідок, – самі спогади. Це явище вказує на сугестивність (навіювання або піддатливість) та помилку атрибуції пам'яті (наша здатність пам'ятати саму інформацію, але помилятися щодо джерела її походження).

Мета пропагандистів – отримати від нас потрібну поведінку. Водночас людина, яка підпала під маніпуляцію, вважає, що діє за власним бажанням і за власним вибором.

Як протидіяти пропаганді на особистому рівні?

- Визначте емоції, які викликає у вас повідомлення.
- Поставте собі запитання:
  - *На кого спрямоване повідомлення? (Хто цільова аудиторія?)*
  - *До чого воно закликає або спонукає?*
  - *Кому це може бути вигідно?*
- Відокремте факти від суджень та оцінок.
- Перевірте наведені факти.
- Оцініть обґрунтованість суджень.

Під час війни пропаганда набуває особливого розквіту. Бельгійська дослідниця Анна Морелі вивела 10 основних принципів воєнної пропаганди:

- «Ми не хочемо війни».
- «У цій війні винні лише наші противники».
- «Наш ворог – це втілення зла та самого диявола».

- «Ми б'ємося за благородну мету, а не за власні інтереси».
- «Ворог навмисно проявляє жорстокість, інциденти з нашого боку вимушені або випадкові».
- «Ворог використовує заборонену зброю».
- «У нас незначні втрати, водночас втрати ворога – величезні».
- «Визнані артисти та інтелектуали нас підтримують».
- «Наша мета – священна».
- «Кожен, хто ставить нашу пропаганду під сумнів, – зрадник».

Експертна думка

Медіа можуть використовувати думки несправжніх експертів, іноді навмисно, а іноді – випадково. Висловлювання, оцінки та прогнози експертів з сумнівною репутацією завжди слід перевіряти в інтернеті. Так звані «експерти» можуть не бути представниками респектабельних установ чи аналітичних центрів. Навпаки, вони можуть співпрацювати з організаціями, які належать політикам або політичним угрупуванням. Висловлювання таких експертів потрібно сприймати скептично, оскільки може виявитися, що вони не є експертами взагалі, а їхні прогнози чи оцінки – сфабриковані.

В квітні 2023 року українське суспільство сколихнуло розслідування про Спартака Суботу, який називав себе психологом, психотерапевтом, кандидатом психологічних наук, який має досвід роботи в СБУ. У цьому розслідуванні наведені факти та аналіз, які спростовують це.

Тому, якщо маєте змогу, перевіряйте експертів. Ось на що варто звертати увагу:

- освіта та кар'єра. Пошукайте, чим займався експерт раніше, скільки працює в сфері. Також варто поцікавитися освітою експерта.
- місце роботи. Навіть якщо на Фейсбук-сторінці експерта вказаний дослідницький центр, не факт, що такий заклад дійсно існує. Або що в цьому аналітичному центрі працює ще хтось крім самого експерта.
- власники дослідницьких організацій. Прозорість структури власності та фінансування дуже важливі. Більшість дослідницьких центрів в Україні отримують фінансування з чотирьох джерел: грантові кошти, державні замовлення, замовлення аналітики від бізнесу, благодійні внески населення.
- наукові дослідження або статті. Справжні експерти досить часто працюють у дослідницьких центрах, мають наукові ступені, вчені звання та пишуть дослідницькі роботи. Якщо експерта цитують у західних наукових роботах або його роботи публікують у великих наукових журналах, його роботи можна знайти на сайті Google Scholar.
- коло експертних тем. Що кращий експерт, то вужче коло тем він або вона коментують. Експерти, які цінують свою репутацію, завжди відмовляються коментувати тему, яку вони не знають або знають поверхово.
- риторика та категоричність. Хороші експерти завжди обережно роблять висновки, намагаються представити всі можливі погляди та взяти до уваги всі можливі фактори. Тому що гарний експерт – обережний у висновках і розуміє, що несе відповідальність за свої слова, адже вони можуть вплинути на життя багатьох людей.

Прихована реклама/джинса

Медіа повинні дотримуватися балансу між своїми комерційними інтересами та дотриманням стандартів журналістики. Іноді ці поняття змішуються, правила – порушуються і, як результат, аудиторія отримує джинсу – рекламу, замасковану під журналістський матеріал.

Прихована реклама, або джинса, спотворює відображення важливих соціальних явищ та подій. Ми отримуємо неточну та маніпулятивну інформацію, за публікацію якої редактори отримали гроші, але презентували її як новину, а не рекламу. Наприклад, фармацевтична компанія може заплатити виданню за публікацію матеріалу, у якому йдеться про неймовірну користь їх нового вітамінного комплексу.

Як розпізнати приховану рекламу?

- опублікований матеріал не містить жодної прив'язки до місця і часу. Запитайте себе: «Чому цей матеріал опублікували саме зараз?»;
- використання соціологічних досліджень сумнівних організацій, результати яких зазвичай дуже відрізняються від інших соціологічних досліджень;
- один зі стандартів журналістики – дотримання балансу думок. Тому надмірно позитивний або гостро негативний матеріал може бути ознакою прихованої реклами;
- деякі журналісти можуть співпрацювати з політиками чи політичними партіями. Тому багато новин містять їхні коментарі, хоча вони не є експертами;
- матеріали без автора: доволі часто журналісти не хочуть залишати своє ім'я під джинсою, тож багато матеріалів публікують без підпису або під псевдонімом.

Маніпуляція фактами/маніпуляція джерелом

Маніпуляція фактами відбувається тоді, коли подані реальні факти, але вони переакцентовані чи вирвані з контексту, подані неповно, щоб ввести в оману. Ознаками можуть бути: думку подають як факт або факт видають за думку; неправдиві факти, твердження, фальшиві зображення видають за правдиві; правдиву інформацію подають вибірково, наводять найкращі факти для підкріплення своєї заяви і найгірші – для протилежного погляду; замовчують важливі, але не вигідні для себе факти; з несуттєвої частини чи факту судять про ціле або роблять великі прогнози; з правильних припущень роблять маніпулятивний висновок. Маніпуляції можуть бути свідомими або несвідомими, проте вони все одно здатні вплинути на прийняття рішень.

Уявіть ситуацію, коли одна людина стверджує, що йде дощ, а інша – заперечує це. Кому б ви повірили? Звісно, ви б просто подивилися у вікно та перевірили, хто має рацію. Це називається перевіркою джерела – ми звертаємося до першоджерела інформації, до первинних документів або до людей, які були присутні під час події.

Першоджерелами можуть бути:

- офіційні пресрелізи урядових та судових органів, місцевих органів влади та міжнародних організацій;
- офіційні листи, звернення та запити на інформацію;
- повідомлення з місця подій (без редагування та коментування);
- офіційні вебсторінки організацій;
- люди, особисто причетні до події, зокрема свідки.

Якщо ви не можете визначити першоджерело, слід обережно ставитися до запропонованої інформації.

Іноді медіа оприлюднюють інформацію з посиланнями на анонімні джерела. Це може статися через різні, цілком обґрунтовані причини. Але навіть якщо ці причини виправдані, інформацію з анонімного джерела неможливо перевірити. У такому разі подумайте, чи має причина замовчування джерела сенс у контексті запропонованої інформації.

Заняття 1.7.2. Інструменти перевірки інформації

Мета: надати учасникам інформацію про сучасні інструменти перевірки достовірності інформації та сприяти формуванню навичок критичного аналізу медіаконтенту.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Інструменти перевірки інформації	Інформаційне повідомлення	15 хв	Додаток 1.7.2.1, мультимедійне обладнання, доступ до інтернету
2.	Що ми знаємо про джерело?	Вправа	10 хв	Додаток 1.7.2.2, мультимедійне обладнання, доступ до інтернету
3.	Базові правила фактчекінгу та пошуку інформації	Робота в групах	30 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.7.2.3
4.	Інформаційна бульбашка	Вправа	10 хв	Мультимедійне обладнання, доступ до інтернету, Додатки 1.7.2.4, 1.7.2.5
5.	Чи це правда?	Вправа	25 хв	Мультимедійне обладнання, доступ до інтернету, Додаток 1.7.2.6

ХІД ЗАНЯТТЯ

1. Інформаційне повідомлення «Інструменти перевірки інформації»

Мета: надати учасникам інформацію про сучасні інструменти перевірки інформації.

Час: 15 хв.

Необхідні матеріали: Додаток 1.7.2.1, мультимедійне обладнання, доступ до інтернету.

Хід проведення:

Тренер/тренерка зазначає: *«Насправді ми відіграємо важливу роль у медіапросторі, адже саме ми поширюємо інформацію в соціальних мережах та усно. Щоразу, коли ми пасивно сприймаємо та поширюємо контент без належної перевірки, ми збільшуємо шум і плутанину, які вже існують у перенасиченому інформаційному середовищі. Отже, ми несемо таку саму відповідальність за перевірку інформації, яку поширюємо, як і її автори.*

Якщо ви не впевнені, чи історія є правдивою, зверніть увагу на такі поради:

***1. Прочитайте** – звертайте увагу на незвичайні URL-адреси чи назви сайтів. Вони часто намагаються виглядати як справжні новинні сайти, але можуть бути не такими. Шукайте ознаки граматичних чи орфографічних помилок, відсутність посилань на джерела чи використання «зображень-приманок». Не обмежуйтеся лише заголовком, прочитайте всю історію.*

***2. Зачекайте** – якщо щось розповсюджується в соціальних мережах величезною кількістю разів, це не означає, що це правда. Якщо інформація виглядає надто добре, щоб бути правдою, то, ймовірніше, так і є.*

***3. Перевірте** – дізнайтеся, хто є автором інформації. Ви можете перевірити автора на сайті або зайти на сторінку «Про нас» чи «Контакти», щоб дізнатися більше про особу чи організацію. Використовуйте Google для пошуку додаткової інформації про цю особу чи*

організацію, щоб упевнитися, що вони є тими, за кого себе видають. Існує кілька способів протидії неправдивим повідомленням, які можна розділити на логічні, технічні та комбіновані. Найбільш простими та дієвими ***логічними*** *способами є такі:*

- *критичне осмислення будь-якої інформації та підвищення власної медіаграмотності;*
- *під час сприйняття інформації намагайтеся більше керуватися розумом, а не емоціями;*
- *перевіряйте факти, які бачите в соціальних мережах, перш ніж довіряти їм;*
- *звертайте увагу на дату, джерело та справжність фото;*
- *намагайтеся знайти першоджерело відповідного інформаційного повідомлення;*
- *звертайте увагу на репутацію інформаційних ресурсів, віддавайте перевагу авторитетним та офіційним джерелам;*
- *перевіряйте інформацію з кількох джерел;*
- *відповідально ставтеся до використання соціальних мереж, періодично переглядайте та видаляйте рекламні уподобання;*
- *беріть на себе зобов'язання прочитати весь текст, а не лише заголовки, перш ніж поширювати публікацію».*

Далі тренер/тренерка презентує інформацію про **технічні** інструменти перевірки інформації із Додатка 1.7.2.1.

Підсумовуючи, тренер/тренерка зазначає: «*Пам'ятайте: якщо у вас виникають сумніви щодо правдивості, не діліться нею на соціальних платформах, щоб запобігти поширенню і потенційному введенню в оману інших. Особливо важливо враховувати, що інформація, яку поширюють офіційні особи, зокрема поліцейські, сприймається суспільством з більшою ймовірністю як правдива».*

До уваги тренера/тренерки!

Під час підготовки до заняття слід перевірити актуальність інформації, наведеної у Додатку, та, за необхідності, оновити чи додати нові інструменти перевірки інформації.

Можна не презентувати всі інструменти, зосередити увагу на окремих з них, зокрема тих, які сам/сама тренер/тренерка використовує та має змогу продемонструвати їх роботу наочно. Наприклад, за наявності часу та технічної можливості, можна задати будь-яке питання ChatGPT, скопіювати отриману відповідь та використати ресурс ZeroGPT для перевірки отриманої відповіді.

Запитання для обговорення:

- *Які інструменти перевірки інформації ви зазвичай використовуєте?*
- *Хто, на вашу думку, повинен відповідати за блокування та видалення недостовірної інформації? Це завдання адміністраторів соціальних мереж, чи ми повинні брати на себе певну відповідальність як користувачі?*
- *На вашу думку, чи сучасні діти обізнані з інструментами перевірки інформації? З якого віку, на вашу думку, слід навчати дітей інструментам перевірки інформації?*

До уваги тренера/тренерки!

Слід наголосити, що сучасні діти звикли використовувати інтернет для пошуку інформації – для домашніх завдань, шкільних проєктів чи просто для розваги. Кількість користувачів

інтернету у світі, за даними Internet World Stats (IWS), становить 5,4 млрд людей за населення 7,9 млрд людей. 1 з 3 користувачів інтернету у світі – дитина. Діти мають цифровий слід ще до того, коли починають ходити та говорити. З одного боку, цифрове середовище забезпечує дітям можливість навчатись, спілкуватись, розважатись, а з іншого – є джерелом підвищеного ризику зіткнення з деякими загрозами віртуального світу: від кібернасильства та шахрайства до сексуальної експлуатації та схиляння до самогубства. Діти повинні здобути важливу життєву навичку – уміння опрацьовувати та відфільтровувати потік інформації. Щоб досягти цього, потрібно тренувати критичне мислення та навчитися використовувати інструменти перевірки інформації.

Відповідно до Закону України «Про медіа» *забезпечення формування та реалізації державної політики з питань медіаграмотності покладається на центральний орган виконавчої влади, що забезпечує формування та реалізацію державної політики в інформаційній сфері (Міністерство культури та інформаційної політики України)*. Також впроваджувати ефективні заходи та інструменти медіаграмотності, підвищувати обізнаність користувачів щодо таких заходів зобов'язані провайдери платформи спільного доступу до відео. Крім того, *Національна рада України з питань телебачення і радіомовлення* зобов'язана самостійно або у співпраці з центральним органом виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері медіа, іншими державними органами, органами місцевого самоврядування, освітніми установами, громадськими об'єднаннями розробляти та впроваджувати проєкти, виставки, друковані та електронні публікації, вебсайти, аудіовізуальні продукти, ігри та інші заходи з метою підвищення медіаграмотності.

2. Вправа «Що ми знаємо про джерело?»

Мета: сформувати вміння аналізувати джерело інформації.

Час: 10 хв.

Необхідні матеріали: Додаток 1.7.2.2, мультимедійне обладнання, доступ до інтернету.

Хід проведення:

Тренер/тренерка виводить на екран слайд, який міститься у Додатку 1.7.2.2 та пропонує учасникам, використовуючи мобільні телефони:

- знайти цю новину;
- визначити, чи відповідає вона дійсності;
- надати характеристику сайту, на якому вона розміщена.

До уваги тренера/тренерки!

Для зручності та економії часу можна вивести на екран QR-код з посиланням на джерело. Для проведення вправи можна обрати іншу новину з цього сайту.

Після висловлення учасниками своїх думок тренер/тренерка звертає їхню увагу на те, що наприкінці сторінки сайту міститься інформація про нього, де безпосередньо зазначено, що «*UaReview – сатиричне онлайн-видання, що публікує вигадані новини українською*». Після цього доцільно вивести на екран Рис. 2 із Додатка 1.7.2.2, на якому видно, що деякі інші видання передрукували цю новину. Резюмуючи, слід звернути увагу учасників на важливість перевірки джерела походження інформації.

Запитання для обговорення:

- *Чи перевіряєте ви джерело інформації?*
- *Уявіть, що ви почули, що всі школи більше не вимагатимуть від учнів носити форму. Куди б ви пішли перевірити, правда це чи ні?*
- *На що слід звертати увагу під час перевірки джерела інформації?*
- *Як спонукати дітей перевіряти інформацію?*

3. Робота в групах «Базові правила фактчекінгу та пошуку інформації»

Мета: актуалізувати та систематизувати знання учасників щодо базових правил фактчекінгу та ефективного онлайн-пошуку.

Час: 30 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.7.2.3.

Хід проведення:

Тренер/тренерка об'єднує учасників у чотири групи, дає кожній із них аркуш для фліпчарту та маркери та оголошує завдання:

Групи 1 та 2 мають зазначити на своїх аркушах базові правила критичного аналізу інформації, тобто, на що саме слід звертати увагу під час ознайомлення з медіаконтентом;

Група 3 та 4 зазначають поради для ефективного онлайн-пошуку.

На роботу в групах відводиться 10 хвилин, після чого група 1 та група 4 протягом п'яти хвилин демонструють напрацювання, інші групи – доповнюють їх.

Тренер/тренерка може доповнювати презентації учасників, використовуючи матеріал, який міститься у Додатку 1.7.2.3.

Запитання для обговорення:

- *Хто, на вашу думку, має навчати дітей критичному аналізу інформації та правилам ефективного онлайн-пошуку?*
- *З якого віку, на вашу думку, слід навчати дітей цим правилам?*

4. Вправа «Інформаційна бульбашка»

Мета: надати інформацію щодо ефекту інформаційної бульбашки та спонукати учасників вживати заходів для запобігання потрапляння в неї.

Час: 10 хв.

Необхідні матеріали: Додатки 1.7.2.4, 1.7.2.5, мультимедійне обладнання, доступ до інтернету.

Хід проведення:

Тренер/тренерка зазначає: «*Інтернет об'єднав людей з усієї планети й навіть за її межами. Алгоритми соціальних мереж і пошукових систем розділили нас на групи за інтересами, уподобаннями, професіями, місцем розташування. Ці групи часто перетинаються в одних точках і віддаляються в інших. Кожен живе у своїй інтернет-реальності, яку умовно можна назвати «інформаційною бульбашкою». Інформаційні бульбашки спотворюють наше сприйняття реальності. Нам здається, що світ переважно такий, яким ми його бачимо на екрані смартфона чи комп'ютера. Ми прагнемо чути й бачити те, з чим ми згодні, що нам подобається. Все, що не вписується в цю картину, ми сприймаємо негативно або навіть вороже. Це робить нас вразливими до маніпуляцій і фейкової інформації, і ми починаємо толерувати мову ненависті й агресію проти тих, хто має інший погляд. Ось у чому полягає основна небезпека бульбашок. Щоби уникнути ефекту інформаційної бульбашки,*

варто іноді читати й переглядати ті канали, де транслюється інший погляд. Ви можете й далі не погоджуватися з ними, але тепер ви будете знати аргументи інших, альтернативні думки та інтерпретації. У цьому балансі ви зможете загартовувати своє критичне мислення та перевіряти факти, в яких раніше були впевнені».

До уваги тренера/тренерки!

Більш детально про ефект «інформаційної бульбашки» та його вплив можна дізнатись із Додатка 1.7.2.4.

Якщо є час та технічна можливість, доцільно продемонструвати учасникам ефект «інформаційної бульбашки» на прикладі пошуку за запитом «гольф» з акаунту тренера/тренерки та декількох присутніх учасників. Система ймовірніше видасть різні результати: про спортивну гру, вид одягу, а також модель авто марки Volkswagen. Те саме можна зробити зі словом «поло». Ми побачимо, що система проаналізує попередні пошуки, покаже варіанти магазинів чи автоцентрів для купівлі одягу, авто, матеріали про гру. Але в кожного буде різний порядок цих результатів і чим далі ми гортатимемо сторінку з результатами, тим більше вони відрізнятимуться. Це і є приклад нашої інформаційної бульбашки.

Як альтернативу для аналізу учасниками власного медіаполя на наявність ознак «інформаційної бульбашки» можна провести вправу «Бінго», інструкція щодо якої міститься в Додатку 1.7.2.5.

Запитання для обговорення:

- *Які загрози для дітей може мати потрапляння в «інформаційну бульбашку»?*
- *Як можна вирватись із «інформаційної бульбашки»?*

Вправа «Чи це правда?»

Мета: відпрацювання вміння розрізняти достовірну та маніпулятивну інформацію з використанням інструментів перевірки інформації.

Час: 25 хв.

Необхідні матеріали: мультимедійне обладнання, доступ до інтернету, Додаток 1.7.2.6.

Хід проведення:

Тренер/тренерка об'єднує учасників у три групи та надає кожній із них матеріали з Додатка 1.7.2.6. Завдання учасників полягає в тому, щоб протягом десяти хвилин, використовуючи інструменти критичного аналізу інформації, визначити, чи надана їм інформація є правдивою.

До уваги тренера/тренерки!

Під час підготовки до заняття тренер/тренерка може самостійно підібрати інформацію з медіа для аналізу.

Для підготовки завдань для роботи в групах також можна використати гру «Конструктор квестів» за посиланням: https://vspu.edu.ua/faculty/lingvo/game.php, розроблену Національним проєктом з медіаграмотності «Фільтр» Міністерства культури та інформаційної політики України. На сайті цього проєкту можна також знайти інші тематичні ігри та завдання.

Після закінчення часу на роботу в групах кожна із груп протягом трьох хвилин демонструє свої напрацювання, інші учасники та тренер/тренерка можуть надавати коментарі.

Запитання для обговорення:

- *Чи складно було виконати завдання?*
- *Які інструменти або правила перевірки інформації ви використовували?*

Тестові питання до заняття:

1. Що таке «інформаційна бульбашка»?

А) люди отримують лише ту інформацію, яка підтримує їхні погляди;

Б) спосіб накопичення інформації в редакції;

В) неперевірена інформація в медіа;

Г) складно відповісти.

2. Під час перевірки інформації слід звертати увагу на:

А) дату;

Б) справжність фото;

В) джерело інформації;

Г) всі відповіді правильні.

3. Що із переліченого може бути використано як інструмент перевірки інформації?

А) Google Images;

Б) Fake news debunker by InVID & WeVerify;

В) Am I Real?;

Г) всі зазначені інструменти можуть бути використані для перевірки інформації.

4. Яке сполучення літер слід додати до пошукового запиту як ключове слово, щоб у результатах пошуку були відображені вебсайти державних органів?

А) .ua;

Б) .com;

В) .gov;

Г) .file.

5. Яка державна інституція забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері?

А) Центр стратегічних комунікацій при Міністерстві культури та інформаційної політики України;

Б) Центр протидії дезінформації при РНБО України;

В) чат-бот «ПЕРЕВІРКА»;

Г) всі відповіді правильні.

Ключі-відповіді:

1. А; 2. Г; 3. Г; 4. В; 5. Б.

Додаток 1.7.2.1

«Достовірна інформація може стати рятівною під час гуманітарних криз, але умови виникнення останніх є зазвичай найскладнішим часом для збору перевірених даних»

Уільям Спіндлер, представник Управління Верховного комісара ООН у справах біженців (УВКБ ООН)

Для перевірки повідомлень та інших матеріалів щодо їх актуальності та достовірності можуть бути використані різні аналітичні методи. Для полегшення цього процесу також варто застосовувати і низку технічних рішень.

Перевірка джерела інформації, власника медіа, достовірності інформації та фото/відео

Для перевірки фото і відео можна використовувати такі сервіси:

- **RevEye Reverse Image Search** – допоможе шукати фотографію в різних пошуковиках, щоб знайти першоджерело. Подібним до описаного розширення є **«Fake news debunker by InVID & WeVerify»**.
- **Google Images** – дозволяє знайти схожі зображення. Так, наприклад, за допомогою цього сервісу знайдений оригінал фото, з якого був зроблений фейк про Королеву Великобританії, вдягнену в українську вишиванку.

- **Google Fact Checker** – ресурс, за допомогою якого можна перевірити правдивість інформації, а також переглянути результати раніше зроблених запитів для перевірки.
- **AnalogExif** – утіліта, яка дає змогу перевірити метадані (дата, координати місця створення тощо) фото.
- **FotoForensics** – сервіс перевірки фотографій, який має зокрема функцію, що аналізує рівень стискання зображення, який на оригінальному фото має бути однаковим. Якщо якась деталь додана штучно, вона підсвічуватиметься білим.
- **Fake Profile Detector (Deepfake, GAN)** – розширення, яке дає змогу ідентифікувати зображення, створені з використанням штучного інтелекту. Саме тому, якщо обличчя реальної людини додано до іншого зображення, воно теж визначатиметься як справжнє.
- **Am I Real?** – сервіс, який допомагає визначити, чи створене зображення за допомогою ресурсу thispersondoesnotexist.
- **Deepfake Detection** – розширення, призначене для виявлення DeepFake-відео в сервісі Ютуб. Також для ідентифікації фейкового відео призначено сервіс **Scan & Detect Deepfake Videos**.
- **GPTZero** – ресурс для аналізу тексту на предмет його створення за допомогою штучного інтелекту.

- **Webmii** (https://webmii.com/) – пошук згадок та посилань на особу в інтернеті, допомагає визначити несправжні облікові записи.
- **@OpenDataUABot** – Телеграм-бот, за допомогою якого можна знайти інформацію з відкритих баз даних з публічною інформацією.
- **Wayback Machine** – інструмент, за допомогою якого можна знайти видалені сторінки, або, наприклад, побачити, який вигляд мала головна сторінка медіа якогось місяця чи року.
- **StopFake** – проєкт викриває фейки рф й поширює спростування тринадцятьма мовами.
- **«По той бік новин»** – проєкт спростовує побутові та щоденні фейки та маніпуляції.
- **Чат-бот «ПЕРЕВІРКА»** – бот для перевірки сумнівної інформації та новин від українських журналістів. Також містить тести з медіаграмотності та кібергігієни загалом.
- **GwardaMedia** – незалежне цифрове медіа, яке займається й аналізом достовірності інформації, зокрема здійснює адміністрування чат-боту «ПЕРЕВІРКА».
- **«Нотаєнота»** – аналізує та спростовує або підтверджує розповсюджену у медіа інформацію, яка викликає суспільний резонанс.
- **«Як не стати овочем»** – волонтерський просвітницький проєкт з інформаційної гігієни.

Державні ініціативи:

- **Центр протидії дезінформації при РНБО України** є робочим органом Ради національної безпеки і оборони України, утвореним відповідно до рішення Ради національної безпеки і оборони України від 11 березня 2021 року, введеного в дію Указом Президента України від 19 березня 2021 року № 106. Центр забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою.
- **Центр стратегічних комунікацій** створений при Міністерстві культури та інформаційної політики України як один з механізмів протидії дезінформації спільними зусиллями держави і громадянського суспільства.
- **Національний проєкт з медіаграмотності «Фільтр» Міністерства культури та інформаційної політики України** – на сайті національного проєкту з медіаграмотності «Фільтр» можна знайти широкий спектр ресурсів для прокачування медіаграмотності. Тут зібрані найкращі закордонні та вітчизняні матеріали для вчителів та учнів, батьків, викладачів та студентів, журналістів, а також для широкої аудиторії.

Соцмережі та месенджери. В соціальних мережах ви завжди можете поскаржитися на публікацію, якщо ви думаєте, що це неправда. За посиланням ви можете знайти інструкції, як це зробити у найбільш розповсюджених соціальних мережах та месенджерах, а також в Ютубі. У разі масового надходження скарг на публікацію, соціальні мережі можуть блокувати публікацію або додавати до публікації повідомлення про неправдивість інформації.

Ресурси для вдосконалення власної медіаграмотності

Онлайн-курси		
Very Verified: онлайн-курс з медіаграмотності	https://verified.ed-era.com/ua	
Дія. Освіта. Основи кібергігієни: онлайн-серіал з основ кібергігієни для держслужбовців	https://osvita.diia.gov.ua/courses/cyber-hygiene	
Prometheus. Інформаційна гігієна під час війни	https://courses.prometheus.org.ua/courses/course-v1:Prometheus+IHWAR101+2022_T2/about	
Онлайн-курс «Як захистити власну цифрову ідентичність» від Українського інституту медіа та комунікацій	https://e-courses.jta.com.ua/%D0%B5-courses/how-to-protect-personal-digital-identity/	

Додаток 1.7.2.2

UaReview

Україна Політика Кримінал **Наука і IT** Культура Фотофакт | Про проєкт Приєднатись Фейкові новини Підтримати Patreon

← Більшість артистів в ефірі московського «Блакитного вогника» виступали мертвими Фільм «Памфір» реанімував легендарний гурт Slayer →

Київський школяр винайшов спосіб видобувати електроенергію зі злості

Опубліковано 17.02.2023, 00:56

Школяр 7 класу з Києва Георгій Баратенюк самотужки розробив прилад для отримання електроенергії з негативних людських емоцій. Про це повідомляє видання "Останній дзвоник онлайн".

Реклама

Останні новини

Фільм «Памфір» реанімував легендарний гурт Slayer

Київський школяр винайшов спосіб видобувати електроенергію зі злості

Більшість артистів в ефірі московського «Блакитного вогника» виступали мертвими

Тисячі росіян вийшли на мітинги в підтримку телеканалу "Дождь"

Власники синьої галочки у Twitter зможуть редагувати твіти, — Ілон Маск

Для економії електроенергії телемарафон стане газетою

Пес Патрон розкритикував дії свого колеги в студії телемарафону

Ілон Маск планує одружитись з Юлією Чичеріною

Росіяни за межами росії вийшли на мітинги за те, що вони нікому нічого не винні

Лисого з Brazzers бачили неподалік Щекавиці

Вибір редакції

Затриманого на хабарі дуже бідного чиновника пожаліли і відпустили

Рис. 1.

Google Київський школяр винайшов спосіб видобувати електроенер

Усі Зображення Новини Відео Карти Більше Інструменти

Приблизна кількість результатів: 15 400 (0,57 с)

uareview.com
https://uareview.com › elektroenerhia-zi-zlosti

Київський школяр винайшов спосіб видобувати ... - UaReview

Школяр 7 класу **з** Києва Георгій Баратенюк самотужки розробив прилад для отримання **електроенергії з** негативних людських емоцій.

https://uareview.com › 2023/02

Лютий – 2023 - UaReview

Київський школяр винайшов спосіб видобувати електроенергію зі злості ... Школяр 7 класу з Києва Георгій Баратенюк самотужки розробив прилад ...

ujournal.com.ua
https://ujournal.com.ua › post

Київський школяр винайшов спосіб видобувати ... - UJournal

Школяр 7 класу **з** Києва Георгій Баратенюк самотужки розробив прилад для отримання **електроенергії з** негативних людських емоцій. Про це повідомляє видання ...

pro.te.ua
https://pro.te.ua › 2023/04/03 › shkolyar-vynajshov-s...

Школяр винайшов спосіб видобувати електроенергію зі ...

3 квіт. 2023 р. — **Школяр** 7 класу **з** Києва Георгій Баратенюк самотужки розробив прилад для отримання **електроенергії з** негативних людських емоцій.

Відсутні: ~~Київський~~ | Показати результати, які містять: Київський

Рис. 2.

Додаток 1.7.2.3

У нас є лише 24 години у добі, які точно не можна витратити лише на перевірку всієї інформації, яку ми споживаємо. Краще навчитись перевіряти інформацію швидко.

Базові правила критичного аналізу інформації

Емоційна мова та лексика. Це правило стосується заголовку, тексту новини або посту. Якщо лексика емоційна, спричиняє обурення або, навпаки, позитив – **дуже ймовірно, що перед вами неправдива інформація.** Відповідно до стандартів журналістики, **заголовки та статті мають бути нейтральними** та подавати сухі факти. Що більше емоцій викликає заголовок або текст, то більша ймовірність, що вам намагаються нав'язати недостовірну інформацію. **Приклади емоційних фраз:** горезвісний, одіозний, так званий, погано пахне, викликає сумніви. А ще – фрази, виділені капслоком: ШОК! СЕНСАЦІЯ! НАЙБІЛЬША ПРАВДА, ВАШЕ ЖИТТЯ ЗМІНИТЬСЯ, КОЛИ ВИ ДІЗНАЄТЕСЬ ЦЕ!

Чого більше у тексті – фактів чи суджень? Професійні журналісти не мають нав'язувати власні думки. Якщо текст публікується як думка журналіста, він обов'язково має бути промаркований як «блог», «погляд» тощо.

Остерігайтеся «вау» – емоції підживлюють фейкові новини. Коли ви бачите щось, що змушує вас почуватися надзвичайно сумним або надзвичайно щасливим, можливо, це грає на ваших емоціях, щоб викликати реакцію.

Остерігайтеся перебільшень: такі слова, як «жахливий», «найгірший», «дивовижний» або «шокуючий», додають історії драматизму та викликають у нас бажання натиснути на неї.

Хто експерти та очевидці? Очевидці не можуть бути єдиними джерелом інформації – адже, як і всі люди, вони також можуть подавати її суб'єктивно. Зверніть увагу на словосполучення: «експерти вважають»**, «**джерело в Адміністрації Президента», «чиновник в Міністерстві фінансів», «депутат, який брав участь в обговоренні», тощо. Якщо журналіст спілкувався з експертами або представниками влади, то обов'язково наведе їхні цитати та імена. Важливо, щоб людина, яка намагається пояснити ситуацію, була справді спеціалістом у цій галузі. Звертайте увагу на те, що саме говорить експерт: це загальні фрази, емоційні заяви чи факти? Пошукайте їх в пошуковику або на сайтах організацій, про які вони згадують у своїх профілях в соціальних мережах. Зазирніть на сторінку webmii.com. Цей ресурс шукає цифрові сліди за іменем людини, а також показує рівень її активності в мережі.

Зверніть увагу на фото. Чи новина, яку ви читаєте, супроводжується фотографією, яка вам здається вирваною з контексту? Виконайте пошук в інтернеті, можливо, це допоможе вам зрозуміти, що це приклад дезінформації.

Дата публікації. Часто під виглядом новини нам подають «старини» – новини, які були актуальними багато років тому. І, можливо, навіть в іншій країні. Доволі часто це відбувається, коли фото до публікації містить слова «Сьогодні», «Терміново» тощо, тому слід звертати увагу на дату публікації, а не лише на текст.

Боріться з «ефектом ілюзорної правди» – чим більше ви чуєте або бачите щось, тим більше шансів повірити, що це правда – навіть якщо це не так. Неправдиві повідомлення дуже небезпечні та набувають популярності лише тоді, коли громадськість ділиться ними через соціальні мережі та месенджери. Дослідження виявили, що чим більше людей робить репост, тим більша ймовірність поширення. Чим вище залученість, тим менша ймовірність, що люди перевірять факти.

Перевірте свою «бульбашку фільтрів» – соціальні мережі та реклама створені, щоб пропонувати історії, які відповідають вашим звичкам вебперегляду, інтересам і думкам.

Два основних **правила інформаційної гігієни:**

1) не ставте «вподобайку», якщо не прочитали матеріал;

2) не поширюйте сумнівну інформацію.

Якщо ви зіткнулися з неправдивою інформацією, не коментуйте і не діліться далі. Це лише допоможе зробити допис більш популярним. Якщо публікацію поширили в соціальних мережах, повідомте про неї платформі. Якщо ви знаєте людину, яка поширила фейкові новини, надішліть їй приватне повідомлення та скажіть, що інформація, яку вони опублікували, ймовірно, неправдива.

Поради ефективного онлайн-пошуку

Успіх пошуку залежить від того, наскільки Google або інший пошуковик зрозуміє, що саме ви від нього хочете. Під час перевірки інформації варто користуватись ключовими словами, часовими межами та операторами (Рис. 1).

tik-tok intitle:how to

Приклад використання заголовка під час пошуку в Google

inflation filetype:xls site:gov.ua

Приклад використання формату файла під час пошуку в Google (2)

inflation filetype:xls

Приклад використання формату файла під час пошуку в Google (1)

jaguar-car-automobile

jaguar+car+automobile

Приклад використання слів із «+» та «-» під час пошуку в Google

site:kyivindependent.com

Приклад використання доменів під час пошуку в Google

Рис. 1.

- Використовуйте конкретні описові ключові слова для звуження пошуку та одержання точніших результатів.

Приклад. У разі використання для пошуку слова «концерти», ви одержите інформацію про різні музичні заходи, можливості придбання квитків і дати їх проведення. У разі використання для пошуку слів «класичний концерт Антоніо Бочеллі», ви одержите точніші результати про локальний захід.

- Якщо перша спроба не є результативною, використовуйте синоніми.

Приклад. Якщо ви зробили спробу знайти «рідкісні коти», однак не знайшли те, що шукали, спробуйте використати слова «екзотичні коти», «рідкісні породи котів» або «екзотичні породи котів».

- Використовуйте лапки для виділення конкретних слів або конкретних фраз, які ви шукаєте.

Приклад. Якщо вам необхідна інформація про резиденцію президента, використовуйте словосполучення «Білий дім», а не білий дім.

- Пошук з виключенням певного слова.

Приклад. Якщо вам необхідна інформація про Університет Грінченка, але в пошуковій системі ви знаходите коледж та університет, використовуйте символ мінус «-». Наприклад: «університет – коледж». Так ви будете знаходитити інформацію, яка буде стосуватись лише запиту «університет».

- Пошук і зосередження уваги на типах доменів URL.

Приклад. Якщо ви шукаєте інформацію про парки і використовуєте сполучення літер .gov як ключове слово, у результатах вашого пошуку будуть вебсайти державних органів. Якщо ви шукаєте інформацію про парки і використовуєте сполучення літер .com як ключове слово, ви одержите інформацію про приватні парки.

- Визначте формат інформації, яка вам необхідна.

Якщо ви шукаєте інформацію про «військову техніку XX сторіччя», ви одержите цю інформацію у різних аспектах: блоги, новини, фотографії, пости, посилання на заходи, виставки, новини, що стосуються цієї теми.

Приклад. Велика кількість пошукових систем забезпечують можливість здійснювати пошук лише зображень, відео, новин, блогів або навіть наукових статей.

- Використовуйте хештеги для пошуку інформації. Хештеги допомагають знайти інформації з різних сфер та джерел, забезпечують швидкий пошук по темах, що цікавлять.

- Використовуйте якомога більше джерел інформації.

Приклад. Пошукові системи нададуть вам доступ до великої бази даних інформації в інтернеті. Не дивіться на перші результати і не використовуйте лише відомі вам джерела, зокрема Wikipedia. Намагайтесь використовувати якомога більше джерел інформації.

Додаток 1.7.2.4

Інформаційна бульбашка

Хто вирішує, що ви бачите у своїй стрічці новин? Фейсбук, якому належить Інстаграм, та Гугл, якому належить Ютуб, досить добре вміють показувати вам те, що ви хочете, і приховувати ідеї, які вам не подобаються або з якими ви не погоджуєтеся. Усе, що суперечить вашим поглядам, відфільтровують, і ви опиняєтеся в **«інформаційній бульбашці»** – явище, яке обмежує доступ людини до повного спектру новин та іншої інформації в інтернеті за допомогою алгоритмічного визначення пріоритетів вмісту, який відповідає демографічному профілю користувача та онлайн-історії, або виключаючи вміст, який йому не відповідає. Термін запропонував інтернет-активіст Елі Парайзер.

Як працює інформаційна бульбашка?

Уявімо, що у вас є два друга на Фейсбук. Один підтримує вакцинацію, інший – ні. Якщо ви «за» вакцинацію, то будете більше «лайкати» та коментувати лише одного друга. Тоді повідомлення того, хто не підтримує вакцинацію, автоматично зникнуть з вашої новинної стрічки. Так ви опинитесь у середовищі людей, з думкою яких погоджуєтеся. Це і є **ефект інформаційної бульбашки** [*filter bubble*] – обмежений інформаційний простір, де світ сприймається однобоко та відповідно до наших уявлень. Інформаційні бульбашки – чудове середовище для поширення неправдивих повідомлень. Якщо фейк потрапив у вашу бульбашку, інформаційний простір буде розривати від неправдивої інформації. І тому, найімовірніше, ви в неї повірите. Без фільтрів ви могли б загубитися в усій інформації, що доступна онлайн. Але, з іншого боку, ви не отримуєте важливу інформацію, яку алгоритми, після аналізу вашої поведінки та інтересів, вважають нецікавою для вас. Вебсторінки можуть застосовувати алгоритми, які відстежують, що ви шукаєте, на що натискаєте, що вам «подобається» або «не подобається», що ви коментуєте і де перебуваєте. Ці алгоритми аналізують усю цю особисту інформацію і за допомогою шаблонів вирішують, що саме ви хочете бачити. Це означає, що пошукові результати, посилання, реклама та дописи у Фейсбуці можуть бути результатом вашої попередньої поведінки онлайн. Наприклад, якщо ви шукали в Гугл інформацію про зміну клімату, ваша стрічка новин може наповнитися дописами, статтями та відеороликами екологічних організації.

Що ви можете зробити, аби звільнитися від інформаційної бульбашки?

- Використовуйте браузер в режимі «Інкогніто», періодично видаляйте історію пошуку, кукіс (реп'яхи, які чіпляються за вас під час візитів на сайти і допомагають їм запам'ятати вас) і намагайтеся рідше реєструватися на сайтах через ваші профілі в соцмережах.
- Свідомо шукайте альтернативну інформацію з різних джерел. Наприклад, якщо ви все життя вірили, що їжу не можна запивати водою, можна ввести пошуковий запит із запитанням: «вода під час їжі за і проти». Запитуйте себе: чому люди можуть мати інші погляди?
- Читайте новини безпосередньо з новинних сайтів, а не натискайте на посилання у соціальних медіа. Перевіряйте джерела інформації. Дуже легко забути про думки інших, якщо ви бачите інформацію, з якою погоджуєтеся. Особливо якщо її поширили ваші друзі у Фейсбуці або люди, яких ви поважаєте.
- Коли ви бачите заголовок, який змушує думати, що стаття вам не сподобається, спробуйте дати їй шанс. Ви не зобов'язані змінити думку, мета – побачити ситуацію з іншого боку.

Додаток 1.7.2.5

Бінго «Інформаційна бульбашка»

Обведіть твердження, з якими ви погоджуєтеся

Я отримую новини із соціальних мереж та сторінок своїх друзів	У моїй стрічці більше думок, з якими я погоджуюся, ніж ні	Я ставлю більше «лайків», ніж смайлів «обурення»
Я відписуюся від тих, хто зі мною не погоджується	Усі мої друзі голосували за того самого політичного кандидата, що і я	У коментарях до моїх постів всі погоджуються з моєю думкою
Я не розглядаю аргументи, які суперечать моїм переконанням та світогляду	Я не видаляю кукіс (cookies) зі своїх пристроїв (або не знаю, що це)	Коли я бачу заголовок, з яким миттєво не погоджуюся, я не читаю статтю

Якщо ви обвели три твердження підряд по діагоналі, вертикалі або горизонталі – бінго! Схоже, ви у «бульбашці».

До уваги тренера/тренерки!

Можна роздати кожному з учасників роздруковану таблицю для виконання вправи, а можна вивести таблицю на слайді на екран.

Додаток 1.7.2.6

Завдання для групи 1

Намагаючись виправдати свій військовий напад на Україну, країна-агресор поширила інформацію, що Україна готувалась до військового взяття Криму. На підтвердження цього були наведені фото медалі «За взяття Криму» та посвідчення до неї.

Проаналізуйте інформацію та об ґрунтуйте, чи є вона правдивою.

Інформація для тренера. **Це фейк.**

Критичний аналіз представленого на фото посвідчення дає змогу спростувати цей фейк. По-перше, Президент України видає не накази, а Укази. По-друге, українською мовою ініціали Президента України не В.А., а В.О. – Володимир Олександрович.

Завдання для групи 2

20 жовтня 2021 року Одеський суд визнав двох молодиків винними у крадіжці. Під час судового засідання молодики пояснили, що крадіжку вчинили через потребу у коштах.

Суддя виявився дуже креативним і в судовому рішенні зазначив: «*Допитуючи обвинувачених в судовому засіданні, судом встановлено, що вони фактично за своїм розвитком ще неповнолітні діти, хоча і мають відповідний вік*».

У рішенні суду було доволі багато відсилок до цитат відомих письменників, а покарання, окрім традиційного за ці вчинки, містило також зобов'язання прочитати твори Марка Твена, Джека Лондона та вірш Тараса Шевченка: «*Суд вважає, що на обвинувачених необхідно додатково покласти (...) обов`язок передбачений п. 6 ч. 3 ст. 76 КК у вигляді дотримуватися встановлених судом вимог щодо вчинення певних дій, які будуть полягати у читанні книжок*».

Інформація для тренера. **Це правда.** Ось посилання на рішення суду: https://reyestr.court.gov.ua/Review/100432616?fbclid=IwAR3eJiOongSOYFM6bG-2R-ridUeak5lYZQGpy5qZLVXcQzrPJ4C-TBxJMBg.

Завдання для групи 3

У соціальних мережах з'явилось зображення з поширеними коментарями, на кшталт: «Здається, українців готують до масової мобілізації жінок. Така реклама із закликом записуватись до тероборони з'явилась на вулицях».

***Інформація для тренера*. Це неправда.** Фото рекламних бордів із дитиною і написом «Мама, я не хочу бути москалем!» є фейком. Зображення хлопчика, який плаче, можна знайти у відкритому доступі з 2020 року. У рекламі використовується емблема ЗСУ, але водночас вказано номер телефону територіальної оборони ЗСУ. Вона має іншу емблему. А мобілізацією до української армії взагалі займаються територіальні центри комплектування. Крім того, українською мовою в кличному відмінку правильно писати «Мамо», а не «Мама».

Джерело спростування:
https://www.stopfake.org/uk/strong-fotofejk-zsu-rozmistili-reklamni-bordi-z-napisom-mamo-ya-ne-hochu-buti-moskalem-strong.

ТЕМА 1.8. Способи побудови небезпечних онлайн-стосунків правопорушників з дітьми. Соціальна інженерія. Фішинг

Мета: ознайомити з методами розпізнавання небезпеки у кіберсфері, видами небезпечного онлайн-спілкування та його наслідками для дитини, способами отримання шахраями особистих даних.

Загальна тривалість: 4 академічні години (180 астрономічних хвилин).

План:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Використання соціальної інженерії проти дітей	Інформаційне повідомлення	40 хв	Мультимедійне обладнання
2.	Захист від фішингових атак	Індивідуальна робота	50 хв	Комп'ютери для учасників з доступом до інтернету, Додаток 1.8.1
3.	Аналіз поштового повідомлення	Індивідуальна робота	50 хв	Комп'ютери для учасників з доступом до інтернету, Додаток 1.8.2
4.	Інструменти виявлення неправдивих повідомлень	Індивідуальна робота	40 хв	Комп'ютери для учасників з доступом до інтернету, Додаток 1.8.3

ХІД ЗАНЯТТЯ

1. Інформаційне повідомлення «Використання соціальної інженерії проти дітей»

Мета: вивчити методи розпізнавання небезпеки в кіберсфері, способи убезпечення особистих даних; розглянути види небезпечного онлайн-спілкування та його наслідки для дитини, способи отримання шахраями особистих даних.

Час: 40 хв.

Необхідні матеріали: мультимедійне обладнання.

Хід проведення:

Тренер/тренерка демонструє фото чоловіка та звертається до аудиторії із запитанням: «*Хто це?*» Після висловлених припущень учасників тренер/тренерка пояснює, що на зображенні британський педофіл Пол Лейтон (Paul Leighton), який протягом певного періоду створив 30-40 несправжніх облікових записів у Фейсбуці для знайомства з дітьми. За допомогою соціальної мережі зловмисник спочатку вмовляв дітей надіслати йому фотографії інтимного характеру, після отримання яких шантажував дітей, змушуючи їх до вчинення сексуальних дій насильницького характеру. Так 14-річного хлопця з Флориди (США) Лейтон змусив зґвалтувати 12 місячну племінницю, 14-річну дівчину з Південної Дакоти (США) примусив до статевих актів зі своїм братом, які вони знімали для зловмисника на відео. В аналогічній ситуації опинилась і 13-річна дівчина з Теннессі (США). Загалом постраждалими серійного педофіла стали понад сто осіб з різних країн. У 2017 році його було засуджено до 16 років позбавлення волі за зґвалтування в режимі онлайн.

Також тренер/тренерка наводить приклади з українського досвіду, наприклад: is.gd/KOlv0e.

Далі тренер/тренерка пояснює (або нагадує, якщо ці питання вже вивчались) зміст понять: грумінг; сексторшен; секстинг; мобінг; імперсонація; флеймінг; ошуканство *(outing & trickery);* хепіслепінг; кіберпереслідування.

На наступному етапі інформаційного повідомлення слід розкрити зміст явища «соціальна інженерія» як психологічної маніпуляції, яка передує заволодінню персональними даними та використовується у більшості атак.

Далі розкриваються популярні технічні (фішинг, вішинг, спам, спливаючі вікна, атаки в довіреному середовищі, завантаження програм, месенджери) та соціальні вектори атак (підглядання та підслуховування, аналіз сміття, імперсонація, зворотна соціальна інженерія, OSINT, посередник, дорожнє яблуко), наводяться приклади.

Наприкінці інформаційного повідомлення тренер/тренерка пропонує учасникам сформулювати правила протидії соціальній інженерії. Наприклад:

1. Не довіряйте підозрілим повідомленням та предметам.
2. Підтверджуйте особу.
3. Утилізуйте сміття належним способом.
4. Навчіться розрізняти працівників.
5. Не робіть компрометуючі фотознімки та відеозаписи.
6. Перевіряйте інформацію з різних джерел.

Запитання для обговорення:

- *Чи стикалися ви в професійном чи особистому житті з випадками соціальної інженерії?*
- *Які вектори атак, на вашу думку, найбільше поширені щодо дітей?*

2. Індивідуальна робота «Захист від фішингових атак»

Мета: продемонструвати елементарну техніку створення сторінки, схожої з популярним інформаційним ресурсом.

Час: 50 хв.

Необхідні матеріали: комп'ютери для учасників з доступом до інтернету, Додаток 1.8.1.

Хід проведення:

Тренер/тренерка звертається до учасників з проханням відкрити відповідний сайт та зазначає: «*Для демонстрації техніки фішингу можуть бути використані декілька способів. Скористаємося одним з них*», після чого пропонує учасникам виконати послідовність дій, яка міститься у Додатку 1.8.1.

Після першого етапу вправи тренер/тренерка зазначає: «*Одним з додаткових інструментів фішингу може бути телефонування особі з підміненого номеру (Caller ID Spoofing), приклад, налаштування та результат якого зображено на Рис. 1.*

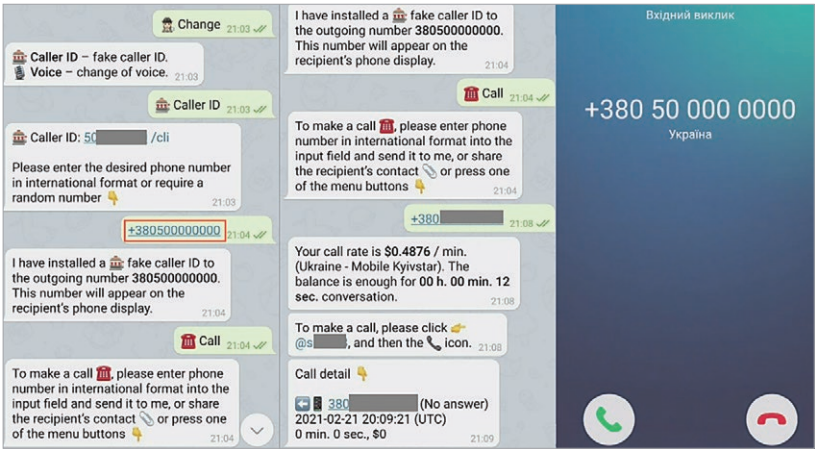


Рис. 1. Caller ID Spoofing

Для того, щоб захиститись від атак подібного виду, потрібно уважно перевіряти повідомлення, які надходять, та користуватись антифішинговими інструментами. Відповідні інструменти нерідко вбудовано у браузерах».

Запитання для обговорення:

- *Чи багато часу займає створення сторінки, яка може використовуватись для фішингу?*
- *На що слід звертати увагу, щоб не постраждати від фішингу?*

3. Індивідуальна робота «Аналіз поштового повідомлення»

Мета: отримати практичні навички аналізу поштового повідомлення.

Час: 50 хв.

Необхідні матеріали: комп'ютери для учасників з доступом до інтернету, Додаток 1.8.2.

Хід проведення:

Тренер/тренерка зазначає: «*Фішингові повідомлення часто надходять користувачам за допомогою електронної пошти. Змоделюємо ситуацію, як це може відбуватися та як можна запобігти цьому негативному явищу*», після чого пояснює алгоритм виконання вправи, використовуючи Додаток 1.8.2.

Після короткого пояснення тренер/тренерка просить учасників:

1. Зареєструвати поштову скриньку та надіслати тестове повідомлення.

2. Проаналізувати заголовок та тіло листа зі своєї електронної поштової скриньки.

Визначити адресу відправника та маршрут руху листа за допомогою сервісів:

https://www.iplocation.net/trace-email

https://mha.azurewebsites.net/

https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=73671c03-950e-4f79-88ee-f78a785b2eef

https://www.ip2location.com/free/email-tracer

https://www.whatismyip.com/email-header-analyzer/.

Запитання для обговорення:

- *Чи отримували ви підозрілі листи електронною поштою? Що ви робили в такому випадку?*
- *Які загрози можуть становити фішингові листи, які надходять електронною поштою?*
- *Як можна убезпечитись від цих загроз?*

4. Індивідуальна робота «Інструменти виявлення неправдивих повідомлень»

Мета: навчитися перевіряти окремі відомості в інтернеті на достовірність.

Час: 40 хв.

Необхідні матеріали: комп'ютери для учасників з доступом до інтернету, Додаток 1.8.3.

Хід проведення:

Тренер/тренерка зазначає: «*Для перевірки повідомлень та інших матеріалів щодо їх актуальності та достовірності можуть бути використані різні аналітичні методи. Для полегшення цього процесу також варто застосовувати і низку технічних рішень*», після чого презентує інформацію, яка міститься в Додатку 1.8.3.

На наступному етапі тренер/тренерка пропонує учасникам виконати індивідуально завдання:

«Створіть декілька зображень за допомогою ресурсу this-person-does-not-exist.com або generated.photos/faces та розмістіть їх у своєму профілі в соціальній мережі.

За допомогою описаних програмних продуктів спробуйте перевірити завантажені вами зображення на справжність. Спробуйте здійснити перевірку із зображеннями, опрацьованими Телеграм-ботом @Pix2MixV2Bot.

Перейдіть за посиланням olx.com та знайдіть декілька оголошень з продажу ігрових приставок. За допомогою розширення «Who stole my pictures» перевірте, чи немає серед фотографій у знайдених оголошеннях зображень, завантажених з інших сайтів».

Запитання для обговорення:

- *Про які інструменти виявлення неправдивих повідомлень ви знали, а про які дізнались вперше?*
- *Які із запропонованих інструментів ви плануєте використовувати надалі?*

Тестові питання до теми:

1. Як називається параметр, який можуть підмінити зловмисники під час телефонування для того, щоб особа вважала, що спілкується зі знайомим?

А) SMS;

Б) MMS;

В) CallerID;

Г) GPS.

2. На ваш телефон надійшло повідомлення з телефону начальника про прохання надіслати службовий документ на електронну пошту pp_minko_pp@mail.ru. Яких заходів ви будете вживати?

А) відправлю документ за вказаною поштовою адресою;

Б) відкриті службові документи слід надсилати тільки на службові електронні поштові адреси. Зателефоную керівнику для з'ясування ситуації;

В) ще раз перегляну телефонну книжку та переконаюся, що повідомлення надійшло з номера, який асоційовано з керівником, після чого відправлю документ;

Г) зачекаю пів години. Якщо прохання повториться, то надішлю документ.

3. Що таке соціальна інженерія?

А) розроблення проєктів розвитку соціальних мереж та створення технологічних механізмів комунікації великої кількості людей в мережі;

Б) психологічна маніпуляція, яка передує заволодінню персональними даними та використовується у більшості атак;

В) правила користування соціальними мережами;

Г) складно відповісти.

4. Чи погоджуєтесь ви з тим, що якщо повідомлення з лінком надіслали знайомі/друзі, його не потрібно додатково перевіряти?

А) так;

Б) ні;

В) залежить від тривалості нашого знайомства;

Г) залежить від месенджера, на який надійшло таке повідомлення.

5. Який з наведених ресурсів найімовірніше є фейковим?

А) facebuk.com;

Б) google.com;

В) i.ua;

Г) microsoft.com.

Ключі-відповіді:

1. В; 2. Б; 3. Б; 4. Б; 5. А.

Додаток 1.8.1

Створення сторінки, схожої з популярним інформаційним ресурсом

1. Створити фейкову сторінку.

Для створення фейку сайту можна скористатися такою технікою:

- завантажити оригінальну сторінку сайту з формою авторизації;
- відкрити вихідний код оригінальної сторінки (наприклад з використанням правої кнопки миші);
- скопіювати вихідний код сторінки в текстовий файл та назвати його index.html.

2. Для розміщення сторінки в мережі слід завантажити утиліту ngrok. Запустити її з командного рядка:

ngrok http 80

Завантажити набір Denwer для створення та управління сайтами та привести його у готовність.

Створити в папці Denwer\Home каталог з назвою виділеної ngrok адреси, а в ньому папку www.

Розмістити в створеній папці www скрипти сайту.

Запустити Denwer.

Перевірити роботу сайту.

Додаток 1.8.2

Аналіз поштового повідомлення

Спершу слід зареєструвати тестову поштову скриньку, на яку будемо одержувати відповідні повідомлення.

Після реєстрації електронної поштової скриньки слід надіслати на неї неправдиве повідомлення з підміною заголовка. Для цього можуть бути використані сервіси https://emkei.cz/, https://anonymousemail.me/ тощо. Приклад відповідним чином сформованого листа наведено на Рис. 1.

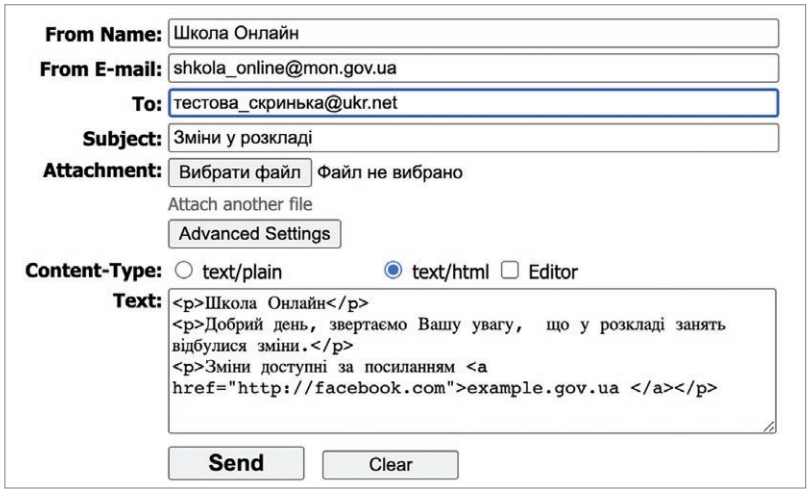


Рис. 1. Відправлення неправдивого повідомлення

У результаті на поштову скриньку надійде лист, як на Рис. 2.

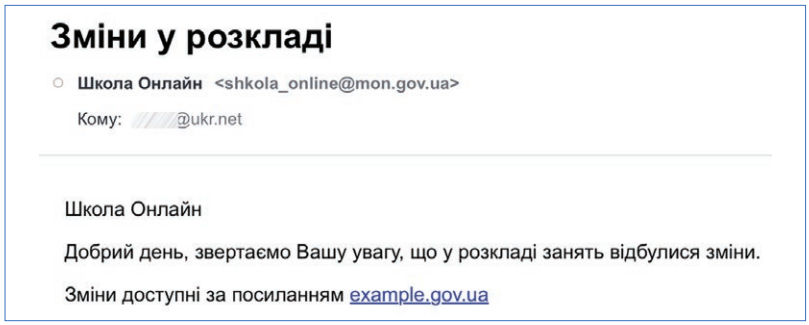


Рис. 2. Повідомлення, що надійшло

Для того, щоб виявити підробку в листі, потрібно дослідити його поштовий заголовок.

Return-path: <shkola_online@mon.gov.ua>

Received: from [10.10.10.73] (helo=frv73.fwdcdn.com) by frv54.fwdcdn.com; Fri, 24 Mar 2023 11:39:31 +0200

Authentication-Result: IP=89.187.129.29; mail.from=shkola_online@mon.gov.ua; dkim= header.i= header.d=; ID=1pfdtT-000Fhu-2X

Received-SPF: fail (frv73.fwdcdn.com: domain of mon.gov.ua does not designate 89.187.129.29 as permitted sender) client-ip=89.187.129.29; envelope-from=shkola_online@mon.gov.ua; helo=emkei.cz;

Received: from emkei.cz ([89.187.129.29])

by frv73.fwdcdn.com with esmtps ID 1pfdtT-000Fhu-2X

for тестова_скринька@ukr.net; Fri, 24 Mar 2023 11:39:31 +0200

Received: by emkei.cz (Postfix, from userid 33)

id D49C6622879; Fri, 24 Mar 2023 10:39:30 +0100 (CET)

To: тестова_скринька@ukr.net

Subject: =?UTF-8?B?0JfQvNGW0L3QuCDRgyDRgNC+0LfQutC70LDQtNGW?=

From: "=?UTF-8?B?0KjQutC+0LvQsCDQntC90LvQsNC50L0=?=" <shkola_online@mon.gov.ua>

X-Priority: 3 (Normal)

Importance: Normal

Errors-To: shkola_online@mon.gov.ua

Reply-To: shkola_online@mon.gov.ua

Content-Type: text/html; charset=utf-8

Message-Id: <20230324093930.D49C6622879@emkei.cz>

Date: Fri, 24 Mar 2023 10:39:30 +0100 (CET)

X-Authentication-Results: mxs.ukr.net;

spf=fail (frv73.fwdcdn.com: domain of mon.gov.ua does not designate 89.187.129.29 as permitted sender) client-ip=89.187.129.29;

X-Ukrnet-Yellow: 16

X-Ukrnet-Flavor: lemon

Школа Онлайн

Добрий день, звертаємо Вашу увагу, що у розкладі занять відбулися зміни.

Зміни доступні за посиланням example.gov.ua

Базовий формат поштових повідомлень (листів, messages) і статей USENET (article) визначається RFC 822 і його «спадкоємцем» RFC 2822. Кожне повідомлення (лист, message, стаття, article) складається з конверта і вмісту. Конверт зберігає адресну інформацію, необхідну для відправлення і передачі повідомлення одержувачеві. Формат конверта визначається середовищем розповсюдження. Для його автоматичного створення може використовуватися інформація з вмісту повідомлення. Стандарт визначає тільки формат вмісту повідомлення і лише у момент передачі, тобто повідомлення можуть зберігатися абсолютно в іншому форматі. Повідомлення діляться на рядки і складається з секції заголовків і тіла повідомлення (можливо порожнього).

Заголовок електронного поштового листа можна дослідити або вручну, або за допомогою програм чи сервісів (Рис. 3).

IP Address	89.187.129.29
Country	Czechia
Region & City	Jihocesky kraj, Ceske Budejovice
Coordinates	48.974470, 14.474340 (48°58'28"N 14°28'28"E)
ISP	COOLHOUSING s.r.o.
Local Time	24 Mar, 2023 11:52 AM (UTC +02:00)
Domain	coolhousing.net
Net Speed	(COMP) Company/T1
IDD & Area Code	(420) 0387
ZIP Code	370 01
Weather Station	Budweis (EZXX0030)

Рис 3. Результат аналізу заголовка поштового листа за допомогою сервісу ip2location.com

Додаток 1.8.3

Інструменти виявлення неправдивих повідомлень

Розширення **Fake Profile Detector** (Deepfake, GAN) працює в браузерах на базі Chrome або Chromium і дає змогу ідентифікувати зображення, створені з використанням штучного інтелекту (Рис. 1), отже обличчя реальної людини, додане до іншого зображення, воно теж визначатиметься як справжнє.

Розширення доступне за посиланням:
https://chrome.google.com/webstore/detail/fake-profile-detector-dee/jbpcgcnnhmjmajjkgdaogpgefbnokpcc/related?hl=en-US.

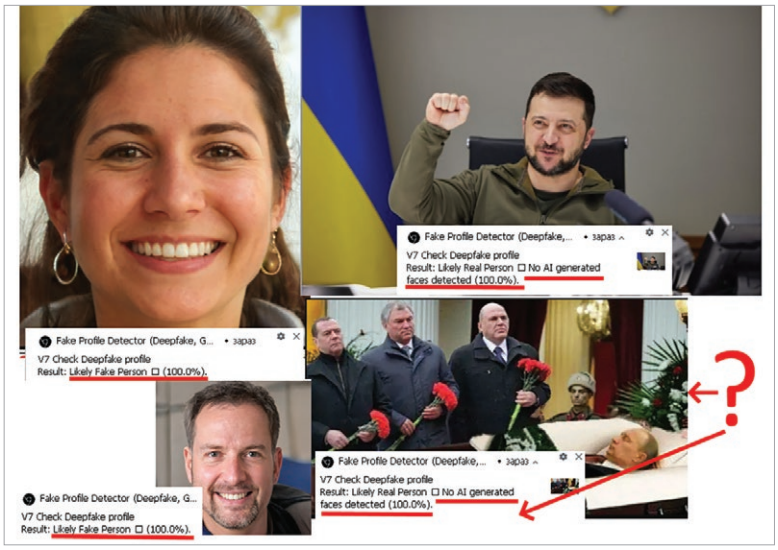


Рис. 1. Результат роботи розширення з виявлення діпфейків

Сервіси **Is your image GAN generated?** (https://gan-detector-mayachitra.azurewebsites.net/) та https://app.illuminarty.ai/#/ **Illuminarty** (https://app.illuminarty.ai/#/) виконують подібну функцію (Рис. 2).

Сервіс Forensically (29a.ch/photo-forensics) дає змогу з використанням нескладних методів аналізу спробувати зрозуміти, чи вносилися до зображення якісь зміни.

Розширення Deepfake Detection (https://github.com/deep2universe/DeepFakeChrome) призначено для виявлення DeepFake відео в сервісі Ютуб.

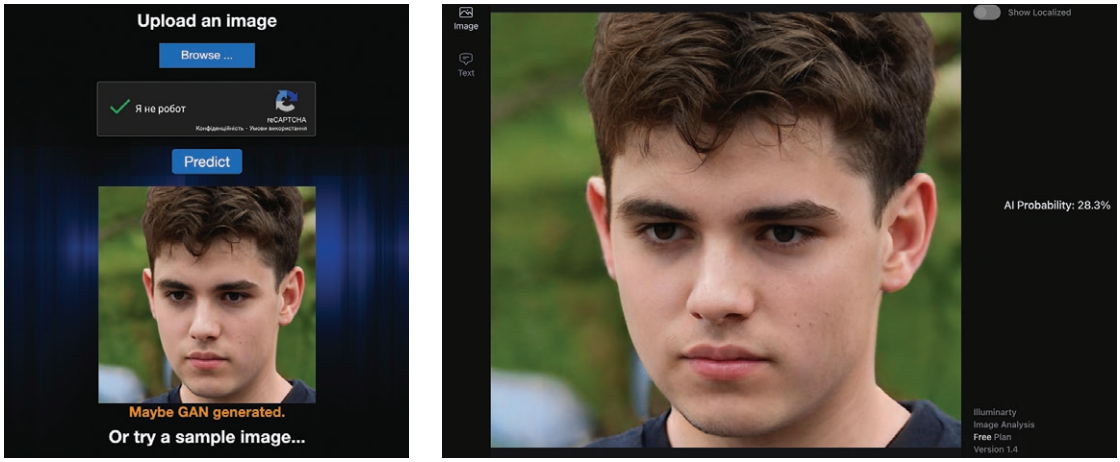


Рис. 2. Результат роботи сервісів з виявлення зображень, згенерованих за допомогою системи штучного інтелекту

Зображення можуть не мати ознак маніпуляцій, проте використовуватися у неправдивих повідомленнях у різних контекстах. Для того, **щоб знайти першоджерело відповідних малюнків, можна використовувати розширення Who stole my pictures** (Рис. 3).

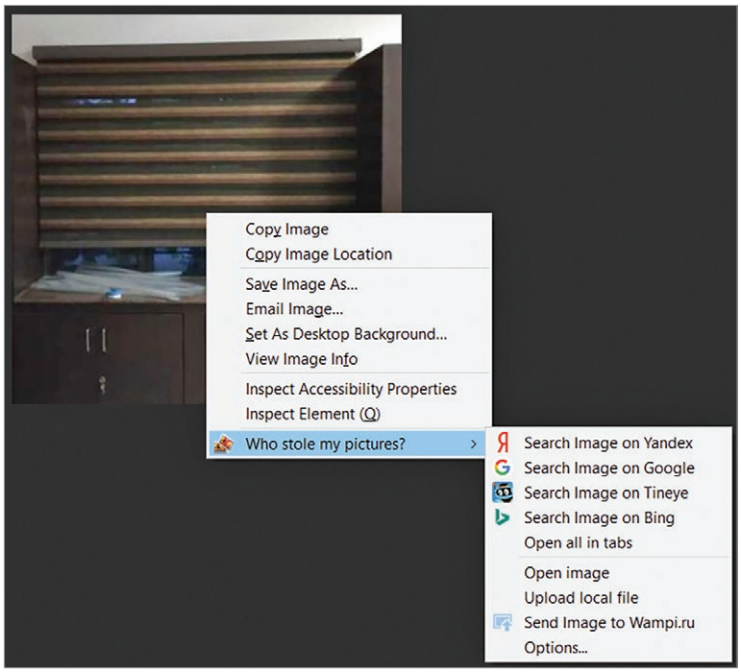


Рис. 3. Використання розширення для пошуку зображень

Завантажити описане розширення можна за адресами:

- для браузеру «Chrome» (https://chrome.google.com/webstore/detail/who-stole-my-pictures/mcdbnfhkikiofkkicppioekloflmaibd);
- для браузеру «Firefox» (https://addons.mozilla.org/ru/firefox/addon/who-stole-my-pictures/).

ТЕМА 1.9. Система захисту прав дітей в кіберпросторі

Заняття 1.9.1. Міжнародні стандарти та національне законодавство щодо захисту дітей від насильства та експлуатації в кіберпросторі

Мета: надати учасникам інформацію про правові основи захисту дітей від насильства та експлуатації в кіберпросторі.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Асоціації, пов'язані з насильством та експлуатацією дітей в кіберпросторі	Обговорення	10 хв	Фліпчарт, аркуші для фліпчарту, маркери або мультимедійне обладнання
2.	Огляд міжнародних документів та національного законодавства у сфері захисту прав дітей в кіберпросторі	Інформаційне повідомлення	25 хв	Додаток 1.9.1.1, мультимедійне обладнання
3.	Визначення понять	Робота в групах	30 хв	Роздруківки з Додатка 1.9.1.2
4.	Як правильно?	Вправа	25 хв	Додаток 1.9.1.3, мультимедійне обладнання

ХІД ЗАНЯТТЯ

1. Обговорення «Асоціації, пов'язані з насильством та експлуатацією дітей в кіберпросторі»

Мета: оцінити рівень інформованості учасників, актуалізувати основні поняття щодо захисту дітей від насильства та експлуатації в кіберпросторі.

Час: 10 хв.

Необхідні матеріали: фліпчарт, аркуші для фліпчарту, маркери або мультимедійне обладнання.

Хід проведення:

Тренер/тренерка на аркуші фліпчарту пише словосполучення «Насильство та експлуатація дітей в кіберпросторі» і пропонує учасникам озвучити асоціації, які виникають у них щодо цього словосполучення: *«Сьогодні ми з вами говоримо про захист дітей від насильства та експлуатації в кіберпросторі, і я пропоную вам навести асоціації, пов'язані з цим словосполученням».*

Тренер/тренерка занотовує всі відповіді, які надають учасники.

До уваги тренера/тренерки!

Якщо дозволяє технічне обладнання, можна зробити опитування за допомогою програми Mentimetr або Slido у вигляді хмаринки думок.

Запитання для обговорення:

- *Чи складно було знайти відповідну асоціацію?*
- *Чи пов'язані якісь із цих асоціацій з вашим власним досвідом?*

Після обговорення тренер/тренерка підсумовує: «*Слід визнати, що діти є найуразливішою та найбільш незахищеною категорією населення. Своєчасно виявити насильство та експлуатацію дитини, яке відбувається офлайн, не завжди вдається, а в кіберпросторі це завдання в рази складніше*».

2. Інформаційне повідомлення «Огляд міжнародних документів та національного законодавства у сфері захисту прав дітей в кіберпросторі»

Мета: ознайомити учасників з переліком правових документів, спрямованих на захист прав дітей в кіберпросторі, пояснити їх роль, зміст і вплив на формування національного законодавства та практики його реалізації.

Час: 25 хв.

Необхідні матеріали: Додаток 1.9.1.1, мультимедійне обладнання.

Хід проведення:

Тренер/тренерка зазначає: «*Нормативно-правове забезпечення захисту дітей від насильства та експлуатації в кіберпросторі охоплює:*

- *міжнародні стандарти*
- *європейські стандарти*
- *національне законодавство*

Правові документи в кожній із цих груп можна поділити на загальні – ті що загалом присвячені забезпеченню та захисту прав дітей і в яких поміж іншим висвітлені питання забезпечення прав дітей в цифровому середовищі, та спеціальні – ті що безпосередньо присвячені захисту прав дітей в кіберпросторі».

Тренер/тренерка презентує інформацію із Додатка 1.9.1.1, після чого зазначає:

«*Розроблення належного національного законодавства щодо боротьби з кіберзлочинністю і гармонізація його на міжнародному рівні є головним кроком до успіху будь-якої національної стратегії щодо захисту дітей в цифровому середовищі. Під час розроблення відповідного національного законодавства важливо також враховувати, що діти не є однорідною групою. Дітям різних вікових груп можуть бути потрібні різні заходи у відповідь, так само як і дітям з особливими потребами*».

До уваги тренера/тренерки!

Слід підготувати презентацію на основі матеріалу, який міститься в Додатку 1.9.1.1, обсяг і зміст якої залежатиме від запитів цільової аудиторії учасників. Доцільно вивести на слайди презентації лише перелік документів, акцентуючи увагу під час інформаційного повідомлення на характеристиці спеціальних документів. Наведений в Додатку перелік документів не є вичерпним. Слід наголосити, що ратифіковані Україною міжнародні та європейські документи є частиною національного законодавства та мають враховуватись в процесі діяльності органами влади.

Запитання для обговорення:

- *Про які із окреслених документів ви були обізнані, а про які почули вперше?*
- *Чи відповідає, на вашу думку, національне законодавство щодо захисту дітей від насильства та експлуатації дітей в кіберпросторі міжнародним та європейським стандартам?*

3. Робота в групах «Визначення понять»

Мета: систематизувати знання основних закріплених в правових документах понять щодо насильства та експлуатації дітей в кіберпросторі, сформувати спільний понятійний апарат.

Час: 30 хв.

Необхідні матеріали: роздруківки з Додатка 1.9.1.2.

Хід проведення:

Тренер/тренерка об'єднує учасників у чотири групи та забезпечує кожну групу роздруківками з поняттями та визначеннями з Додатка 1.9.1.2. Учасникам протягом 15 хвилин слід співвіднести поняття та визначення. Після завершення роботи групи по черзі презентують напрацювання по одному поняттю-визначенню. Інші групи звіряють, чи їх відповідь збігається з озвученою. Якщо відповіді відрізняються, тренер/тренерка озвучує та коментує правильну відповідь.

До уваги тренера/тренерки!

В Додатку 1.9.1.2 поняття та визначення співвіднесені правильно. Перед роздрукуванням та розрізанням поняття можна позначити цифрами, а визначення – літерами та поміняти їх місцями, щоб не збігалися. Водночас тренеру/тренерці доцільно підготувати ключ з правильними відповідями для зручності перевірки відповідей учасників. Під час обговорення результатів роботи в групах з метою економії часу учасники можуть не зачитувати все визначення, а просто називати відповідність цифри та літери.

Запитання для обговорення:

- *Чи всі терміни були вам знайомі?*
- *Чи важливим є єдине розуміння понять фахівцями? Чому?*

До уваги тренера/тренерки!

Термін «грумінг» не закріплено у міжнародному праві; в деяких юридичних системах, зокрема в Канаді, використовується термін «заманювання», а в Україні – «домагання дитини для сексуальних цілей».

Після обговорення тренер/тренерка підсумовує: «*Термінологія має значення, особливо в питаннях виявлення та розслідування правопорушень, вчинених за допомогою інтернету, на території різних країн. Неправильне вживання термінів може призводити до непорозуміння між колегами з різних країн, застосування невідповідних процедур, уникнення правопорушниками відповідальності та несвоєчасного захисту постраждалих осіб. Важливо слідкувати за появою нових термінів, усвідомлювати, які з них закріплені в правових документах, а які – ні, як співвідносяться назви правопорушень, закріплених в міжнародних документах і національному законодавстві, тощо*».

4. Вправа «Як правильно?»

Мета: сформувати усвідомлення важливості вжиття коректних термінів під час діяльності щодо захисту дітей від сексуального насильства та сексуальної експлуатації, зокрема і в кіберпросторі.

Час: 25 хв.

Необхідні матеріали: Додаток 1.9.1.3, мультимедійне обладнання.

Хід проведення:

Тренер/тренерка зазначає: «*Відповідно до рекомендацій Європолу, особи, які надають першу допомогу постраждалій від насильства дитині, зокрема поліцейські, мають максимально поважати її права. Фахівці, які перші дізналися про випадок насильства щодо дитини, зокрема в кіберпросторі, повинні бути особливо обережними, щоб не допустити дискримінації та знецінення потреб постраждалої дитини. Термінологія, яку вживають поліцейські, також має значення в цьому контексті. Робоча група проєкту зі встановлення єдиної міжвідомчої термінології та семантики з питань сексуальної експлуатації дітей провела дослідження й аналіз із метою створення рекомендацій щодо міжнародної термінології. Тепер вони відомі як «Люксембурзькі рекомендації». Серед групи розробників були також представники Інтерполу».*

Тренер/тренерка по черзі парами виводить на екран терміни із Додатка 1.9.1.3 та запитує в учасників, який термін є більш коректним та чому? Після відповідей учасників, тренер/тренерка зазначає правильну відповідь.

До уваги тренера/тренерки!

Для залучення до обговорення всіх присутніх можна завчасно підготувати онлайн-опитування.

Запитання для обговорення:

- *Чи відповідають закріплені в національному законодавстві терміни Люксембурзьким рекомендаціям?*
- *Чи можуть поліцейські використовувати коректні терміни, навіть якщо в національному законодавстві вони не закріплені?*

Тестові питання до заняття:

1. Якому терміну відповідає таке визначення: «психологічне, фізичне, економічне чи сексуальне насильство, тобто будь-яке умисне діяння (дія або бездіяльність) із застосуванням засобів електронних комунікацій, яке систематично вчиняється особою стосовно дитини, з якою вони є учасниками одного колективу, або дитиною стосовно іншого учасника одного колективу та яке порушує права, свободи, законні інтереси потерпілої особи та/або перешкоджає виконанню нею визначених законодавством обов'язків»?

А) матеріали сексуального насильства щодо дітей;

Б) дитяча порнографія;

В) грумінг;

Г) кібербулінг.

2. Вживання якого із термінів вважається некоректним відповідно до Люксембурзьких рекомендацій, рекомендацій Європолу та Комітету Лансароте?

А) матеріали сексуального насильства щодо дітей;

Б) дитяча порнографія;

В) грумінг;

Г) кібербулінг.

3. Чи застосовуються положення Лансаротської конвенції до сексуальних злочинів проти дітей, вчинених за допомогою інформаційних і комунікаційних технологій (ІКТ)?

А) так;

Б) ні;

В) частково;

Г) тільки в країнах ЄС.

4. В якому нормативно-правовому акті міститься норма, згідно з якою, крім виняткових випадків, коли неможливо інакше забезпечити найкращі інтереси дитини, суб'єкти у сфері медіа не мають права без письмової згоди хоча б одного з батьків або інших законних представників дитини оприлюднювати фото дитини, яка зазнала фізичного чи сексуального насилля?

А) Закон України «Про захист суспільної моралі»;

Б) Закон України «Про охорону дитинства»;

В) Закон України «Про медіа»;

Г) Конституція України.

5. Матеріали, пов'язані з сексуальною експлуатацією та сексуальним насильством стосовно дітей (CSEM / CSAM), – це:

А) запис матеріалів, пов'язаних із сексуальними зловживаннями щодо дітей з боку дорослих;

Б) зображення дітей, залучених до відвертих сексуальних дій;

В) зображення статевих органів дітей, коли зображення створюються або використовуються насамперед з метою сексуального характеру;

Г) всі відповіді правильні.

Ключі-відповіді:

1. Г; 2. Б; 3. А; 4. В; 5. Г.

Додаток 1.9.1.1

Міжнародні стандарти.
Загальні

- ***Конвенція ООН про права дитини та Факультативний протокол до неї щодо торгівлі дітьми, дитячої проституції та дитячої порнографії***

Кожна дитина має право на захист від усіх форм фізичного та психологічного насильства, образ, зловживань, відсутності піклування чи недбалого і брутального поводження та експлуатації, включаючи сексуальні зловживання, з боку батьків, законних опікунів або будь-якої іншої особи, яка опікується дитиною (*ст.19 Конвенції ООН про права дитини*).

Держави-учасниці зобов'язуються захищати дитину від усіх форм сексуальної експлуатації та сексуальної зловживання:

(a) спонукання або примус дитини займатися будь-якими незаконними сексуальними діями;

(b) використання дітей у проституції з метою експлуатації або інші незаконні сексуальні дії;

(c) експлуатації дітей у порнографічних виставах та матеріалах (*стаття 34 Конвенції ООН про права дитини*).

Хоча у Конвенції про права дитини та Факультативному протоколі до неї право дитини на захист від «онлайн» сексуальної експлуатації та насильства над дітьми безпосередньо не згадується, *Генеральний комітет з прав дитини у Коментарі №25 (2021) про права дитини в цифровому середовищі підтверджує зобов'язання держав-учасниць захищати дітей від всі форми насильства в цифровому середовищі, зокрема за допомогою правових заходів.*

- ***Цілі сталого розвитку 2030***

Ціль 16.2 полягає в тому, щоб до 2030 року покласти край нарузі, експлуатації та всім формам насильства і тортур щодо дітей. Зазначається, що стрімке поширення інформаційно-комунікаційних технологій дало дітям та молоді безпрецедентні можливості для спілкування, обміну, навчання, доступу до інформації та висловлювання своєї думки з питань, що стосуються їхнього власного життя та життя їхніх спільнот. Проте розширення та спрощення доступу до інтернету і технологій рухомого зв'язку також пов'язано із серйозними викликами для безпеки та добробуту дітей як в цифровому середовищі, так і в реальному житті. Щоб знизити ризики, які несе в собі цифровий світ, і водночас зробити так, аби більше дітей та молодих осіб могли користуватися його благами, уряди, представники громадянського суспільства, місцеві спільноти, міжнародні організації та галузеві підприємства повинні об'єднати свої зусилля задля спільної мети.

Спеціальні

- ***Люксембурзькі рекомендації (2016 р.)*** – міжвідомчий проєкт термінології та семантики щодо сексуальної експлуатації та сексуального насильства над дітьми. Метою цього документа є надання всім особам і установам, які працюють над запобіганням і викоріненням усіх форм сексуальної експлуатації та сексуального насильства над дітьми, інструкцій щодо розуміння та використання різних термінів і понять, з якими вони можуть стикатися у своїй роботі.

- ***Глобальний посібник із удосконалення законодавчої бази для захисту дітей від сексуальної експлуатації та насильства в інтернеті***

Має на меті надати вказівки щодо того, як зміцнити законодавчу базу для захисту дітей від сексуальної експлуатації та насильства в інтернеті. У цьому посібнику зокрема містяться

рекомендації щодо процедур та методів розслідування випадків сексуального насильства та експлуатації дітей в інтернеті, зокрема:

- у законодавстві має бути визначено «контактну точку» для отримання повідомлень та надання негайної допомоги з метою розслідування або провадження щодо злочинів, пов'язаних із сексуальною експлуатацією та насильством над дітьми в інтернеті;
- необхідно створити спеціалізовані слідчі підрозділи правоохоронних органів на регіональному рівні, до повноважень яких входитиме розслідування випадків сексуальної експлуатації та насильства над дітьми в інтернеті;
- слід розглянути можливість запровадження законодавчої вимоги до персоналу таких підрозділів стосовно кваліфікації та проходження регулярного навчання без відриву від роботи;
- «таємні розслідування» повинні бути дозволені, але регулюватися законом і відповідати міжнародним правовим стандартам;
- слід забезпечити можливість притягнення до відповідальності за спробу вчинити сексуальне насильство та експлуатацію дитини, навіть якщо фактично вчинення правопорушення було б неможливе (для охоплення випадків, коли правоохоронні органи прикидаються дитиною, іншим правопорушником («замовником») або співучасником);
- законодавство має встановлювати правила щодо прийнятності цифрових доказів.

Європейські стандарти.
Загальні

- ***Стратегія Ради Європи з прав дитини (2022-2027) «Права дитини на практиці: від стабільної реалізації до спільного новаторства»***, яка акцентує увагу на житті без насильства; правосудді, дружньому до дітей, та правах дитини в цифровому середовищі. В підрозділі 2.3. Стратегії «Доступ і безпечне використання технологій для всіх дітей» наголошено: «.... *Цифрове середовище надає дітям безліч можливостей для реалізації та відстоювання своїх прав як онлайн, так і офлайн, але також наражає їх на ризики заподіяння шкоди, які можуть мати згубний вплив на значну кількість прав людини, гарантованих Конвенцією ООН з прав людини, ЄСПЛ*».
- ***Рекомендація Комітету міністрів Ради Європи CM/Rec(2009)10 щодо інтегрованих національних стратегій захисту дітей від насильства***

В рекомендації приділяється увага *освіті і підвищенню обізнаності громадськості* шляхом проведення інформаційних кампаній та кампаній у ЗМІ з питань прав дитини, зокрема права на захист від усіх форм насильства. У всьому суспільстві має підтримуватися чітка та міцна нетерпимість до всіх форм насильства над дітьми, навіть до її найменш тяжких форм.

Також в рекомендації акцентується увага *на професійній підготовці.* Представники всіх професій, які працюють з дітьми, повинні вміти запобігати та виявляти випадки насильства над дітьми, а також ефективно реагувати на них.

Окрема увага приділяється питанням *ЗМІ та інформаційного суспільства.* Особи, які відповідають за ЗМІ, повинні цілком усвідомлювати свою відповідальність і за все, що стосується демонстрації насильства та поширення потенційно шкідливого для дітей контенту, виконуючи водночас свої обов'язки, пов'язані зі здійсненням права на свободу вираження поглядів. Це може втілюватися через усунення чи блокування доступу до шкідливих матеріалів або через розроблення автоматизованих систем класифікації контенту, впровадження механізмів контролю та подання скарг щодо якості контенту тощо.

- ***Рекомендація Комітету міністрів Ради Європи Rec(2001)16 щодо захисту дітей від сексуальної експлуатації***

Серед заходів рекомендує:

- залучити постачальників послуг інтернету до підвищення обізнаності про сексуальну експлуатацію та її ризики, особливо в інтернеті та за допомогою сучасних комунікаційних технологій;
- визнати, що правоохоронні органи повинні мати змогу використовувати дані з'єднання для відстеження підозрілого контенту, а потім знаходити, ідентифікувати та допитувати тих, хто редагує чи поширює дитячу порнографію або заохочує чи підбурює до дитячої проституції;
- надавати інформацію батькам, опікунам, усім іншим, хто відповідає за дітей, і самим дітям про ризики сексуальної експлуатації в інтернеті, форми, які вона може мати, і про те, як обмежити доступ до неї;
- створити «гарячі лінії» та заохочувати громадян повідомляти про випадки дитячої порнографії чи заохочення до дитячої проституції на вебсайті, що дасть змогу відповідним правоохоронним органам вжити конкретних заходів.

- ***Стратегія ЄС з прав дитини***

Стратегія акцентує увагу на шести тематичних сферах, які є пріоритетними для ЄС, серед яких «Цифрове та інформаційне суспільство: ЄС, де діти можуть безпечно орієнтуватися в цифровому середовищі та використовувати його можливості». Поміж інших Європейська комісія пропонує державам-членам такі кроки:

1) підтримувати акції медіаграмотності як частину освіти, розвивати здатність дітей критично оцінювати онлайн-контент, виявляти дезінформацію та образливі матеріали;
2) підтримувати та сприяти роботі центрів безпечного інтернету, які співфінансуються ЄС, а також підтримувати дитячі телефони довіри та «гарячі лінії» у розвитку онлайн-способів спілкування.

Європейська Комісія пропонує компаніям у сфері ІКТ продовжувати свої зусилля щодо виявлення, повідомлення та видалення незаконного контенту в інтернеті, серед них і сексуальне насильство над дітьми, зі своїх платформ та служб.

Спеціальні

- ***Конвенція про кіберзлочинність (Будапештська конвенція) та Додатковий протокол до неї про криміналізацію актів расистського та ксенофобського характеру, скоєних через комп'ютерні системи (ETS №189)***

Відповідно до п. 1 ст. 9, кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, таких дій:

a) виготовлення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем;
b) пропонування або надання доступу до дитячої порнографії за допомогою комп'ютерних систем;
c) розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем;
d) здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи;
e) володіння дитячою порнографією в комп'ютерній системі чи на комп'ютерному носії інформації.

- ***Конвенція Ради Європи про захист дітей від сексуального насильства та сексуальної експлуатації (CETS №201)*** (Лансаротська конвенція). Україна ратифікувала її у 2012 році. Держави зобов'язані запропонувати заходи протидії сексуальному насильству стосовно дітей в межах підходу чотирьох «Р» (*Prevention, Protection, Prosecution and Promotion*): запобігання, захисту, кримінального переслідування та зміцнення національної і міжнародної співпраці. Серед іншого, Лансаротська конвенція передбачає:

- діти мають знати про ризики, пов'язані з сексуальною експлуатацією та сексуальним розбещенням, і мати змогу захистити себе;
- осіб, які працюють у тісному контакті з дітьми, потрібно перевіряти та навчати;
- потрібно заохочувати інформування про підозру в сексуальній експлуатації або сексуальному розбещенні;
- потрібно створити служби телефонної допомоги або допомоги в мережі інтернет;
- потрібно створити програми підтримки постраждалих та їхніх сімей;
- потрібно задіяти доброзичливі для дитини судові процеси для захисту постраждалої особи, її приватного життя, особистості та репутації (наприклад кількість опитувань постраждалих дітей повинна бути обмежена, а опитування повинні здійснюватися у спеціальному місці та проводитися професіоналами, підготовленими для цих цілей).

Глава VI «Матеріальне кримінальне право» Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального розбещення зобов'язує Сторони вжити необхідних законодавчих або інших заходів для забезпечення криміналізації таких діянь: сексуальне розбещення (ст. 18); правопорушення, що стосуються дитячої проституції (ст. 19); правопорушення, що стосуються дитячої порнографії (ст. 20); правопорушення, що стосуються участі дитини в порнографічних виставах (ст. 21); розбещення дітей (ст. 22); домагання дитини для сексуальних цілей (ст. 23). Незважаючи на те, що Конвенція ратифікована Україною ще у 2012 р., лише в лютому 2021 року було криміналізоване домагання дитини в сексуальних цілях, зокрема з використанням інформаційно-телекомунікаційних систем або технологій (ст. 156-1 Кримінального кодексу України), а також одержання доступу до дитячої порнографії (ст. 301-1 ККУ) та проведення видовищного заходу сексуального характеру, зокрема з використанням інформаційно-телекомунікаційних систем або технологій, за участю неповнолітньої особи (ст. 301-2 ККУ).

Кожна країна, яка ратифікувала цю конвенцію, має вживати таких заходів, які можуть бути необхідні для забезпечення *спеціалізації осіб, підрозділів та служб*, що займаються розслідуваннями у сфері боротьби із сексуальною експлуатацією та сексуальним насильством стосовно дітей, або забезпечує навчання відповідних працівників для цих цілей (ст. 34).

Комітет Лансароте уточнив дію Конвенції щодо цифрового середовища, прийнявши низку документів, зокрема:

- *Висновок про зображення та/або відеоматеріали непристойного чи явно сексуального характеру за участю дітей, які створюються, пересилаються та отримуються дітьми (6 червня 2019 року);*
- *Пояснювальний висновок про можливість застосування Лансаротської конвенції до сексуальних злочинів проти дітей, вчинених за допомогою інформаційних і комунікаційних технологій (ІКТ) (12 травня 2017 року);*
- *Декларація про вебадреси, що містять рекламу матеріалів або зображень, що пропагують сексуальну експлуатацію дітей чи будь-які інші злочини, визнані такими відповідно до Конвенції Лансароте (16 червня 2016 р.);*

- *Домагання дитини для сексуальних цілей за допомогою інформаційно-комунікаційних технологій (грумінг)/ висновок за статтею 23 Лансаротської конвенції та пояснювальна записка до неї (17 червня 2015 року).*

- ***Рекомендація Комітету міністрів Ради Європи CM/Rec(2009)5 про заходи щодо дітей від шкідливого контенту й поведінки та сприяння їх активній участі в новому інформаційному та комунікаційному середовищі***

Створення безпечного простору для дітей в інтернеті:

- створення безпечних і захищених вебсайтів для дітей, наприклад за допомогою розроблення онлайн-порталів, що відповідають віку;
- розроблення професійних стандартів для обслуговування таких вебсайтів і порталів в інтернеті, зокрема щодо посилань на інші сайти;
- підвищення обізнаності про ці безпечні та захищені інтернет-сайти для дітей, зокрема серед батьків, педагогів, розробників контенту та їхніх відповідних асоціацій.

Заохочення розвитку загальноєвропейських знаків довіри та систем маркування.

Маркування онлайн-контенту сприяє розвитку безпечного та захищеного простору для дітей в інтернеті.

Сприяння розвитку навичкам медіаграмотності серед дітей, батьків та педагогів.

Неможливо повністю усунути небезпеку впливу дітей на контент або поведінку, що несе ризик заподіяння шкоди, і що, отже, медіаграмотність для дітей, батьків і педагогів залишається ключовим елементом у забезпечення узгодженого захисту дітей від таких ризиків.

- ***Рекомендація Комітету міністрів Ради Європи CM/Rec(2014)6 «Посібник з прав людини для інтернет-користувачів»***

Основний меседж посібника такий: права та основоположні свободи людини (зокрема дитини) діють однаковою мірою офлайн та онлайн.

- ***Рекомендація Комітету міністрів Ради Європи CM/Rec(2018)7 щодо Керівних принципів поваги, захисту та реалізації прав дитини в цифровому середовищі та Посібник з питань прав дитини в цифровому середовищі для органів державної влади***

У п. 51 перелічені основні ризики та загрози, пов'язані з цифровим середовищем, які здатні негативно вплинути на фізичний, емоційний та психологічний добробут дитини:

- сексуальної експлуатації та зловживання, домагання для сексуальних цілей («грумінг», розбещування), онлайн-вербування дітей для вчинення злочинів, участь у екстремістських політичних чи релігійних рухах або для цілей торгівлі людьми (контактні ризики);
- принизливе та стереотипне зображення та надмірна сексуалізація жінок та дітей; зображення насильства й нанесення собі ушкоджень, зокрема самогубств; принизливі, дискримінаційні або расистські вислови або заклик до такої поведінки; реклама, контент для дорослих (ризики контенту);
- залякування, переслідування та інші форми утисків, розповсюдження без отримання згоди сексуальних зображень, шантаж, висловлювання ненависті, хакерство, азартні ігри, незаконне завантаження або інші порушення прав інтелектуальної власності, комерційна експлуатація (ризики поведінки);
- надмірне використання, позбавлення сну та фізична шкода (ризики для здоров'я).

Відповідно до п. 62, «державам слід постійно відстежувати, чи перебувають у їх юрисдикції матеріали про сексуальне насильство над дітьми, і вимагати від правоохоронних органів встановлення баз даних «хеш» з метою прискорення дій щодо виявлення та знаходження дітей, які зазнають сексуальної експлуатації або насильства, та затримання винних».

- ***Директива ЄС 2011/93/ЄС щодо протидії сексуальному насильству та сексуальній експлуатації дітей та дитячій порнографії***

Статтями 3-6 визначені злочини стосовно дітей на сексуальному підґрунті, зокрема з використанням інформаційно-комунікаційних технологій (зокрема схиляння дитини до сексуальних дій; примушування до статевих стосунків, також з третіми особами; спонукання або вербування дитини до участі в порнографічних матеріалах; правопорушення, пов'язані з дитячою порнографією, домагання дитини тощо).

Щодо діяльності правоохоронних органів стосовно розслідування таких правопорушень в Директиві зазначається, що «*Особам, відповідальним за розслідування та судове переслідування правопорушень, мають бути доступні ефективні інструменти розслідування.... У відповідних випадках і відповідно до національного законодавства, такі інструменти також повинні включати можливість для правоохоронних органів використовувати приховану особу в інтернеті*» (п. 27).

- ***Цифрове десятиліття для дітей та молоді: нова європейська стратегія кращого інтернету для дітей (BIK+)***

Стратегія ЄС пропонує дії навколо **трьох стовпів:**

1. *Безпечний цифровий досвід*, захист дітей від шкідливого та незаконного онлайн-контенту, поведінки та ризиків і покращення їхнього добробуту завдяки безпечному цифровому середовищу, яке відповідає віку.
2. *Розширення цифрових можливостей*, щоб діти здобували необхідні навички та вміння безпечно та відповідально виражати себе в онлайн-середовищі.
3. *Активна участь*, повага до дітей, надання їм права голосу в цифровому середовищі.

Національне законодавство. Загальні

- ***Закон України «Про охорону дитинства»***

Стаття 10. Право на захист від усіх форм насильства.

Адміністрація підприємств, установ і організацій незалежно від форми власності та господарювання, до штатів яких входять особи, які в своїй роботі контактують з дітьми, зобов'язана проводити їх періодичне інформування про захист дітей від усіх форм насильства та експлуатації. Забороняється працювати у контакті з дітьми особам, інформацію про яких внесено до Єдиного реєстру осіб, засуджених за злочини проти статевої свободи та статевої недоторканості малолітньої особи

Стаття 30-2. Захист дітей, які постраждали від сексуального насильства або стали його свідками (очевидцями).

Держава здійснює захист дітей від сексуального насильства (зокрема від сексуальної експлуатації та вчиненого з боку батьків або осіб, які їх замінюють), а також дітей, які постраждали від такого насильства або стали його свідками (очевидцями).

Організація функціонування, кадрове, методичне і матеріально-технічне забезпечення спеціального приміщення, передбаченого для опитування (допиту) дитини, яка постраждала від сексуального насильства або стала його свідком (очевидцем), із застосуванням дружньої до дитини методики, здійснюється спеціалізованими службами підтримки постраждалих осіб, що утворюються місцевими органами виконавчої влади та органами місцевого самоврядування відповідно до законодавства.

- ***Закон України «Про основні засади забезпечення кібербезпеки в Україні»*** визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їх діяльності із забезпечення кібербезпеки.
- ***Постанова Кабінету Міністрів України «Про забезпечення соціального захисту дітей, які перебувають у складних життєвих обставинах» від 1 червня 2020 р. №585,*** якою затверджений порядок забезпечення соціального захисту дітей, які перебувають у складних життєвих обставинах, зокрема дітей, які постраждали від жорстокого поводження.

Спеціальні

- ***Стратегія кібербезпеки України та План реалізації****,* який містить низку пунктів щодо дітей:
  - п. 17 передбачає розроблення концептуальних підходів щодо реалізації державної політики у сфері забезпечення прав громадян у кіберпросторі (особливо найбільш вразливих груп населення, насамперед дітей). Відповідальними за реалізацію цього заходу визначені Міністерство цифрової трансформації України, Міністерство внутрішніх справ України, Національна поліція України, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації.
  - п. 90 передбачає поглиблення співпраці з міжнародними організаціями у сфері захисту дітей від сексуального онлайн-насильства. Відповідальними є Міністерство цифрової трансформації України, Національна поліція України.
- ***Закон України «Про медіа»***

Крім виняткових випадків, коли неможливо інакше забезпечити найкращі інтереси дитини, суб'єкти у сфері медіа не мають права без письмової згоди хоча б одного з батьків або інших законних представників дитини оприлюднювати фото дитини, яка зазнала фізичного чи сексуального насилля, а також розголошувати будь-яку інформацію, яка:

1) може сприяти ідентифікації дитини, яка задіяна у провадженні у справах про адміністративні правопорушення, в кримінальному провадженні у будь-якому статусі або стосовно якої є інформація про здійснення нею правопорушення;
2) стосується факту самогубства дитини, водночас ідентифікує її особу.

На території України в медіа та на платформах спільного доступу до відео забороняється поширювати порнографічні матеріали, а також матеріали, що заохочують сексуальну експлуатацію та насильство над дітьми, демонструють статеві відносини дітей, використовують образ дітей (візуальний запис образу дітей) у візуалізованих заходах сексуального чи еротичного характеру. Критерії віднесення інформації до такої, що порушує вимоги цієї норми, розробляє та затверджує Національна рада України з питань телебачення і радіомовлення спільно з органом спільного регулювання. До затвердження відповідних критеріїв Національна рада України з питань телебачення і радіомовлення обґрунтовує застосування обмежень, передбачених частиною першою цієї статті, самостійно у своїх рішеннях.

- ***Кримінальний кодекс України***

Передбачає відповідальність за вчинення насильства та експлуатації дітей, зокрема у кіберпросторі.

- ***Кодекс України про адміністративні правопорушення***

Передбачає відповідальність за вчинення кібербулінгу, мобінгу тощо.

Додаток 1.9.1.2

Поняття

Геш	Унікальний цифровий відбиток, присвоєний цифровим файлам, зокрема тим, що зображують матеріали сексуального насильства над дітьми. Завдяки цьому можна провести швидкий аналіз великої кількості даних, без необхідності окремо досліджувати потенційні зображення сексуального насильства стосовно дітей. (*Посібник з питань прав дитини в цифровому середовищі для органів державної влади*).
Грумінг у цифровому середовищі	Означає процес налагодження/побудови взаємин із дитиною особисто або за допомогою інтернету чи інших цифрових технологій, з метою домогтися сексуальних зв'язків із цією особою в цифровому середовищі або в реальному житті, схиливши дитину вступити в сексуальний зв'язок (*Люксембурзькі рекомендації*). Процес, спрямований на заманювання дітей у дії чи бесіди сексуального характеру, як з їхнього відома, так і без нього, або процес, що передбачає спілкування та встановлення взаємин між порушником і дитиною, з метою зробити останню вразливішою перед сексуальними зловживаннями (*Рекомендації для директивних органів щодо захисту дитини в цифровому середовищі*). Налагодження довірливих стосунків із дитиною в інтернеті з метою сексуального насильства *(проєкт StopSextинг).*
Дитина	Особа віком до 18 років (повноліття), якщо згідно з законом, застосовуваним до неї, вона не набуває прав повнолітньої раніше (ст. 1 Закону України «Про охорону дитинства»). Кожна людська істота віком до вісімнадцяти років, якщо згідно із законом, застосовним до дитини, повноліття не досягається раніше *(стаття 1 Конвенції ООН про права дитини*). Усі особи віком до 18 років (*стаття 2 Конвенції Міжнародної організації праці (МОП) №182 про найгірші форми дитячої праці*). Будь-яка особа до 18 років (*стаття 3(d) Протоколу про запобігання і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї, що доповнює Конвенцію ООН проти транснаціональної організованої злочинності («Палермський протокол»*). Будь-яка особа віком до 18 років *(стаття 3(a) Конвенції Лансароте*). Всі особи віком до 18 років. Проте держава-учасниця може вимагати нижчу вікову межу, яка не може бути нижчою за 16 років *(стаття 9 Конвенції Ради Європи про кіберзлочинність* *(«Будапештська конвенція»*).

Дитяча порнографія	Будь-які матеріали, які візуально зображують дитину, залучену до реальної або модельованої явно сексуальної поведінки; будь-яке зображення дитячих статевих органів, здебільшого із сексуальною метою (*стаття 20 Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального розбещення, CETS № 201; Факультативний протокол до Конвенції про права дитини, що стосується торгівлі дітьми, дитячої проституції та дитячої порнографії*). Зображення у будь-який спосіб дитини чи особи, яка виглядає як дитина, у реальному чи змодельованому відверто сексуальному образі або задіяної у реальній чи змодельованій відверто сексуальній поведінці, або будь-яке зображення статевих органів дитини в сексуальних цілях (*примітка до ст.156[1] ККУ*).
Дитяча проституція	Використання дитини у діяльності сексуального характеру за винагороду або будь-яку іншу форму відшкодування (*Факультативний протокол до Конвенції про права дитини, що стосується торгівлі дітьми, дитячої проституції та дитячої порнографії*). Факт використання дитини для діяльності сексуального характеру, коли гроші чи інша форма винагороди або компенсація надаються чи обіцяються як оплата, незалежно від того, чи надано цю платню, обіцянку або винагороду дитині чи третій особі (*стаття 19 Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального розбещення, CETS №201*).
Домагання дитини із сексуальними цілями	Правопорушення, що полягає в зумисній пропозиції, зробленій дорослою людиною за допомогою інформаційно-комунікаційних засобів, зустрітися з дитиною, яка не досягла встановленого національним законодавством повноліття, для вступу в сексуальні зносини, з метою залучення дитини до діяльності сексуального характеру або виготовлення дитячої порнографії, якщо після цієї пропозиції відбулися істотні дії, що призвели до такої зустрічі (*стаття 23 Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального розбещення, CETS №201*).

Кібербулінг/ булінг в цифровому середовищі	Навмисна агресивна дія, що неодноразово вчиняється групою осіб або окремою особою за допомогою цифрових технологій, яка передбачає використання цифрових технологій та інтернету для розміщення чутливої інформації про будь-кого, навмисне поширення відомостей особистого характеру, небажаних світлин або відео, надсилання повідомлень із погрозами чи образами (електронною поштою, у форматі миттєвого обміну повідомленнями, в чатах і текстових повідомленнях), поширення пліток та неправдивої інформації про особу або навмисне виключення її з онлайн-спілкування. Може відбуватися безпосередньо (в чатах або текстових повідомленнях), у межах спільноти з обмеженим доступом (розсилання постів та дратівливих повідомлень за списком електронних адрес) або ж у громадському доступі (наприклад створення сайтів для навмисного знущання з постраждалої особи) (*Рекомендації для директивних органів щодо захисту дитини в цифровому середовищі, Guide to Using the Child Online Safety Assessment Tool (UNICEF) 2016*). Психологічне, фізичне, економічне чи сексуальне насильство, тобто будь-яке умисне діяння (дія або бездіяльність) із застосуванням засобів електронних комунікацій, яке систематично вчиняється особою стосовно дитини, з якою вони є учасниками одного колективу, або дитиною стосовно іншого учасника одного колективу та яке порушує права, свободи, законні інтереси потерпілої особи та/або перешкоджає виконанню нею визначених законодавством обов'язків *(Закон України «Про охорону дитинства»)*.
Матеріали, пов'язані з сексуальною експлуатацією та сексуальним насильством стосовно дітей (CSEM/CSAM)	Запис матеріалів, пов'язаних із сексуальними зловживаннями щодо дітей з боку дорослих; зображення дітей, залучених до відвертих сексуальних дій, статевих органів дітей, коли зображення створюються або використовуються насамперед з метою сексуального характеру *(Рекомендації для директивних органів щодо захисту дитини в цифровому середовищі)*. Стосується представлення будь-якими засобами, включаючи, але не обмежуючись, фотографії, відео, малюнки, мультфільми, текст і прямі трансляції – дитини, яка бере участь у реальних або імітованих відвертих діях сексуальні дії або будь-яке зображення статевих органів дитини перш за все в сексуальних цілях (*Guide to Using the Child Online Safety Assessment Tool (UNICEF) 2016 на основі статті 2 Факультативного протоколу до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції та дитяча порнографія*). Будь-які матеріали, зазвичай зображення, відео та аудіофайли, із зображенням актів сексуального насильства над дітьми, включаючи зображення відвертих зображень інтимних частин тіла для сексуальних та фінансових цілей *(Європол)*.

Сексуальний примус або вимаганням в цифровому середовищі	Шантаж особи за допомогою власноруч створених зображень цієї особи з метою вимагання у неї сексуальних послуг, грошей або інших благ під загрозою поширення матеріалу без згоди особи, що фігурує в ньому (наприклад через публікування зображень у соціальних мережах) *(Рекомендації для директивних органів щодо захисту дитини в цифровому середовищі).*
Секстинг (Sexting)	Самостійно створений контент сексуального характеру, надісланий іншим за допомогою текстових повідомлень мобільного телефону або в іншій мережі повідомлень (*OPSC Guidelines*). Зазвичай визначається як надсилання, отримання власноруч створеного сексуального контенту, зокрема зображення, повідомлення або відео, чи обмін ними за допомогою мобільних телефонів та/або інтернету *(Рекомендації для директивних органів щодо захисту дитини в цифровому середовищі).* Надсилання інтимних фото/відео із використанням сучасних засобів зв'язку *(проєкт StopSextинг).*
Сексторшен	Налагодження довірливих стосунків з дитиною в інтернеті з метою отримання приватних матеріалів, шантажування та вимагання додаткових матеріалів чи грошей *(проєкт StopSextинг).*
Сексуальне насильство над дітьми в інтернеті	Термін широко використовується для позначення сексуального насильства над дітьми, якому сприяють інформаційно-комунікаційні технології (наприклад онлайн-грумінг) і до сексуального насильства над дітьми, яке вчинено в іншому місці, а потім публікується в інтернеті. Це відбувається, коли, наприклад дитина зазнає сексуального насильства офлайн, але фотографії або відео насильства потім завантажуються, розповсюджуються та доступні в інтернеті (що є матеріалом сексуального насильства над дітьми) *(Luxembourg Guidelines).*
Сексуальна експлуатація дитини	Це відбувається, коли дитина бере участь у сексуальній діяльності в обмін на щось (наприклад прибуток або вигода, або навіть обіцянка такого) від третьої сторони або злочинець. Дитина може бути примушена до ситуації сексуальної експлуатації через фізичну силу чи погрози або переконання брати участь у сексуальних діях як результат людських або ситуаційних факторів, таких як дисбаланс сил між потерпілим і правопорушником (*Luxembourg Guidelines*). Це включає «всі дії сексуального характеру, що здійснюються проти дитини, яка на певному етапі має зв'язок з інтернетом» (*Luxembourg Guidelines*).
Участь дитини у порнографічних виставах	Правопорушення, що передбачають такі зумисні дії: а) вербування дітей для участі в порнографічних виставах або спонукання до участі в таких виставах; б) примушування дитини до участі в порнографічних виставах чи отримання вигоди від цього чи іншого використання дитини з цією метою; в) свідоме відвідування порнографічних вистав, до яких залучено дітей (*стаття 21 Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального розбещення, CETS № 201*).

Додаток 1.9.1.3.

Терміни, які слід використовувати з обережністю або повністю уникати	Рекомендовано
Дитячий секс-туризм	Сексуальна експлуатація дітей у контексті подорожей і туризму
Дитячий секс-турист	Мандрівні виконавці сексуальних злочинів над дітьми
Дитяча проституція	Експлуатація дітей у/для проституції
Дитина-повія, дитячий секс-працівник	Постраждала від сексуальної експлуатації
Клієнт	Зловмисник, сексуальний злочинець
Вебкамера дитячого секс-туризму/ вебкамера сексуального насильства над дітьми	Сексуальне насильство над дітьми в прямому етері

Жертва (*victim*)	Постраждала особа (*survivor*)
Людина, яка зазнала сексуального насильства, може називати та вважати себе «жертвою» або «постраждалою» («особою, яка вижила»). Термін «жертва» часто асоціюється з слабкістю. З іншого боку, термін «постраждала» може означати силу та свободу волі.	

Дитяча порнографія	Матеріали сексуального насильства щодо дітей
Європол заохочує використовувати термін «матеріали (сексуального) насильства щодо дітей», а не «дитяча порнографія». Використання терміну «дитяча порнографія» наводить на думку, що діти позують у «провокаційних» позах, а не зазнають жахливих образ. Водночас фотографія або відео фіксує реальну ситуацію, коли дитина зазнала насильства. Це не порнографія. У Люксембурзьких рекомендаціях наголошується на тому, що дитяча порнографія може (довільно чи мимоволі) сприяти полегшенню ступеня важкості, зменшенню значущості або навіть легітимізації того, що фактично є сексуальними зловживаннями щодо дітей та/або їх сексуальною експлуатацією [...]. Термін «дитяча порнографія» створює небезпеку його таким тлумаченням, ніби дії вчиняються за згодою дитини і є законним матеріалом сексуального характеру. Від терміну «дитяча порнографія» поступово відмовляються численні правоохоронні органи та міжнародна спільнота із захисту дітей, оскільки в ньому використано лексику, що не орієнтована на постраждалу особу, та яка може ненавмисно узаконити матеріали із сексуальним насильством над дітьми через застосування слова «порнографія». Серйозність жорстокого поводження з ними не слід зменшувати такими словами, як «порно». Порнографія – це термін, який використовується для дорослих, які беруть участь у статевих актах за згодою, які поширюються (переважно) легально серед широкої громадськості для отримання сексуального задоволення. Такі терміни, як «дитяча порнографія» та «дитяча порнографія», також використовуються злочинцями, і вони не повинні бути законною мовою, яку використовують правоохоронні органи, судові органи, громадськість чи ЗМІ.	

Заняття 1.9.2. Суб'єкти забезпечення та захисту прав дітей в кіберпросторі

Мета: систематизувати знання учасників щодо кола суб'єктів забезпечення та захисту прав дітей в кіберпросторі та принципів їх діяльності.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Коло суб'єктів	Інформаційне повідомлення	20 хв	Додаток 1.9.2.1, мультимедійне обладнання
2.	«Гарячі лінії» як суб'єкт забезпечення та захисту прав дітей в кіберпросторі	Тестовий дзвінок	15 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, мобільний телефон
3.	Права дітей в цифровому середовищі	Робота в групах	40 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.9.2.2
4.	Принципи діяльності суб'єктів	Обговорення	15 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери або мультимедійне обладнання, Додаток 1.9.2.3

ХІД ЗАНЯТТЯ

1. Інформаційне повідомлення «Коло суб'єктів»

Мета: надати учасникам інформацію щодо переліку суб'єктів забезпечення та захисту прав дітей в кіберпросторі.

Час: 20 хв.

Необхідні матеріали: Додаток 1.9.2.1, мультимедійне обладнання.

Хід проведення:

Тренер/тренерка зазначає: «*Відповідно до Рекомендації CM/Rec (2018)7 Комітету міністрів про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі, державам слід впроваджувати скоординований підхід, заснований на співпраці із зацікавленими сторонами, включно з національними, регіональними та місцевими правоохоронними та іншими органами влади, освітніми та соціальними службами, незалежними правозахисними установами, правоохоронними органами, професіоналами, які працюють як для дітей, так і з дітьми, громадянським суспільством, зокрема організаціями, що працюють з дітьми та молоддю, підприємствами, галузевими асоціаціями, дослідниками, сім'ями та дітьми, відповідно до їхніх ролей та функцій. Суб'єкти забезпечення та захисту прав дітей в кіберпросторі умовно можна поділити на три рівні: міжнародний, європейський та національний*», після чого презентує інформацію із Додатка 1.9.2.1.

До уваги тренера/тренерки!

Слід підготувати презентацію на основі матеріалу, який міститься в Додатку 1.9.2.1, обсяг і зміст якої залежатиме від запитів цільової аудиторії учасників. Доцільно вивести на слайди презентації перелік суб'єктів на кожному із рівнів: міжнародному, європейському та національному, акцентуючи особливу увагу на Інтерполі та Європолі. Слід врахувати, що наведений в Додатку перелік суб'єктів не є вичерпним. Під час підготовки до заняття доцільно перевірити актуальність інформації, викладеної у Додатку.

Запитання для обговорення:

- *Про яких суб'єктів захисту дітей в кіберпросторі ви дізнались вперше?*
- *Чи мали ви досвід взаємодії з іншими суб'єктами під час діяльності, спрямованої на захист прав дітей в кіберпросторі?*

2. Тестовий дзвінок «Гарячі лінії» як суб'єкт забезпечення та захисту прав дітей в кіберпросторі»

Мета: надати учасникам інформацію щодо діяльності «гарячих ліній» для дітей та сприяти усвідомленню важливості інформування дітей про їх існування.

Час: 15 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, мобільний телефон.

Хід проведення:

Тренер/тренерка зазначає: *«Як зазначалось у попередній презентації, одними із важливих суб'єктів захисту прав дітей у кіберпросторі є «гарячі лінії». В Україні функціонують три «гарячі лінії» для дітей, спрямовані на захист їх від насильства, зокрема онлайн – 116 111, 15 47, 15 45 (*3)».* Тренер/тренерка зазначає на аркуші фліпчарту номери телефонів та звертається до учасників із пропозицією здійснити тестові дзвінки на «гарячі лінії», після чого обирає трьох добровольців, які повинні з використанням режиму гучного звуку здійснити по черзі тестовий дзвінок на одну із «гарячих ліній», під час якого дізнатись рекомендації у разі вчинення насильства щодо дітей в інтернеті, або як часто діти звертаються з питаннями щодо безпеки в інтернеті та захисту їхніх прав, або отримати консультацію з будь-якого іншого тематичного питання, яке може запропонувати група.

Запитання для обговорення:

- *Чи отримали ви відповіді на поставлені питання під час здійснення тестового дзвінка?*
- *У яких випадках діти можуть звертатись на «гарячі лінії»?*
- *Чи важливим є функціонування «гарячих ліній» для дітей?*

Тренер/тренерка звертається до учасників з проханням зафіксувати номери «гарячих ліній» для дітей в телефонні книги мобільних телефонів та розповсюджувати їх серед дітей, зокрема під час проведення інформаційно-просвітницьких заходів.

До уваги тренера/тренерки!

Якщо добровольців для здійснення тестових дзвінків у групі не знайдеться, тренер/тренерка може зробити їх особисто.

Якщо учасники/учасниці будуть незадоволені отриманою консультацією на «гарячій лінії», слід обговорити людський фактор, який може впливати на професійність в будь-якій сфері.

3. Робота в групах «Права дітей в цифровому середовищі»

Мета: надати інформацію про права дітей в цифровому середовищі, відпрацювати вміння пояснення цих прав доступною для дітей мовою.

Час: 40 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.9.2.2.

Хід проведення:

Тренер/тренерка зазначає: *«Відповідно до Резолюції 32-й сесії Ради ООН з прав людини «Заохочення, захист і здійснення прав людини в інтернеті», ті самі права, які людина має в офлайн-середовищі, повинні також захищатися в онлайн-середовищі. Крім того, в Рекомендації CM/Rec (2018)7 Комітету міністрів про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі виокремлено основні права дитини в цифровому середовищі».*

Тренер/тренерка об'єднує учасників у шість груп та закріплює за кожною із них одне із прав дитини в цифровому середовищі:

група 1 – доступ до цифрового середовища;

група 2 – свобода слова та вираження поглядів;

група 3 – участь та свобода об'єднань;

група 4 – конфіденційність та захист даних;

група 5 – право на освіту;

група 6 – право на захист і безпеку.

До уваги тренера/тренерки!

Доцільно завчасно підготувати стікери із зазначеними на них правами та запропонувати одному із учасників кожної групи витягнути один із них так, щоб учасники інших груп не бачили напис на стікері.

Кожна група протягом 15 хвилин має обговорити, як вони розуміють це право, а також схематично викласти його зміст на аркуші фліпчарту та підготуватись до його пояснення доступною для дітей мовою. Крім того, слід обговорити в групі, чи повною мірою це право дотримується в Україні, та якою є роль поліцейських у його забезпеченні або захисті.

Після завершення часу на роботу в групах кожна із груп протягом трьох хвилин демонструє свої напрацювання. На початку презентації кожної групи учасники з інших груп по зображенню на аркуші фліпчарту мають здогадатись, про яке право дитини у цифровому середовищі йтиметься. Водночас слід пам'ятати про обмежений час на вправу: якщо протягом однієї хвилини правильної відповіді не пролунає, група розпочинає презентацію.

Тренер/тренерка може доповнювати відповіді груп, використовуючи інформацію із Додатка 1.9.2.2. Так само слід звернути увагу на доступність для дітей мови, якою учасники презентували напрацювання.

До уваги тренера/тренерки!

Після завершення презентації всіх груп слід акцентувати увагу, що Радою Європи розроблена та має український переклад адаптована для дітей версія Рекомендації Ради Європи щодо поваги, захисту та здійснення прав дитини в цифровому середовищі, з якою можна ознайомитись за посиланням: https://rescentre.org.ua/images/Uploads/Images/Internet-safety_blog/Learn_about_your_rights_in_a_digital_environment_UKR.pdf.pdf.

За необхідності, можна вивести Qr-код з посиланням на екран.

Запитання для обговорення:

- *Чи складно було виконувати вправу?*
- *Забезпечення якого із розглянутих нами прав дітей в цифровому середовищі безпосередньо залежить від рівня підготовки поліцейських?*

4. Обговорення «Принципи діяльності суб'єктів»

Мета: надати інформацію про принципи діяльності суб'єктів забезпечення та захисту прав дітей, сприяти усвідомленню учасниками важливості їх дотримання та врахування у власній діяльності.

Час: 15 хв.

Необхідні матеріали: мультимедійне обладнання, Додаток 1.9.2.3.

Хід проведення:

Тренер/тренерка зазначає: «*У своїй діяльності, спрямованій на забезпечення та захист прав дітей в цифровому середовищі, суб'єкти мають враховувати такі принципи:*

- *забезпечення найкращих інтересів дитини;*
- *динамічних можливостей дитини;*
- *недопущення дискримінації;*
- *участі;*
- *залучення інших зацікавлених осіб*»

та звертається до учасників із запитанням: «*Чи всі принципи вам знайомі та зрозумілі?*»

До уваги тренера/тренерки!

Доцільно зафіксувати зазначені принципи на аркуші фліпчарту або вивести їх перелік на екран.

За потреби, тренер/тренерка пояснює зміст тих принципів, які незнайомі або незрозумілі учасникам, використовуючи Додаток 1.9.2.3.

До уваги тренера/тренерки!

Якщо учасники зазначають, що всі принципи їм знайомі та зрозумілі, варто попросити учасників пояснити зміст цих принципів.

Запитання для обговорення:

- *Чи вдається вам дотримуватись всіх розглянутих принципів під час діяльності, спрямованої на забезпечення та захист прав дітей в цифровому середовищі? Якщо ні, то чому?*
- *Чи відрізняються принципи забезпечення та захисту прав дітей в онлайн- та офлайн-середовищі?*

Тестові питання до заняття:

1. Який із зазначених номерів не є номером «гарячої лінії», спрямованої на захист прав дітей?

А) 116 111;

Б) 15 47;

В) 15 45 (3);

Г) всі номери телефонів є «гарячими лініями» для дітей, зокрема з питань захисту їхніх прав в інтернеті.

2. Який суб'єкт є володільцем Міжнародної бази даних про сексуальну експлуатацію дітей (ICSE)?

А) Міжнародна мережа «гарячих ліній» INHOPE;

Б) Європол;

В) Інтерпол;

Г) ECPAT International.

3. Які права дитини в цифровому середовищі закріплені в Рекомендації Комітету Ради Європи CM/Rec (2018)7?

А) доступ до цифрового середовища;

Б) конфіденційність та захист даних;

В) захист та безпека;

Г) всі зазначені права і не тільки закріплені в цій рекомендації Комітету Ради Європи.

4. До взаємодії із забезпечення та захисту прав дітей в кіберпросторі варто залучати комерційні підприємства?

А) так;

Б) ні;

В) тільки в країнах ЄС;

Г) складно відповісти.

5. Який принцип мають враховувати суб'єкти під час своєї діяльності, спрямованої на забезпечення та захист прав дітей в цифровому середовищі?

А) динамічних можливостей дитини;

Б) участі;

В) залучення всіх зацікавлених осіб;

Г) всі відповіді правильні.

Ключі-відповіді:

1. Г; 2. В; 3. Г; 4. А; 5. Г.

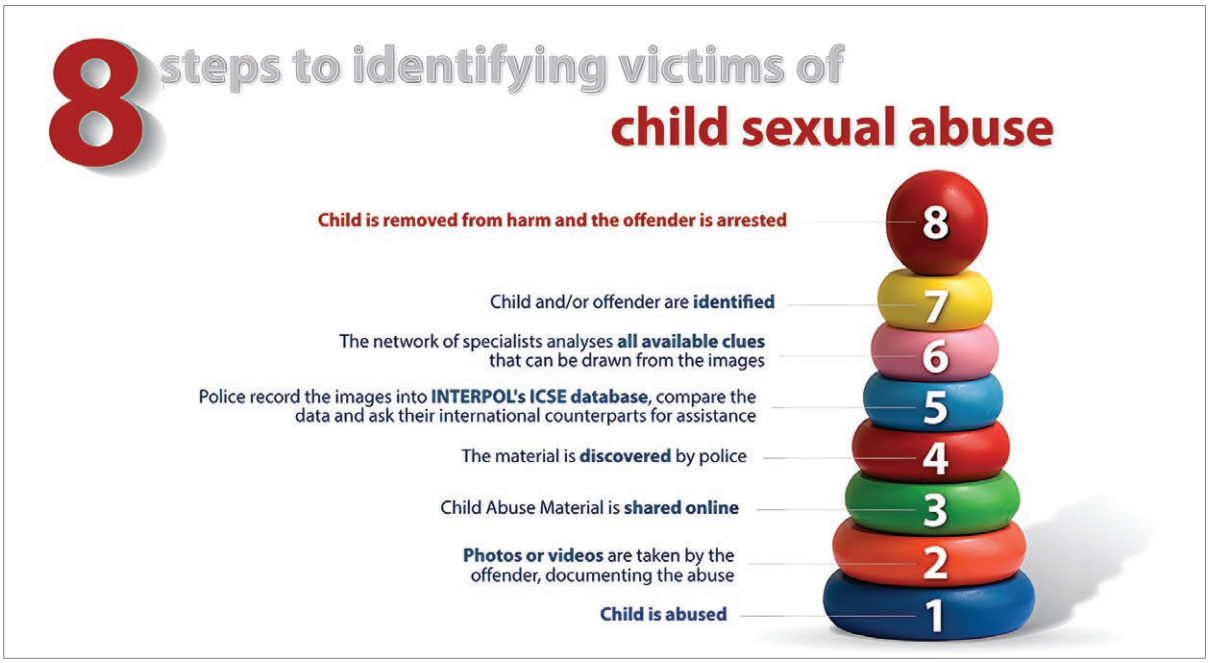
Додаток 1.9.2.1

Суб'єкти забезпечення та захисту прав дітей в кіберпросторі. Міжнародний рівень

- Організація Об'єднаних Націй (ООН)
- **Спеціальний представник Генерального секретаря ООН з питань насильства над дітьми**, який щорічно звітує про стан дотримання прав дітей перед Генеральною Асамблеєю ООН;
- **ЮНІСЕФ (UNICEF)** – Агентство ООН у справах дітей, при якому створено дослідницький офіс ЮНІСЕФ – Innocenti, який координує та сприяє дослідженню використання дітьми цифрових технологій за допомогою розроблення методологій дослідження, які можна застосувати для отримання національних даних. Також ЮНІСЕФ Innocenti координує дві багатонаціональні програми досліджень, Global Kids Online і Disrupting Harm, які слугують для дослідження можливостей і ризиків, з якими діти з усього світу можуть зіткнутися в епоху цифрових технологій.
- **Міжнародний союз електрозв'язку (ITU)** започаткував ініціативу «Захист дитини в цифровому середовищі» (COP), покликану об'єднати партнерів з усіх секторів світової спільноти в інтересах створення безпечних і таких, що розширюють безпечні можливості в цифровому середовищі для дітей у цілому світі. ITU підготовлено рекомендації щодо захисту дітей у цифровому середовищі. Відповідно до рекомендацій, для органів влади важливо, щоб працівники правоохоронних органів пройшли належну підготовку для проведення розслідування злочинів проти дітей та молодих осіб, пов'язаних з інтернетом. Їм потрібен належний рівень технічних знань та доступ до сучасних інструментів, щоб вони могли вилучати й інтерпретувати дані, отримані з комп'ютерів чи із мережі, за мінімальний час. Крім того, дуже важливо, щоб органи охорони правопорядку сформували чіткі механізми, які дозволяють дітям та молоді чи будь-якому іншому громадянину повідомляти про будь-які випадки або побоювання, які можуть виникнути у них щодо безпеки дитини чи підлітка в цифровому середовищі. У багатьох країнах, наприклад, створено «гарячі лінії» для спрощення передавання повідомлень про CSAM, і є аналогічні спеціальні механізми для спрощення передавання повідомлень про інші види проблем, наприклад про булінг. Правоохоронні органи є основним суб'єктом виявлення та вилучення CSAM. Необхідно організувати процес вивчення цих матеріалів, щоб установити, чи можна ідентифікувати місцевих постраждалих. Там, де це неможливо, матеріали слід передати до Інтерполу для включення до бази даних ICSE. Також в рекомендаціях перелічені конкретні міркування, які слід узяти до уваги представникам директивних органів під час розгляду онлайн-ризиків.
- **End Violence Against Children** – у липні 2016 року Генеральний секретар ООН заснував Глобальне партнерство та Фонд для припинення насильства щодо дітей. Партнерство працює з унікальною коаліцією з понад 750 організацій, зокрема уряди, агентства ООН, науково-дослідні установи, міжнародні неурядові організації, фонди, місцеві громадські організації, групи приватного сектору та релігійні організації. Поміж іншим, End Violence Against Children спільно з ЮНІСЕФ інвестують у технологічні стартапи, щоб забезпечити захист дітей в кіберпросторі.
- **ECPAT International** – координує дослідження та дії, спрямовані на припинення сексуальної експлуатації дітей, підтримує захист дітей і розширення можливостей у 103 країнах.
- **INHOPE** – міжнародна мережа «гарячих ліній» для повідомлень про матеріали сексуального насильства та сексуальної експлуатації щодо дітей онлайн. Держави-члени впровадили процедури «виявити та видалити» (*notice and takedown*) щодо контенту, який

містить сексуальну експлуатацію та насильство щодо дітей, через національні «гарячі лінії», за допомогою яких користувачі можуть повідомити про відповідні матеріали. Станом на 2023 рік мережа охоплює 50 «гарячих ліній» у 46 країнах. «Гарячі лінії» зазвичай спочатку отримують повідомлення від користувачів про місцезнаходження протиправного контенту (URL-адреса), потім проводять аналіз контенту та, у разі його протиправності, інформують хостинг провайдера та правоохоронні органи. Щодо видалення контенту, то часто воно можливе без залучення правоохоронних органів, залежно від домовленості між операторами «гарячих ліній», правоохоронними органами та провайдерами (наприклад у Франції, Угорщині, Польщі, Португалії, Великій Британії тощо). У деяких країнах правоохоронні органи інформують провайдерів про необхідність видалення протиправного контенту (зокрема у Німеччині, Болгарії, Естонії, Фінляндії, Словаччині), а у деяких – необхідне рішення суду з можливістю, щоправда, тимчасово блокувати контент до винесення відповідного рішення (Кіпр та Хорватія). Якщо контент, що містить сексуальну експлуатацію та насильство щодо дітей, знаходиться у юрисдикції третьої країни, то держави-члени ЄС використовують ресурси мережі INHOPE для його видалення, в інших випадках «гарячі лінії» спрямовують звернення до відповідальних правоохоронних органів у цих країнах (часто через Європол чи Інтерпол). У випадках, коли видалення контенту з різних причин є неможливим, держави-члени ЄС також використовують механізми блокування, які у деяких країнах потребують дозволу суду (Іспанія, Угорщина), запитів правоохоронних органів (Франція, Італія, Португалія) або ж впроваджуються провайдерами добровільно (Болгарія, Чехія, Велика Британія). Здебільшого правоохоронні органи або галузеві регулятори формують список протиправних вебсторінок та передають його провайдерам.

- **Insafe** – всесвітня мережа центрів обізнаності, що сприяють безпечному та відповідальному використанню інтернету молодими людьми. Кожен національний центр проводить просвітницькі та просвітницькі кампанії, працює з телефонною лінією довіри та тісно співпрацює з молоддю. Insafe підтримує кампанію День безпечного інтернету, який щорічно відзначається у першу суботу лютого приблизно у 180 країнах і територіях у всьому світі, зокрема і в Україні.
- **WeProtect Global Alliance (WPGA)** є глобальним рухом для трансформації методів боротьби з сексуальною експлуатацією дітей в цифровому середовищі у світі. Це союз урядових структур, глобальних технологічних компаній та організацій громадянського суспільства. Станом на 2023 рік Глобальний альянс складається зі 101 уряду, 65 компаній приватного сектору, 87 організацій громадянського суспільства, 9 міжурядових організацій, серед яких Інтерпол, Європол, ЮНІСЕФ тощо. Уряди створюють і впроваджують правове середовище для запобігання та реагування на сексуальну експлуатацію та насильство над дітьми. Приватні компанії працюють над тим, щоб допомогти обмежити негативний вплив своєї продукції. Організації громадянського суспільства підтримують постраждалих осіб; працюють над створенням кращих інструментів для виявлення та відстеження незаконних матеріалів. Місія Глобального альянсу WePROTECT полягає у виявленні та захисті більшої кількості постраждалих осіб, затриманні більшої кількості злочинців та припиненні сексуальної експлуатації дітей в цифровому середовищі. Глобальний Альянс розробив Модель національного реагування (MNR) (https://www.weprotect.org/resources/frameworks/model-national-response/), у якому викладено рекомендації для країн і організацій, щоб підтримати їх у запобіганні та боротьбі з сексуальною експлуатацією та насильством над дітьми.
- **Інтерпол** – допомагає поліції виявити постраждалих від сексуальної експлуатації та насильства дітей через аналіз фото і відео, знайдених в інтернеті або на вилучених пристроях.



Ідентифікація. Ідентифікація постраждалих дітей, зображених у матеріалах про сексуальне насильство, є головним пріоритетом для правоохоронних органів, оскільки це також може допомогти знайти злочинців. Вирішальне значення має Міжнародна база даних зображень сексуальної експлуатації дітей (ICSE) (https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database), яка використовує складне програмне забезпечення для порівняння зображень, щоб встановити зв'язки між постраждалими та місцями. ICSE дозволяє сертифікованим користувачам отримувати доступ до бази даних у режимі реального часу – досліджувати наявні елементи, завантажувати нові дані, сортувати матеріали, проводити аналіз та спілкуватися з іншими експертами у всьому світі з питань, пов'язаних із розслідуванням випадків сексуальної експлуатації дітей. Вона містить понад 4,3 мільйона зображень і відео та допомогла ідентифікувати понад 32 000 постраждалих дітей у всьому світі, а також понад 14 000 злочинців станом на 2023 рік. Після вивчення випадкового відбору відео та зображень у базі даних ICSE INTERPOL та ECPAT International у лютому 2018 року опублікували спільний звіт під назвою «Назустріч глобальному показнику щодо невідомих постраждалих у матеріалах сексуальної експлуатації дітей». Дослідження виявило низку тенденцій:

- чим молодша постраждала дитина, тим важче насильство;
- 84% зображень містили відверту сексуальну активність;
- понад 60% неідентифікованих постраждалих були в препубертатному віці, включно з немовлятами і дітьми раннього віку;
- 65% невідомих постраждалих були дівчатами;
- на зображеннях жорстокого насильства, болю, ймовірно, зображені хлопчики;
- 92% видимих правопорушників були чоловіками.

Запобігання розповсюдженню матеріалів сексуального насильства над дітьми. Інтерпол тісно співпрацює з постачальниками послуг інтернету, щоб заблокувати доступ до матеріалів про насильство над дітьми в інтернеті. Блокування доступу запобігає повторній віктимізації дітей, що зазнали жорстокого поводження, і має виховний вплив на користувачів, які, можливо, збираються переглядати чи завантажувати незаконні матеріали. Щоб заблокувати доступ до інтернет-доменів, які поширюють матеріали сексуального насильства над діть-

ми, поліція може надати інтернет-провайдерам список доменів або вебадрес («*Worst of*»), які потрібно заблокувати в їх мережах. Коли користувачі намагаються переглянути сторінку, вони можуть бути перенаправлені на «зупинену сторінку», яка містить інформацію про причину перенаправлення, посилання на законодавство, куди поскаржитися, тощо. Список «*Worst of*» містить домени, які поширюють матеріали сексуального насильства над дітьми та які були перевірені принаймні двома різними країнами/агенціями. Домени, внесені до списку «*Worst of*», містять зображення та відео, які відповідають таким критеріям:

- діти «справжні»;
- вік зображених дітей є (або здається) меншим за 13 років;
- зловживання вважається тяжким.

Відповідна термінологія. Існує очевидна потреба, щоб поліція та її партнери «говорили однією мовою», особливо в контексті ідентифікації постраждалих дітей, щоб посилити збір даних і співпрацю між установами, секторами та країнами. Разом із міжнародними експертами Інтерпол рекомендує використовувати відповідну термінологію для опису сексуального насильства над дітьми або сексуальної експлуатації. Люксембурзькі рекомендації були розроблені групою з 18 міжнародних партнерів, включно з Інтерполом. Інтерпол рекомендує використовувати їх правоохоронним органам у всьому світі.

Навчання. Основна функція спеціалізованих експертів Інтерполу у цій галузі полягає в тому, щоб допомогти поліції в країнах-членах розширити свій потенціал для розслідування сексуальної експлуатації дітей. Інтерпол організовує навчальні курси в усіх регіонах світу та охоплює весь спектр розслідувань сексуального насильства над дітьми: проведення розслідувань в онлайн-середовищі; використання міжнародної бази даних Інтерполу про сексуальну експлуатацію дітей; методи ідентифікації потерпілих; техніка опитування постраждалої особи та правопорушника; категоризація та сортування матеріалів сексуального насильства над дітьми. Спеціалізовані офіцери Інтерполу можуть надавати поради країнам щодо створення підрозділів ідентифікації постраждалих дітей і можуть надати індивідуальну підтримку національним органам влади.

Група спеціалістів зі злочинів проти дітей (SGCAC) збирається щорічно, щоб сприяти та посилювати розслідування сексуальних злочинів проти дітей. Об'єднуючи правоохоронні органи, регіональні та міжнародні організації, неурядові організації, приватний сектор та наукові кола, група визначає нові тенденції та методи і розвиває передовий досвід. Через саму свою природу ідентифікація потерпілих є складною роботою, яка потребує спеціалістів із самих різних галузей. Часто співробітники правоохоронних органів тісно співпрацюють з уповноваженими цивільними аналітиками, щоб визначити походження серії зображень або відео. Фахівці з ідентифікації постраждалих осіб тісно співпрацюють зі своїми колегами у всьому світі, щоб гарантувати, що унікальні, типові або легко впізнавані докази в одній країні не будуть пропущені в іншій країні.

Мандрівні сексуальні злочинці. Деякі сексуальні злочинці перетинають кордони, що дає змогу їм залишатися поза полем зору місцевої влади та отримувати доступ до дітей. Інтерпол може видати зелене сповіщення, щоб попередити про злочинну діяльність особи, якщо ця особа вважається загрозою для дітей, або блакитне сповіщення, щоб зібрати інформацію про особу, її місцезнаходження чи діяльність, пов'язану зі злочином.

Зниклі, викрадені та продані діти. За запитом країни-члена Інтерпол може видати жовте повідомлення, щоб допомогти знайти зниклих безвісти осіб, особливо дітей. Ці повідомлення поширюються на міжнародній основі та реєструються в базі даних про зниклих і викрадених дітей. Жовте сповіщення також можна використовувати, щоб допомогти ідентифікувати особу, яка не може ідентифікувати себе. Поліція однієї з країн-членів запитує жовте

повідомлення через своє Національне центральне бюро та надає інформацію про випадок. Повідомлення потім публікується Генеральним секретаріатом у базі даних Інтерпол, яка сповіщає поліцію в усіх країнах-членах.

Європейський рівень

- **Рада Європи** приділяє особливу увагу розширенню можливостей дітей та їхніх близьких безпечно орієнтуватися у цифровому середовищі. Цьому сприяють освітні інструменти, включно з такими посібниками: Довідник з питань грамотності в інтернеті (2017 р.); «Батьки в цифрову епоху» – настанова для батьків щодо захисту дітей від сексуальної експлуатації та сексуальних зловживань в цифровому середовищі (2017 р.); «Це наш світ» – погляди дітей на те, як захистити їхні права в цифровому середовищі (2017 р.); «Цифрове громадянство... і ваша дитина» – те, що повинен знати і робити кожен із батьків (2019 р.); «Два кліки вперед і один клік назад» – доповідь про дітей з інвалідністю у цифровому середовищі (2019 р.).
- **Комітет Міністрів Ради Європи** в Рекомендації CM/Rec (2014) 6 («Посібник з прав людини для інтернет-користувачів»: https://rm.coe.int/16802e3e96) зазначає, що права людини та основні свободи рівною мірою стосуються як офлайн-, так і онлайн-простору. Діти та молодь мають право на особливий захист і допомогу під час роботи в інтернеті. З відео, розробленими відповідно до цього посібника, можна ознайомитись за посиланням: https://www.youtube.com/channel/UCeuQLmBXJMdjLl5lUEUQDlA.
- **Проєкт Ради Європи «Боротьба з насильством щодо дітей в Україні»**, який реалізується в України з 2017 року, спрямований на запобігання та захист дітей від насильства, зокрема сексуальної експлуатації та насильства, в цифровому середовищі також. В межах реалізації цього проєкту було підготовлено Аналіз прогалин у законодавстві, політиках і практиках, спрямованих на запобігання та протидію сексуальній експлуатації та насильству щодо дітей в інтернеті та їх подоланні в Україні, а також Звіт з оцінки прогресу стосовно рекомендацій: https://rm.coe.int/progress-assessment-report-ukr/16809fab80.
- **Проєкт «Права людини та інтернет»** спрямований на формування знань та навичок свідомого користування інтернетом, навчання правам людини онлайн та запуск механізмів реагування на їх порушення. Проєкт здійснюється за фінансової та технічної підтримки Ради Європи та Європейського Союзу.
- **Лансаротський комітет** (Комітет Сторін Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства) – це орган, створений для здійснення моніторингу процесу ефективного впровадження Конвенції державами-учасницями у власному законодавстві та політиці. Процедура моніторингу поділяється на раунди, кожен з яких стосується конкретної тематичної сфери та водночас охоплює усі держави. Другий тематичний раунд моніторингу Комітет Лансароте вирішив зосередитись на викликах, пов'язаних зі створеними дітьми сексуальними зображеннями та/або відео. Результатом цього раунду моніторингу є звіт «Захист дітей від сексуальної експлуатації та сексуального насильства шляхом інформаційно-комунікаційних технологій (ІКТ): вирішення проблем створених дітьми сексуальних зображень та/або відео», прийнятий 10 березня 2022 року. Основні результати моніторингу Комітету Лансароте:
- щодо правової бази:
  - не переслідувати дітей за володіння ними створених власних сексуальних зображень та/або відео іншої дитини (якщо зображена дитина надала свою інформовану згоду) та іншої дитини, якщо такий матеріал отримано без активного запиту;
  - не переслідувати дітей за те, що вони поширюють такі матеріали з іншою дитиною, якщо вони призначені винятково для власного приватного користування;

- притягнення до кримінальної відповідальності має бути крайнім засобом за поширення або передачу дітьми сексуального матеріалу, створеного іншими дітьми, якщо такий матеріал кваліфікується як «дитяча порнографія»;
- забезпечити, щоб у разі звільнення від кримінальної відповідальність за володіння дорослими зображеннями сексуального характеру та/або відео, які створили самі діти, діяли такі запобіжні заходи:
  - зображена дитина досягла встановленого законом віку для сексуальної згоди та дала згоду на наявність таких матеріалів цій дорослій особі;
  - особа, яка володіє такими матеріалами, і дитина на зображеннях і/або відео є однакового віку та зрілості (наприклад встановивши максимально можливу різницю у віці між ними);
  - виробництво та володіння такими матеріалами не передбачають жодних зловживань;
- використовувати термін «матеріали сексуального насильства над дітьми» (CSAM) замість «дитячої порнографії» для матеріалів, що відображають акти сексуального насильства над дітьми та/або фокусування на геніталіях дитини;
- передбачити на правовому рівні чіткі алгоритми реагування на виявлені зображення та/або відео сексуального характеру, створені дитиною;
- розглянути можливість криміналізації злочину «грумінг» (домагання дітей для сексуальних цілей), навіть якщо це не призводить до особистої зустрічі або створення CSAM, тощо.
- щодо розслідування та притягнення до відповідальності:
- забезпечити створення спеціалізованого слідчого підрозділу;
- для фахівців, які працюють з випадками сексуального насильства щодо дітей, мають бути організовані тренінги з ІКТ, які сприяють сексуальним злочинам проти дітей.

Консультативна Місія Європейського Союзу (КМЄС)

КМЄС надає підтримку державним органам України у послідовному реформуванні сектору цивільної безпеки за допомогою стратегічних консультацій і практичної підтримки заходів з реформування згідно зі стандартами ЄС та міжнародними принципами належного врядування та дотримання прав людини.

Європол

- Для посилення реагування правоохоронних органів на кіберзлочинність в ЄС Європолом в 2013 році був створений **Європейський центр боротьби з кіберзлочинністю (ЕС3)**. На рівні операцій цей центр зосереджує увагу зокрема на сексуальній експлуатації дітей. ЕС3 також бере участь у віртуальній глобальній цільовій групі (VGT), яку було створено як пряму відповідь на зростання кількості правопорушників, які націлюються на дітей у всьому світі через соціальну взаємодію в інтернеті та виїжджають за кордон для вчинення контактного сексуального насильства. ЕС3 Європолу надає допомогу та сприяє обміну досвідом у боротьбі з розповсюдженням матеріалів про жорстоке поводження з дітьми в онлайн-середовищі, а також бореться з усіма формами злочинної поведінки в інтернеті проти дітей, як-от грумінг, непристойні матеріали, створені власними силами, сексуальне вимагання та прямі трансляції в інтернеті. Боротьба з розповсюдженням матеріалів про жорстоке поводження з дітьми включає запобігання та перехоплення їх, а також припинення їх поширення через однорангові мережі, а також через комерційні платформи. У зв'язку з цим ЕС3 бере участь у Європейській фінансовій коаліції проти комерційної сексуальної експлуатації дітей в інтернеті (EFC) – мережі, яка фінансується Європейською комісією і складається з правоохоронних органів, неурядових організацій, а також представників державного та приватного секторів.

Приклад. Європол підтримав міжнародне розслідування щодо десятків тисяч облікових записів, власники яких володіли та поширювали матеріали про сексуальне насильство над дітьми в інтернеті. В операції брали участь правоохоронні органи з Австралії, Австрії, Канади, Хорватії, Чехії, Греції, Угорщини, Словенії, Іспанії, Великобританії та США. Розслідування було розпочато в 2019 році після звіту від постачальника онлайн-послуг, який вказав, що велика кількість правопорушників використовували платформу для обміну особливо тривожними зображеннями жорстокого поводження з дітьми, включно із зображеннями садистських актів сексуального насильства над немовлятами та дітьми. На сьогодні міжнародне розслідування призвело до відкриття 836 справ на міжнародному рівні, арешту 46 осіб у Новій Зеландії, ідентифікації понад 100 підозрюваних у всьому ЄС та захисту 146 дітей у всьому світі. У двох випадках, в Австрії та Угорщині, підозрювані знущалися над власними дітьми, яким було шість і вісім років відповідно.

- У 2017 році Європолом була започаткована **ініціатива «Зупинити жорстоке поводження з дітьми – відстежити об'єкт»**. Правоохоронні органи в усьому світі тісно співпрацюють, щоб виявити якомога більше правопорушників і постраждалих осіб. Процес ідентифікації часто дуже складний, ідентифікація невеликих об'єктів на фоні зображень може призвести до прориву в розслідуванні. Європол завантажує об'єкти, які взято із зображення з матеріалами відверто сексуального характеру за участю дітей, на спеціальну вебсторінку та звертається до широкої громадськості з проханням перевірити, чи можуть вони розпізнати об'єкти, щоб відстежити їх походження (місце/країна). Громадяни можуть допомогти, натиснувши на об'єкт, який вони впізнають, і надати Європолу інформацію, яку вони мають про об'єкт. Це можна зробити анонімно. Після встановлення походження предмета Європол повідомляє компетентний правоохоронний орган країни для подальшого розслідування цієї інформації, що потенційно пришвидшить ідентифікацію як злочинця, так і постраждалої дитини.

STOPCHILDABUSE TRACE an OBJECT

Європол визначив ключові загрози у сфері сексуальної експлуатації дітей:

- одноранговi (P2P) мережі та анонімний доступ, такі як мережі Darknet (наприклад Tor). Ці комп'ютерні середовища залишаються основною платформою для доступу до матеріалів про насильство над дітьми та основним засобом некомерційного розповсюдження;
- пряма трансляція сексуального насильства над дітьми на замовлення;
- онлайн-домагання та сексуальне вимагання. Зростання кількості дітей і підлітків, які володіють смартфонами, супроводжується виробництвом непристойних матеріалів, створених власними силами. Такі матеріали, спочатку передані з невинним наміром, часто потрапляють до «колекціонерів», які часто продовжують експлуатувати постраждалу особу, зокрема через вимагання;
- нетворкінг та криміналістична обізнаність правопорушників. Правопорушники вчаться на помилках тих, кого затримали правоохоронці.

У травні 2021 року Європол ліквідував сайт сексуального насильства над дітьми в Darknet з понад 400 000 зареєстрованих користувачів.

Європейський Суд прав людини

У справі *Soderman v. Sweden (2013)* батько дівчини здійснював її приховану зйомку, коли вона була оголеною. Спроби звернення до державних органів не дали результату через прогали-

ни правового регулювання. ЄСПЛ визнав порушення права на приватність (права на фізичну цілісність), яке посилювалось тим, що дівчина була неповнолітньою, а події відбувалися у її кімнаті і здійснювались особою, яка користувалась особливою довірою.

У справі *K. U. v. Finland (2009 p.)* Суд встановив принцип, згідно з яким, хоча користувачі телекомунікацій та інтернет-послуг повинні мати гарантії поваги до свого приватного життя та свободи вираження поглядів, такі гарантії не можуть бути абсолютними та повинні інколи поступатися іншим правомірним імперативам, таким як запобігання правопорушенням, захист прав та свобод інших осіб. У цій справі невідомий розмістив оголошення сексуального характеру з ім'ям заявника, якому було 12 років, на сайті знайомств у інтернеті без його відома. Оголошення містило інформацію про нього, а також зазначалося, що він шукає інтимних стосунків із чоловіком. Оголошення також містило посилання на вебсторінку заявника з його зображенням і номером телефону. Дізнавшись про оголошення, заявник звернувся в поліцію, яка намагалася виявити особу, яку провайдер послуг відмовився назвати, вважаючи себе зв'язаним умовами конфіденційності; а суди через відсутність чітких положень закону відмовилися зобов'язати провайдера послуг розкрити інформацію про цю особу. Європейський суд з прав людини констатував порушення права на повагу до приватного життя, зокрема через потенційну загрозу фізичному і психічному добробуту молодої людини у такому вразливому віці.

У справі *Perrin v. the United Kingdom (2005)* заявник вимагав забезпечення його свободи вираження поглядів через можливість опублікування непристойних матеріалів на сайті. Однак Суд дійшов висновку, що потреба в охороні моралі та прав інших осіб, особливо дітей, виправдовує кримінальне покарання у вигляді засудження за публікацію у вільному доступі попереднього огляду вебсторінки, що не мала вікових обмежень і містила відверто непристойні зображення, які, ймовірно, могли бути знайдені молодими людьми без будь-яких перешкод.

Національний рівень

- **Міністерство цифрової трансформації України** поміж іншим приділяє увагу безпеці дітей в інтернеті, зокрема за допомогою розроблення соціальної реклами (https://youtu.be/OoZmLcQMa9s?si=88u6Bt6fr9zpQ0bf), участі в організації виставки «Сексуальне насильство над дітьми: онлайн-вимір».
- **Уповноважений Верховної Ради України з прав людини**, якому можна подати звернення з приводу порушення прав людини, зокрема і в кіберпросторі.
- **Міністерство внутрішніх справ України та Національна поліція України, до складу якої входить Департамент кіберполіції Національної поліції України**. У разі, якщо виявлено факт вчинення злочину за допомогою інтернету, можна подати електронне звернення, заповнивши форму зворотного зв'язку на сайті Департаменту кіберполіції Національної поліції України https://ticket.cyberpolice.gov.ua/. До завдань кіберполіції належать: реалізація державної політики у сфері протидії кіберзлочинності; завчасне інформування населення про появу нових кіберзлочинців; впровадження програмних засобів для систематизації кіберінцидентів; реагування на запити зарубіжних партнерів тощо. Особливу увагу Департамент кіберполіції приділяє питанням захисту дітей в кіберпросторі. Так на сайті цього департаменту містяться рекомендації з питань безпеки дітей в інтернеті: https://cyberpolice.gov.ua/article/pravyla-dytyachoyi-bezpeky-v-interneti--porady-kiberpolicziyi-8250/.
- **Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA** функціонує в складі Державної служби спеціального зв'язку та захисту інформації України.
- **Міністерство освіти і науки України** – на сайті міністерства є матеріали, спрямовані на підвищення обізнаності учасників освітнього процесу з питань безпеки в інтернеті,

методичні рекомендації для проведення занять з дітьми, посилання на громадські організації та їх ресурси, присвячені цим питанням тощо. Міністерство освіти і науки України періодично звертає увагу закладів освіти на важливість проведення профілактики сексуального насильства, щодо дітей, зокрема в кіберпросторі. Так, наприклад, міністерством було надіслано в заклади освіти листи «Щодо захисту дітей від сексуальної експлуатації та сексуального насильства» від 10.11.2022 №4/3250-22, «Щодо запобігання та протидії сексуальному насильству, пов'язаному зі збройною агресією російської федерації та території України» від 22 червня 2022 року №1/6885-22, тощо.

- **Суди** – розглядають звернення у разі порушення прав дитини в інтернеті. До суду може звернутись людина самостійно, якщо їй виповнилось 14 років, у молодшому віці за захистом прав дитини можуть звернутись до суду законні представники дитини.
- **Інтернет-провайдери, адміністратори соціальних мереж і сайтів** розглядають скарги щодо неналежного (шкідливого) контенту, вживають заходів щодо його блокування.
- **«Гарячі лінії» (телефони довіри).**

В Україні функціонує **Національна «гаряча лінія» для дітей та молоді** за номером 116 111 при ГО «Ла Страда-Україна», а також **Урядова «гаряча лінія»**, яка також уповноважена консультувати з питань насильства стосовно дітей, за телефоном 15 47 та 15 45 (на IVR кнопка 3) – «гаряча лінія» з питань безпеки дітей в інтернеті.

- **Міністерство юстиції України**, яке координує діяльність Міжвідомчої координаційної ради з питань правосуддя щодо неповнолітніх.
- **Nadiyno** – онлайн-платформа для екстреної допомоги з цифрової безпеки (https://nadiyno.org/about-us/).

Інформаційними партнерами платформи стали Міністерство цифрової трансформації України та національний проєкт Дія. Цифрова освіта. Онлайн-платформа Nadiyno допоможе: посилити власну онлайн-безпеку та захистити себе від онлайн-загроз, підвищити цифрову грамотність громадян, надати поради із захисту персональних даних і пристроїв, підтримку від операторів «гарячої лінії» та інших фахівців з цифрової безпеки.

- **Проєкт #stop_sextинг** започатковано за підтримки компанії Київстар, у партнерстві з Міністерством цифрової трансформації та Уповноваженим Президента України з прав дитини. В межах цього проєкту функціонує чат-бот, розроблені рекомендації батькам та вчителям, а також розроблені та розміщені на офіційному сайті проєкту матеріали з питань захисту дітей від сексуального насильства та експлуатації в інтернеті. Проєкт має інтернет-портал повідомлень про матеріали, що зображують сексуальне насильство над дітьми за адресою: https://stop-sexting.in.ua/send/. Портал працює як лінія звітування: знаходячись в Україні, будь-яка людина може повідомити про контент сексуального насильства над дітьми, який вона виявила в інтернеті. Всі повідомлення, які надсилаються через цей портал, обробляються **громадською організацією Internet Watch Foundation (IWF)** у Великобританії. IWF, видаляючи зображення сексуального насильства над дітьми, керується такими визначеннями: зображення сексуального насильства над дітьми – це зображення, на яких видно дитячі статеві органі або анус, або демонструються такі акти:

- вчинення статевого акту з дитиною або в присутності дітей;
- вчинення сексуальних дій з тваринами в присутності дитини;
- вчинення сексуальних дій (з проникненням або без) щодо дитини;
- мастурбація дитиною, або мастурбація дорослого в присутності дитини.

Такі зображення можуть набувати форм фото, відео, а також бути згенеровані комп'ютером. Зображення, які розміщені у відкритому інтернеті, можуть бути видалені. Зображення, що не містять ознак сексуального насильства над дітьми (що описані вище), а також зображення, що передані через канали з наскрізним шифруванням (наприклад через месенджери, такі як Телеграм або Вотсап), не підлягають видаленню через цей портал.

- **Інформаційно-ресурсний центр «Дитинство без насильства»** (https://rescentre.org.ua/bezpeka-ditei-v-interneti) створений в межах проєкту «Дитинство без насильства – покращення системи захисту дітей у Східній Європі», який впровадив Український фонд «Благополуччя дітей» за сприяння OAK Foundation. На цьому ресурсі розміщуються та оновлюються матеріали і з питань безпеки дітей в інтернеті.

Всеукраїнський громадський центр «Волонтер» спільно з Управлінням протидії кіберзлочинам у м. Києві Департаменту кіберполіції Національної поліції України за підтримки Представництва Дитячого фонду ООН (ЮНІСЕФ) в Україні розробив безоплатний онлайн-курс для молодих людей, які хочуть знати, як захистити себе та свою інформацію в кіберпросторі (https://cyber.volunteer.kyiv.ua/#/). Також на сайті цієї організації містяться публікації, присвячені питанням захисту прав дітей.

Додаток 1.9.2.2

Права дитини в цифровому середовищі

Доступ до цифрового середовища

Доступ та використання цифрового середовища є важливими для реалізації прав і основних свобод людини, освіти, участі та підтримки сімейних і соціальних відносин. Державам слід вживати відповідних заходів для забезпечення того, щоб усі діти мали доступний та надійний доступ до пристроїв, підключення, послуг і контенту, які спеціально призначені для дітей. Наскільки це можливо, у спеціальних публічних просторах держави варто вживати заходів для безоплатного доступу до цифрового середовища.

Державам слід забезпечити доступ до цифрового середовища в навчальних та інших установах для дітей. Особливі заходи мають бути вжиті щодо дітей у вразливих ситуаціях, зокрема це діти, які живуть у системі альтернативного догляду, діти, які позбавлені волі чи чиї батьки позбавлені волі, діти вулиці й діти в сільських громадах. Зокрема, державам слід вимагати від постачальників інтернет-послуг забезпечити доступність їх послуг для дітей з інвалідністю. Підключення та доступ до пристроїв, послуг і контенту повинні супроводжуватися відповідними заходами освіти та грамотності.

Держави повинні забезпечити, щоб положення та умови, пов'язані з використанням пристрою, який може підключатися до інтернету або застосовуватися для надання онлайн-послуг або контенту, були доступними, справедливими, прозорими, зрозумілими для дитини й чітко сформульованими прийнятною для дітей та відповідною для їхнього віку мовою.

Свобода слова та вираження думок

Цифрове середовище має значний потенціал для підтримки реалізації права дітей на свободу вираження думок, зокрема на право шукати, отримувати й поширювати інформацію та різні ідеї.

До дітей, як до творців і розповсюджувачів інформації в цифровому середовищі, повинна бути донесена державами, особливо через освітні програми, інформація про те, як здійснювати своє право на свободу вираження думок у цифровому середовищі, поважаючи права і гідність інших людей, інших дітей. Зокрема, такі програми повинні стосуватися таких аспектів, як дотримання прав інтелектуальної власності або заборона підбурювання до ненависті й насильства.

Право на свободу вираження думок – не абсолютне право. Це означає, що право дітей на свободу вираження думок та інформації може бути обмеженим для захисту їхніх інтересів (наприклад обмеження доступу до матеріалів, які вважаються шкідливими для них за допомогою інтернет-фільтрів або систем перевірки віку), або для захисту інтересів інших. Держави повинні вживати заходів, щоб діти були поінформовані про наявні обмеження, такі як фільтрація контенту, у спосіб, відповідний їхнім динамічним можливостям, і гарантувати, що дітям надано керівництво щодо відповідних засобів правового захисту, зокрема про те, як і кому подавати скаргу, повідомляти про зловживання або просити про допомогу й консультування.

Важливо!

- Діти повинні знати про обмеження.
- Діти повинні бути поінформовані про наслідки їхньої поведінки в інтернеті щодо їхніх однолітків.
- Діти повинні мати засіб захисту для усунення обмежень, які вони вважають незаконними (наприклад подати скаргу щодо невиправданого видалення зображення).

Право на участь та свободу об'єднань

Цифрове середовище забезпечує особливі можливості для права дитини бути залученою, брати участь у грі та у мирних зібраннях і об'єднаннях, зокрема через онлайн-спілкування, ігри, встановлення контактів та участі у розвагах.

Державам слід підтримувати розроблення онлайн громадських і соціальних платформ для сприяння їхній участі та здійсненню права на зібрання та об'єднання, посилюючи їхню здатність до демократичного громадянства та політичної обізнаності.

Державам слід вжити заходів для захисту дітей, які використовують своє право на мирні зібрання та об'єднання в цифровому середовищі, від моніторингу та нагляду, незалежно від того, чи здійснюють їх органи державної влади безпосередньо чи у співпраці з суб'єктами приватного сектору.

Конфіденційність та захист даних

Діти мають право на приватне та сімейне життя в цифровому середовищі, що включає захист їхніх персональних даних і повагу конфіденційності їхньої кореспонденції та приватних повідомлень. Держави повинні поважати, захищати й виконувати право дитини на недоторканність приватного життя і захист персональних даних. Держава повинна забезпечити, щоб відповідні зацікавлені сторони, зокрема ті, хто обробляє персональні дані, а також однолітки дитини, батьки чи законні представники, були обізнані та поважали право дитини на конфіденційність і захист даних. Державам та іншим зацікавленим сторонам слід забезпечити, щоб діти знали про те, як реалізовувати своє право на приватне життя і захист даних з урахуванням їхнього віку та зрілості.

Визнаючи, що персональні дані можуть бути оброблені на користь дітей, держави повинні вживати заходів щодо забезпечення того, щоб персональні дані дітей були оброблені законно й безпечно, для конкретних цілей та з вільною, очевидною та однозначною згодою дітей та/або їхніх батьків, законних представників або відповідно до іншої законної мети, встановленої законодавчо. Державам слід забезпечити, щоб діти та/або їхні батьки, законні представники мали право скасувати свою згоду на обробку особистих даних, мати доступ до своїх особистих даних, а також мати змогу виправити або знищити їх, особливо коли обробка є незаконною, або коли це компрометує їхню гідність, безпеку та конфіденційність.

Державам слід забезпечити надання доступної, значущої й зручної за віком інформації для дітей про засоби захисту конфіденційності, налаштування та засоби правового захисту. Діти та/або їх батьки, законні представники мають бути поінформовані про те, як обробляються їхні дані. Це повинно включати інформацію, наприклад про те, як збираються, зберігаються, використовуються та розкриваються дані, про доступ до їхніх даних, про виправлення чи знищення цих даних.

Профілювання дітей, тобто будь-яка форма автоматизованої обробки персональних даних, яка полягає у застосуванні «профілю» до дитини, зокрема для аналізу її особистих уподобань, поведінки та ставлення, має бути заборонене законом. Держави не повинні забороняти анонімність, псевдонімічність або використання технологій шифрування для дітей.

Право на освіту

Державам слід активно інвестувати і просувати можливості, які пропонує цифрове середовище для реалізації права дітей на освіту.

Цифрова грамотність. Державам слід сприяти розвитку цифрової грамотності, зокрема медіа- та інформаційну грамотність й освіту в галузі цифрового громадянства, щоб гаран-

тувати, що діти мають знання, щоб розумно долучатися до цифрового середовища, і стійкість до пов'язаних ризиків. Освіта у сфері цифрової грамотності повинна бути включена в основний навчальний план із ранніх років, з урахуванням динамічних можливостей дітей. На підтримку широкого кола прав дитини освіта у сфері цифрової грамотності повинна включати технічні або функціональні компетенції для використання широкого кола онлайн-інструментів і ресурсів, а також навичок, пов'язаних зі створенням контенту, і критичним розумінням цифрового середовища, його можливостей та ризиків. Державам слід також заохочувати і підтримувати цифрову освіту батьків або опікунів. Держави та інші відповідні зацікавлені сторони через систему освіти та культури повинні докладати особливі зусилля для підтримки і просування цифрової грамотності дітей, які мають мало доступу до цифрових технологій або не мають доступу до них за соціально-географічними або соціально-економічними міркуваннями, а також іноді з міркувань місця проживання, а також дітей, котрі мають доступ до цифрових технологій, але не використовують їх, які не мають навичок використання або недостатньо використовують цифрові технології з причин вразливості, зокрема для дітей з інвалідністю.

Освітні програми та ресурси. Державам слід забезпечити наявність достатніх високоякісних освітніх ресурсів, фізичних пристроїв та інфраструктур, що полегшують діяльність дітей у цифровому середовищі та підтримують формальну й неформальну освіту дітей. Вони можуть бути розроблені та розповсюджені у співпраці з іншими зацікавленими сторонами. Слід розвивати і зміцнювати ініціативи та програми з підвищення освіченості й підвищення обізнаності, а також програми для дітей, батьків та законних представників, а також педагогів і волонтерів, які працюють з дітьми, із залученням дітей. Такі програми повинні включати знання про запобіжні заходи, про права та обов'язки в цифровому середовищі, про ідентифікацію й повідомлення про порушення, засоби захисту та відшкодування шкоди. Зокрема, такі програми повинні навчити дітей розуміти, залежно від їхнього віку, що означає надання згоди, повага до прав, використовувати наявні інструменти, щоб захищати й реалізовувати свої права в цифровому середовищі. Крім того, вони повинні дозволяти дітям розпізнавати і боротися з потенційно шкідливим контентом (таким як насильство та нанесення собі ушкоджень, порнографія, матеріали про сексуальне насильство над дітьми, дискримінація та расизм, мова ворожнечі) і поведінкою (наприклад домагання до дітей із сексуальними цілями чи «грумінг», залякування чи переслідування, незаконна обробка персональних даних, порушення прав інтелектуальної власності) та можливі наслідки того, як інформація про дітей або така, що розповсюджується серед дітей, може бути поширена іншими особами. Формальні і неформальні навчальні та культурні установи (зокрема архіви, бібліотеки, музеї, організації, що працюють з дітьми і молоддю, та інші навчальні заклади) слід підтримувати і заохочувати до розроблення й надання різноманітних цифрових та інтерактивних навчальних ресурсів.

Право на захист та безпеку

Заходи щодо запобігання ризикам у цифровому середовищі. Пам'ятаючи про швидкість, з якою можуть розвиватись нові технології, держави повинні вживати запобіжних заходів, зокрема регулярно оцінюючи будь-які ризики і шкоду, які вони можуть становити для здоров'я дітей. Коли держави заохочують розроблення, виробництво та регулярне оновлення підприємствами програм батьківського контролю для зменшення ризиків для дітей в цифровому середовищі, вони повинні забезпечити розроблення цих заходів контролю, зважаючи на динамічні можливості дітей і те, що вони не мають посилювати дискримінаційне ставлення, порушувати право дітей на недоторканність приватного життя або позбавляти дітей права на інформацію відповідно до їхнього віку та зрілості.

Заходи захисту та підвищення обізнаності. Держави повинні: 1) вимагати застосування

ефективних систем вікової перевірки для забезпечення захисту дітей від продуктів, послуг і контенту в цифровому середовищі, які юридично обмежуються з урахуванням конкретних вікових категорій; 2) вживати заходів для забезпечення захисту дітей від комерційної експлуатації в цифровому середовищі, зокрема вплив реклами та маркетингу, що є невідповідними їхньому віку; 3) співпрацювати із медіа з належною повагою до свободи медіа, з навчальними закладами та іншими відповідними зацікавленими сторонами для розроблення програм підвищення обізнаності, спрямованих на захист дітей від шкідливого контенту, а також запобігання їхньої участі в незаконній онлайн-діяльності; 4) вживати заходів, щоб заохотити підприємства та інші відповідні зацікавлені сторони розробляти і впроваджувати політики, спрямовані на боротьбу із залякуванням в інтернеті, утисками та підбурюванням до ненависті й насильства в цифровому середовищі.

Заходи, що стосуються матеріалів про сексуальне насильство над дітьми. Політика стосовно матеріалів, що стосуються сексуального насильства над дітьми, має бути спрямована на підтримку постраждалих, водночас першочергову увагу слід приділяти ідентифікації, виявленню, захисту та наданню допомоги дітям, зображеним у таких матеріалах. Державам слід: 1) постійно відстежувати, чи перебувають у їх юрисдикції матеріали про сексуальне насильство над дітьми, і вимагати від правоохоронних органів встановлення баз даних «хеш» з метою прискорення дій щодо виявлення та знаходження дітей, які зазнають сексуальної експлуатації або насильства, та затримання винних; 2) співпрацювати з підприємствами з метою надання ними допомоги правоохоронним органам, зокрема з питань належної технічної підтримки та обладнання, для прискорення виявлення осіб, які вчинили злочини проти дітей, і збору доказів, необхідних для кримінального провадження; 3) вимагати від відповідних підприємств застосовувати хеш-списки, аби забезпечити, щоб їх мережі не використовувалися для зберігання й розповсюдження зображень, пов'язаних із сексуальним насильством над дітьми; 4) вимагати, щоб підприємства й інші відповідні зацікавлені сторони негайно вжили всіх необхідних заходів для забезпечення доступності метаданих стосовно будь-яких матеріалів про сексуальну експлуатацію і насильство над дітьми, які є на локальних серверах, надавати їх правоохоронним органам, видаляти ці матеріали та, до їх видалення, обмежувати доступ до таких матеріалів, розміщених на серверах поза межами своєї юрисдикції.

Засоби правового захисту. Справжнє та ефективне здійснення прав дітей вимагає наявності засобів захисту в разі порушення їхніх прав, зокрема в цифровому середовищі. Це передбачає забезпечення наявних, відомих, доступних, бюджетних і дружніх для дітей способів, за допомогою яких діти, а також їхні батьки або законні представники можуть подавати скарги та шукати захисту. Ефективні засоби правового захисту можуть включати, залежно від порушеного питання: запит, пояснення, відповідь, виправлення, провадження, негайне вилучення незаконного контенту, вибачення, відновлення порушеного права, повторне підключення та компенсацію. Дітям слід надавати інформацію й поради щодо доступних засобів так, щоб вони були адаптовані до їхнього віку і зрілості, мовою, яку вони можуть зрозуміти, і яка є чутливою до статі та культури.

Процедури розгляду скарг, дружні до дітей. Для того щоб процедура розгляду скарг була дружня до дитини, вона повинна містити такі елементи: 1) бути безпечною та доступною; 2) діти отримують інформацію та допомогу в процесі подання скарг; 3) інформація надається у формах, що відповідають віку та рівню розвитку дітей, зокрема у вигляді листівок, брошур, плакатів, вебсайтів, які розповсюджуються там, де діти можуть її знайти; 4) відповідь на скарги надсилається безпосередньо дітям протягом розумного періоду способом, що відповідає їхньому вікові та рівню розвитку.

Додаток 1.9.2.3

Основні принципи діяльності суб'єктів захисту прав дітей в кіберпросторі

Забезпечення найкращих інтересів дитини. Під час ухвалення будь-яких рішень, що стосуються дітей у цифровому середовищі, добробут дитини має бути на першому місці. Оцінюючи найкращі інтереси дитини, суб'єкти повинні докласти зусиль, щоб збалансувати право дитини на захист з іншими правами, зокрема правом на свободу вираження поглядів та інформації, а також правом на участь.

Врахування динамічних можливостей дитини. Можливості дитини розвиваються поступово від народження до 18 років. Крім того, окремі діти досягають різних рівнів зрілості в різному віці. Суб'єкти повинні враховувати динамічні можливості дітей, зокрема дітей з інвалідністю або в уразливих ситуаціях. Це також означає, що політики, ухвалені для реалізації прав підлітків, можуть суттєво відрізнятися від тих, що застосовуються для молодших дітей, адже підлітки та малюки мають різні здібності та потреби.

Недопущення дискримінації. Права дитини в цифровому середовищі гарантуються всім дітям без будь-якої дискримінації., незалежно від віку, раси, кольору шкіри, статі, мови, релігії, політичних або інших переконань дитини чи її батьків або законних представників, національного, етнічного або соціального походження, майнового стану, інвалідності, народження або іншого статусу. Водночас для дітей в уразливих ситуаціях можуть бути необхідні спеціальні заходи.

Участі. Діти мають право вільно висловлюватися з усіх питань, що впливають на них, а їхні погляди повинні бути належним чином враховані відповідно до їхнього віку та зрілості. Суб'єкти забезпечення та захисту прав дитини повинні надавати дітям інформацію про їхні права у зрозумілий спосіб, що відповідає їхньому віку та рівню розвитку. Діти повинні бути також поінформовані про послуги, а також процедури подання скарг, поновлення прав або відшкодування завданої шкоди, якщо їхні права порушуються. Така інформація повинна бути також доступна їхнім батькам або законним представникам, щоб вони могли підтримувати дітей у реалізації їхніх прав. Держави та інші відповідні зацікавлені сторони повинні активно залучати дітей до участі в розробленні, впровадженні та оцінці законодавства, політик, механізмів, практик, технологій і ресурсів, які спрямовані на захист та реалізацію прав дитини в цифровому середовищі.

Залучення всіх зацікавлених сторін. Суб'єкти зобов'язані поважати, захищати й забезпечувати права кожної дитини в межах своїх повноважень, а також залучати всі відповідні зацікавлені сторони, зокрема органи та заклади освіти, соціальні служби, установи та підприємства, громадські організації, а також самих дітей та їхніх батьків, законних представників або будь-яку іншу особу, яка піклується про дитину, для ефективного виконання цих зобов'язань.

ТЕМА 1.10. Відповідальність за вчинення протиправних дій щодо дітей та дітьми в мережі інтернет

Заняття 1.10.1. Відповідальність за вчинення протиправних дій щодо дітей в мережі інтернет

Мета: надати учасникам інформацію про особливості відповідальності за вчинення протиправних дій щодо дітей в мережі інтернет та відпрацювати вміння кваліфікувати відповідні випадки.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Асоціації, пов'язані із вчиненням протиправних дій щодо дітей в мережі інтернет	Обговорення	15 хв	Фліпчарт та аркуші для фліпчарту, маркери або мультимедійне обладнання
2.	Відповідальність за вчинення протиправних дій сексуального характеру щодо дітей в мережі інтернет	Робота в групах	40 хв	Додаток 1.10.1.1, фліпчарт та аркуші для фліпчарту, маркери
3.	Практика ЄСПЛ	Обговорення	15 хв	Додаток 1.10.1.2, мультимедійне обладнання
4.	Відповідальність за вчинення протиправних дій щодо дітей в мережі інтернет	Робота в групах	20 хв	Додаток 1.10.1.3, фліпчарт та аркуші для фліпчарту, маркери

До уваги тренера/тренерки!

Слід врахувати, що ця тема передбачає попереднє засвоєння учасниками тем, присвячених питанням онлайн-ризиків та загроз для дітей в мережі інтернет, а також правовим засадам забезпечення та захисту прав дітей в мережі інтернет.

Більш доцільно це заняття проводити в межах курсів підвищення кваліфікації та службової підготовки або для випускних курсів здобувачів вищої освіти.

ХІД ЗАНЯТТЯ

1. Обговорення «Асоціації, пов'язані із вчиненням протиправних дій щодо дітей в мережі інтернет»

Мета: оцінити рівень інформованості учасників, актуалізувати основні поняття щодо протиправних дій щодо дітей в мережі інтернет.

Час: 15 хв.

Необхідні матеріали: фліпчарт, аркуші для фліпчарту, маркери або мультимедійне обладнання.

Хід проведення:

Тренер/тренерка на аркуші фліпчарту пише словосполучення «*Протиправні дії щодо дітей в мережі інтернет*» і пропонує учасникам озвучити асоціації, які виникають у них щодо цього словосполучення: «*Сьогодні ми з вами говоримо про відповідальність за вчинення протиправних дій щодо дітей в мережі інтернет, і я пропоную вам навести асоціації, пов'язані з цим словосполученням*».

Тренер/тренерка занотовує всі відповіді, які надають учасники.

До уваги тренера/тренерки!

Якщо дозволяє технічне обладнання, можна зробити опитування за допомогою програми «Mentimetr» у вигляді хмаринки думок.

Підсумовуючи, тренер/тренерка зазначає: «*За протиправні діяння стосовно дітей винні несуть покарання відповідно до законодавства України незалежно від місця вчинення правопорушення – онлайн чи офлайн. Те, що в нормах права, які передбачають відповідальність за вчинення правопорушення, не зазначається безпосередньо спосіб їх вчинення за допомогою інформаційно-комунікаційних технологій, не означає, що у такому разі відповідальність не наставатиме.*

Внаслідок протиправних діянь щодо дітей, вчинених з використанням інформаційно-комунікаційних технологій, настають різні види юридичної відповідальності.

*Так **до адміністративної відповідальності** можливе притягнення за вчинення таких правопорушень:*

- *поширення неправдивих чуток (ст. 173-1 КУпАП);*
- *вчинення домашнього насильства (ст. 173-2 КУпАП);*
- *булінг (цькування) учасника освітнього процесу (ст. 173-4 КУпАП).*

*Настання **кримінальної відповідальності** тягне вчинення зокрема таких правопорушень:*

- *вчинення домашнього насильства (ст. 126-1 ККУ);*
- *торгівля людьми (ст. 149 ККУ);*
- *зґвалтування (ст. 152 ККУ);*
- *сексуальне насильство (ст. 153 ККУ);*
- *примушування до вступу в статевий зв'язок (ст. 154 ККУ);*
- *вчинення дій сексуального характеру з особою, яка не досягла шістнадцятирічного віку (ст. 155);*
- *розбещення (ст. 156 ККУ);*
- *домагання дитини для сексуальних цілей (ст. 156-1 ККУ);*
- *порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163 ККУ);*
- *порушення недоторканності приватного життя (ст. 182 ККУ);*
- *ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 300 ККУ);*
- *ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301 ККУ);* одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження (ст.301-1 ККУ);

- проведення видовищного заходу сексуального характеру за участю неповнолітньої особи (ст. 301-2 ККУ);
- несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 ККУ) тощо.

Перелік правопорушень, безумовно, не є вичерпним.

Окремий фокус уваги слід звернути на можливе настання відповідальності батьків (опікунів, піклувальників) потерпілої від таких правопорушень дитини відповідно до ст. 166 ККУ «Злісне невиконання обов'язків по догляду за дитиною або за особою, щодо якої встановлена опіка чи піклування» у разі, якщо правопорушення щодо дитини спричинило тяжкі наслідки і було вчинено в результаті їхнього злісного невиконання обов'язків по догляду за дитиною.

Крім відповідальності фізичних осіб за вчинення протиправних дій стосовно дітей в інтернеті, в Україні передбачена також відповідальність юридичних осіб. Так Закон України «Про медіа» передбачає настання ***відповідальності медіа*** *у вигляді фінансових санкцій за:*

- поширення інформації, що може завдати шкоди фізичному, психічному або моральному розвитку дітей;
- поширення порнографічних матеріалів, а також матеріалів, що заохочують сексуальну експлуатацію та насильство над дітьми, демонструють їхні статеві відносини, використовують образ дітей (його візуальний запис) у видовищних заходах сексуального чи еротичного характеру;
- порушення вимог щодо нерозголошення інформації про дитину без письмової згоди хоча б одного з батьків або законних представників, за винятком випадків, якщо це здійснюється в найкращих інтересах дитини. До інформації про дитину, на яку розповсюджується така вимога щодо нерозголошення суб'єктами у сфері медіа, належить:
  - *фото дитини, яка зазнала фізичного чи сексуального насилля;*
  - *будь-яка інформація, яка:*
    - *може сприяти ідентифікації дитини, яка задіяна у провадженні у справах про адміністративні правопорушення, в кримінальному провадженні у будь-якому статусі або стосовно якої є інформація про здійснення нею правопорушення;*
    - *стосується факту самогубства дитини, водночас ідентифікує її особу.*

Крім адміністративної та кримінальної відповідальності за вчинення протиправних дій стосовно дітей в інтернеті, може наставати ***цивільно-правова відповідальність,*** *зокрема у вигляді відшкодування потерпілій стороні завданої моральної шкоди».*

До уваги тренера/тренерки!

Доцільно висвітлити інформацію, зазначену вище, у вигляді презентації.

Запитання для обговорення:

- *Які ще протиправні діяння, за які настає відповідальність, можуть бути вчинені щодо дітей в інтернеті?*
- *З якими із окреслених протиправних діянь ви зустрічались під час практичної діяльності або в особистому житті?*

2. Робота в групах «Відповідальність за вчинення протиправних дій сексуального характеру щодо дітей в мережі інтернет»

Мета: систематизувати знання учасників щодо особливостей відповідальності за вчинення протиправних дій сексуального характеру щодо дітей в мережі інтернет та проаналізувати відповідність національного законодавства з цих питань європейським стандартам.

Час: 40 хв.

Необхідні матеріали: Додаток 1.10.1.1, мультимедійне обладнання.

Хід проведення:

Тренер/тренерка зазначає: «*Боротьба з протиправними діями щодо дітей в інтернеті має певні переваги, порівнюючи з офлайн-правопорушеннями, зокрема у зв'язку з можливістю ідентифікувати правопорушника в іншій країні. Однак має й недоліки, зокрема технологічні труднощі, з якими стикаються правоохоронці, а також відмінності в законодавстві різних країн. Протиправні дії сексуального характеру щодо дітей, зокрема вчинені в інтернеті або за допомогою інтернету, є одним із грубих порушень прав дитини та мають тягнути невідворотне настання відповідальності винних осіб. Одним із ключових документів, в якому містяться стандарти відповідальності за протиправні дії сексуального характеру щодо дітей, зокрема в мережі інтернет, є Лансаротська конвенція. Наразі в нас є нагода проаналізувати, наскільки її положення відображені в нашому національному законодавстві*».

Тренер/тренерка об'єднує учасників у чотири групи та надає кожній із них роздатковий матеріал із Додатка 1.10.1.1:

Група 1 – ст. 20 Лансаротської конвенції та роз'яснення до неї, а також ст. 301-1 Кримінального кодексу України;

група 2 – ст. 21 Лансаротської конвенції, а також ст. 301-2 Кримінального кодексу України;

група 3 – ст. 22 Лансаротської конвенції та роз'яснення до неї, а також ст. 156 Кримінального кодексу України;

група 4 – ст. 23 Лансаротської конвенції та роз'яснення до неї, а також ст. 156-1 Кримінального кодексу України.

Учасники в групах протягом десяти хвилин мають проаналізувати отримані статті, стисло викласти їх зміст на аркуші фліпчарту та визначити, чи відповідає в цьому випадку національне законодавство європейським стандартам. Під час роботи в групах учасники зокрема можуть використовувати науково-практичні коментарі цих норм.

Після закінчення часу на роботу в групах учасники протягом п'яти хвилин презентують свої напрацювання. Тренер/тренерка та представники інших груп можуть доповнювати презентації груп.

До уваги тренера/тренерки!

Під час підготовки до заняття слід проаналізувати чинність та актуальність матеріалу, що міститься у Додатку 1.10.1.1.

Якщо рівень підготовки учасників недостатній для самостійного аналізу документів, тренеру/тренерці доцільно самостійно презентувати цей матеріал, завчасно підготувавши презентацію з використанням інформації, що міститься у Додатку 1.10.1.1.

Крім того, презентацію можна доповнити актуальними на час проведення заняття статистичними даними.

Підсумовуючи, тренер/тренерка зазначає: «*Ця категорія правопорушень потребує високого професіоналізму представників правоохоронних органів з метою притягнення до відповідальності винних осіб, а також постійного* ***моніторингу змін до чинного законодавства***.

- *Так в 2021 році були внесені зміни та доповнення до Кримінального кодексу України з метою приведення національного законодавства до положень Лансаротської конвенції, яка є одним із ключових документів, що встановлює стандарти відповідальності за протиправні дії сексуального характеру щодо дітей, також в мережі інтернет. Зокрема було криміналізовано: 1) домагання дитини в сексуальних цілях, зокрема з використанням інформаційно-телекомунікаційних систем або технологій (ст. 156-1 ККУ); 2) одержання доступу до дитячої порнографії (ст. 301-1 ККУ); 3) проведення видовищного заходу сексуального характеру, зокрема з використанням інформаційно-телекомунікаційних систем або технологій, за участю неповнолітньої особи (ст. 301-2 ККУ). Невелика кількість облікованих справ за цими статтями не є свідченням того, що такі правопорушення не вчиняються. Це пояснюється значною латентністю таких правопорушень, необізнаністю населення про те, що такі діяння є кримінально караними, складністю їх виявлення, розслідування, доведення тощо.*
- *З 19 грудня 2024 року наберуть чинності зміни до Кодексу України про адміністративні правопорушення, передбачені Законом України від 22 травня 2024 року №3733-IX, серед яких основними в контексті нашої теми є:*

– *ст.173-2 КУпАП передбачатиме відповідальність винятково за вчинення домашнього насильства, водночас за вчинення домашнього насильства щодо неповнолітньої або малолітньої особи передбачена відповідальність за окремою частиною (ч. 2) цієї статті;*

– *відповідальність за вчинення насильства за ознакою статті буде передбачена ст. 173-6 КУпАП;*

– *відповідальність за невиконання термінового заборонного припису буде передбачена ст. 173-8 КУпАП;*

– *встановлено відповідальність за сексуальні домагання (ст. 173-7 КУпАП), тобто умисне вчинення проти бажання особи образливих, принизливих дій сексуального характеру, виражених вербально або невербально (слова, жести, рухи тіла), зокрема з використанням електронних комунікацій.*

Всі окреслені правопорушення можуть бути вчинені також в мережі інтернет, хоча безпосередньо вказівка на можливе використання електронних комунікацій міститься лише щодо сексуальних домагань в ст.173-7 КУпАП. Наприклад, невиконання термінового заборонного припису може проявлятися у вигляді порушення обмеження спілкування з постраждалою від домашнього насильства дитиною, водночас таке спілкування може відбуватись через надсилання повідомлень у месенджерах, електронних листах, коментарях у соціальних мережах тощо. Те саме стосується і випадків домашнього насильства, коли погрози, залякування та інші протиправні діяння вчиняються щодо дитини із використанням електронних комунікацій.

- *З 06 жовтня 2024 року набирають чинності зміни до деяких законів України щодо запобігання насильству та унеможливлення жорстокого поводження з дітьми, передбачені Законом України від 06 червня 2024 року №3792-IX, серед яких:*

– *доповнення поняття жорстокого поводження з дитиною в Законі України «Про охорону дитинства» такими формами насильства, як насильство за ознакою статі, булінг (цькування), мобінг (цькування);*

– *закріплення у Законі України «Про охорону дитинства» визначення булінгу (цькування) як психологічного, фізичного, економічного чи сексуального насильства, тобто будь-яких умисних дій, що вчиняються всупереч волі, бажання, без згоди потерпілої особи, зокрема із застосуванням засобів електронних комунікацій, і порушують її права, свободи, законні інтереси та/або перешкоджають виконанню нею визначених законодавством обов'язків, що систематично вчиняються стосовно дитини або дитиною стосовно іншої особи, які є учасниками одного колективу. Водночас колектив – це група осіб, які об'єднані (організовані) відповідно до законодавства з метою навчання, тренування, творчості, оздоровлення, відпочинку, лікування тощо, та не перебувають між собою у трудових відносинах. Тобто фактично булінгом (цькуванням) будуть вважатися не лише діяння між учасниками освітнього процесу, розширюється сфера застосування цього поняття».*

Запитання для обговорення:

– *Чи вважаєте ви, що національне законодавство в питаннях відповідальності за правопорушення щодо дітей в інтернеті відповідає Лансаротській конвенції?*

– *Чи вважаєте ви ефективним національне законодавство в контексті відповідальності за вчинення протиправних дій щодо дітей в мережі інтернет? Якщо ні, то чому, що саме потребує удосконалення?*

3. Обговорення «Практика ЄСПЛ»

Мета: надати учасникам інформацію про наявні рішення ЄСПЛ стосовно протиправних дій щодо дітей в мережі інтернет та сформувати усвідомлення учасниками ролі ЄСПЛ у захисті порушених прав дитини в мережі інтернет.

Час: 15 хв.

Необхідні матеріали: Додаток 1.10.1.2, фліпчарт та аркуші для фліпчарту, маркери.

Хід проведення:

Тренер/тренерка презентує по черзі наявні рішення ЄСПЛ з питань протиправних дій щодо дітей в мережі інтернет, використовуючи Додаток 1.10.1.2, не зазначаючи висновок суду. Після короткого розкриття обставин кожної справи тренер/тренерка звертається до учасників із запитанням: «*Як ви вважаєте, які права порушено в цій справі (якщо порушено); хто порушник та яке рішення прийняв ЄСПЛ?*».

Після висловлювання учасниками своїх думок, тренер/тренерка презентує правильну відповідь.

До уваги тренера/тренерки!

Під час підготовки до заняття доцільно промоніторити наявність нових рішень ЄСПЛ з питань вчинення протиправних дій щодо дітей в мережі інтернет.

Якщо є час, можна об'єднати учасників у групи та надати п'ять хвилин часу для ознайомлення з суттю різних справ та надання відповідей на питання.

Запитання для обговорення:

– *Як ви вважаєте, якби схожі справи розглядались в національних судах України, чи були би задоволені позови?*

– *Чи знаєте ви в яких випадках українці можуть звернутись до ЄСПЛ за захистом своїх прав?*

4. Робота в групах «Відповідальність за вчинення протиправних дій щодо дітей в мережі інтернет»

Мета: формування вміння ідентифікувати протиправні дії щодо дітей в мережі інтернет та здійснювати їх кваліфікацію.

Час: 20 хв.

Необхідні матеріали: Додаток 1.10.1.3, фліпчарт та аркуші для фліпчарту, маркери.

Хід проведення:

Тренер/тренерка об'єднує учасників у чотири групи та надає кожній із них ситуаційну задачу із Додатка 1.10.1.3. Завдання для груп: протягом десяти хвилин проаналізувати ситуацію, визначити, склад яких правопорушень наявний у цій ситуації, та яку кваліфікацію можна дати діянням з врахуванням наявної в умові інформації.

Після завершення роботи в групах учасники презентують напрацювання, а тренер/тренерка доповнює їхні відповіді, спираючись на судові рішення, з яких були взяті фабули ситуацій.

До уваги тренера/тренерки!

Під час підготовки до заняття можна самостійно знайти фабули протиправних діянь, які були вчинені щодо дитини в мережі інтернет, або скористатись запропонованими у Додатку 1.10.1.3. Для пошуку судових рішень доцільно використовувати Єдиний державний реєстр судових рішень: https://reyestr.court.gov.ua/.

Запитання для обговорення:

- *Чи погоджуєтесь ви з кваліфікацією протиправних діянь, наданих судами у розглянутих справах?*
- *Чи були у вашій практичній діяльності справи, пов'язані з вчиненням протиправних дій щодо дитини в інтернеті?*

До уваги тренера/тренерки!

Слід нагадати учасникам, що вчинення кримінального правопорушення щодо малолітньої дитини або у присутності дитини є обтяжуючою відповідальність обставиною (п. 6 ч. 1 ст. 67 ККУ). Крім того, обтяжуючою обставиною є вчинення злочину з використанням умов воєнного стану (п. 11 ч. 1 ст. 67 ККУ) та адміністративного правопорушення в умовах стихійного лиха або за інших надзвичайних обставин (п. 5 ч. 1 ст. 35 КУпАП).

Підсумовуючи, тренер/тренерка зазначає: «*Швидкість, з якою розвиваються інтернет-технології, і, відповідно, поява дедалі нових загроз для безпеки дітей, призводить до того, що діяння правопорушників не завжди можуть охоплюватись традиційно відомими на національному рівні юридичними складами правопорушень. Водночас завжди важливо:*

- *ідентифікувати та документувати протиправність таких дій;*
- *шукати відповідні норми у ратифікованих Україною міжнародних та європейських документах;*
- *залучати адвокатів дітей до таких справ, які можуть допомогти звернутись до ЄСПЛ за захистом порушених прав дитини, у разі відсутності відповідної норми в національному законодавстві;*
- *завжди виходити в своїх діях з найкращих інтересів дитини*».

Тестові питання до заняття:

1. Закон України «Про медіа» передбачає настання відповідальності медіа у вигляді фінансових санкцій за:

А) поширення інформації, що може завдати шкоди фізичному, психічному або моральному розвитку дітей;

Б) порушення вимог щодо нерозголошення інформації про дитину без письмової згоди хоча б одного з батьків або інших законних представників дитини, за винятком випадків, якщо це здійснюється в найкращих інтересах дитини;

В) поширення порнографічних матеріалів, а також матеріалів, що заохочують сексуальну експлуатацію та насильство над дітьми, демонструють статеві відносини дітей, використовують образ дітей (візуальний запис образу дітей) у видовищних заходах сексуального чи еротичного характеру;

Г) усі відповіді правильні.

2. Якою статтею та якого нормативно-правового акту передбачена відповідальність за кібербулінг?

А) 156-1 ККУ;

Б) 173-4 КУпАП;

В) 173-5 КУпАП;

Г) 301-2 ККУ.

3. В якій справі ЄСПЛ підкреслив, що право на приватність в інтернеті не має перешкоджати захисту та відновленню порушених прав та інтересів дітей, та зазначив про важливість розроблення законодавства, яке дозволить провайдерам порушувати принцип конфіденційності, зокрема з метою виявлення осіб, які вчиняють насильство щодо дітей в інтернеті?

А) Reklos and Davourlis v. Greece;

Б) K.U. v. Finland;

В) I.V.Ț. v. Romania;

Г) немає правильної відповіді.

4. До правопорушень, що стосуються дитячої порнографії, згідно з Лансаротською конвенцією, належить:

А) виготовлення дитячої порнографії;

Б) свідоме одержання доступу до дитячої порнографії за допомогою інформаційно-комунікаційних технологій;

В) володіння дитячою порнографією;

Г) всі відповіді правильні.

5. Яку мету може передбачати пропозиція зустрічі в контексті домагання дитини для сексуальних цілей, відповідальність за яке передбачена ст. 156-1 ККУ?

А) вчинення стосовно особи, яка не досягла шістнадцятирічного віку, будь-яких дій сексуального характеру або розпусних дій;

Б) втягнення неповнолітньої особи у виготовлення дитячої порнографії;

В) правильні відповіді А та Б;

Г) немає правильної відповіді.

Ключі-відповіді: 1. Г; 2. Б; 3. Б; 4. Г; 5. В.

Додаток 1.10.1.1

Група 1

ЛАНСАРОТСЬКА КОНВЕНЦІЯ. СТАТТЯ 20. ПРАВОПОРУШЕННЯ, ЩО СТОСУЮТЬСЯ ДИТЯЧОЇ ПОРНОГРАФІЇ.

1. Кожна Сторона вживає необхідних законодавчих або інших заходів для забезпечення криміналізації такої умисної поведінки, учиненої без правових підстав:
   a) виготовлення дитячої порнографії;
   b) пропонування або надання доступу до дитячої порнографії;
   c) розповсюдження або передавання дитячої порнографії;
   d) придбання дитячої порнографії для себе або іншої особи;
   e) володіння дитячою порнографією;
   f) свідоме одержання доступу до дитячої порнографії за допомогою інформаційно-комунікаційних технологій.
2. Для цілей цієї статті термін «дитяча порнографія» означає будь-які матеріали, які візуально зображують дитину, залучену до реальної або модельованої очевидно сексуальної поведінки, чи будь-яке зображення дитячих статевих органів, здебільшого із сексуальною метою.
3. Кожна Сторона може залишити за собою право не застосовувати цілком або частково підпунктів «a» та «e» пункту 1 цієї статті до виготовлення порнографічної продукції та володіння нею:
   - яка складається лише з модельованих образів або реалістичних зображень неіснуючої дитини;
   - до якої залучено дітей, які досягли віку, визначеного під час застосування пункту 2 статті 18 цієї Конвенції, якщо за їхньою згодою й тільки для їхнього приватного використання вони виготовили ці зображення або володіють ними.
4. Кожна Сторона може залишити за собою право не застосовувати цілком або частково підпункту «f» пункту 1 цієї статті.

Роз'яснення:

«Дитяча порнографія» – це будь-які матеріали, які візуально зображують дитину, залучену до реальної або модельованої явно сексуальної поведінки, чи будь-яке зображення дитячих статевих органів, здебільшого із сексуальною метою.

Для того, щоб забезпечити ефективну реакцію правоохоронних органів на таке явище як «дитяча порнографія», надзвичайно важливо встановити кримінальну відповідальність за діяльність кожного учасника ланцюга, від виготовлення до володіння/споживання. Як викладено в Пояснювальній доповіді до Лансаротської конвенції, володіння дитячою порнографією у будь-якій формі, такій як журнали, відеокасети, DVD-диски або портативні телефони, зокрема такою, яка зберігається в комп'ютерній системі або на носії даних, а також на знімному запам'ятовуючому пристрої, дискеті або CD-Rom криміналізується відповідно до підпункту e) пункту 1.

У Конвенції також введено новий елемент, який призначений для сприяння виявлення тих, хто переглядає дитячі зображення в інтернеті, отримуючи доступ до вебсайтів з дитячою порнографією, але без завантаження таких матеріалів, тому в деяких юрисдикціях такі особи не можуть бути виявлені та звинувачені у придбанні чи володінні. Для того, щоб нести кримінальну відповідальність, особа повинна мати намір зайти на сайт, де доступна

дитяча порнографія, та знати, що там можна знайти такі зображення. Санкції не повинні застосовуватися до осіб, які ненавмисно заходять на сайти, що містять дитячу порнографію. Навмисний характер кримінального правопорушення може бути визначений, зокрема, з того факту, що він повторюється, або що злочини були скоєні через певну послугу в обмін на оплату. Крім того, визначені в Лансаротській конвенції злочини надалі підлягають такій самій криміналізації відповідно до національного законодавства незалежно від того, якими б засобами не користувались злочинці, що вчиняють правопорушення сексуального характеру, для їх здійснення, тобто з використанням ІКТ чи без них, навіть якщо в Лансаротській конвенції очевидно не згадано ІКТ.

Криміналізація та кримінальне переслідування зображень та/або відео, що містять сексуальний підтекст чи відвертих зображень та/або відео сексуального характеру, які створюються, поширюються та отримуються дітьми (так званий секстинг) повинні здійснюватися з обережністю, як це описано у Висновку Лансаротського комітету щодо цього питання. Термін «дитяча порнографія» досі застосовується під час розгляду правових питань та контекстів, зокрема коли йдеться про міжнародні та національні правові договори, що прямо включають цей термін. Однак цього терміну варто уникати, наскільки це можливо, зокрема коли йдеться про неправові контексти. У таких контекстах потрібно вибирати терміни «матеріали сексуального насильства над дітьми» чи «матеріали сексуальної експлуатації дітей».

КРИМІНАЛЬНИЙ КОДЕКС УКРАЇНИ

Стаття 301[1]. Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження

1. Умисне одержання доступу до дитячої порнографії з використанням інформаційно-телекомунікаційних систем чи технологій або умисне її придбання, або умисне зберігання, ввезення в Україну, перевезення чи інше переміщення дитячої порнографії без мети збуту чи розповсюдження –

   караються арештом на строк від трьох до шести місяців або обмеженням волі на строк до п'яти років, або позбавленням волі на строк від двох до шести років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

2. Ввезення в Україну дитячої порнографії з метою збуту чи розповсюдження або її зберігання, перевезення чи інше переміщення з тією самою метою –

   караються позбавленням волі на строк від семи до десяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

3. Виготовлення, розповсюдження, збут дитячої порнографії або примушування неповнолітньої особи до участі у створенні дитячої порнографії –

   караються позбавленням волі на строк від восьми до дванадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

4. Дії, передбачені частинами другою або третьою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або з отриманням доходу у великому розмірі, або примушування малолітньої особи до участі у створенні дитячої порнографії –

   караються позбавленням волі на строк від дев'яти до п'ятнадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

5. Не підлягає кримінальній відповідальності неповнолітня особа за виготовлення, зберігання, перевезення чи інше переміщення дитячої порнографії, якщо такі дії вчинені без мети збуту чи розповсюдження.

6. Не підлягає кримінальній відповідальності за діяння, передбачені частиною першою цієї статті, особа, яка вчинила їх з метою виконання покладених на неї повноважень на підставах і в порядку, передбачених законодавством.

Примітка. У цій статті одержання доступу до дитячої порнографії з використанням інформаційно-телекомунікаційних систем або технологій слід вважати умисним, якщо доведено, що особа усвідомлювала, що у такий спосіб вона отримає доступ до дитячої порнографії (наприклад доведено, що особа отримала такий доступ повторно або через внесення плати тощо).

У більшості країн створення, поширення та зберігання зображень дітей сексуального характеру є незаконним. У разі поширення зображень дітей сексуального характеру, дорослі не повинні переглядати їх. Демонстрація зображень сексуального характеру дитині дорослим завжди є злочинним діянням.

Група 2

ЛАНСАРОТСЬКА КОНВЕНЦІЯ. СТАТТЯ 21. ПРАВОПОРУШЕННЯ, ЩО СТОСУЮТЬСЯ УЧАСТІ ДИТИНИ В ПОРНОГРАФІЧНИХ ВИСТАВАХ

1. Кожна Сторона вживає необхідних законодавчих або інших заходів для забезпечення криміналізації такої умисної поведінки:
   a) вербування дітей для участі в порнографічних виставах або спонукання дитини до участі в таких виставах;
   b) примушування дитини до участі в порнографічних виставах або отримання користі від цього чи іншого використання дитини із цією метою;
   c) свідоме відвідування порнографічних вистав, у яких залучено дітей.
2. Кожна Сторона може залишити за собою право обмежити застосування підпункту «c» пункту 1 цієї статті до випадків, коли дітей вербували або примушували відповідно до підпунктів «a» чи «b» пункту 1 цієї статті.

КРИМІНАЛЬНИЙ КОДЕКС УКРАЇНИ

Стаття 301². Проведення видовищного заходу сексуального характеру за участю неповнолітньої особи

1. Проведення видовищного заходу сексуального характеру, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, у якому задіяно неповнолітню особу, –

   карається позбавленням волі на строк від п'яти до семи років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.
2. Відвідування видовищного заходу сексуального характеру з метою його перегляду, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, у якому завідомо для відвідувача задіяно малолітню чи неповнолітню особу, –

   карається позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.
3. Втягнення неповнолітньої особи до участі у видовищному заході сексуального характеру, що проходить, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, або примушування неповнолітньої особи до участі у такому заході з використанням обману, шантажу, уразливого стану особи або із застосуванням чи погрозою застосування насильства –

   караються позбавленням волі на строк від семи до десяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.
4. Дії, передбачені частиною третьою цієї статті, вчинені стосовно малолітньої особи, –

   караються позбавленням волі на строк від восьми до п'ятнадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Примітка. Під видовищним заходом сексуального характеру у цій статті слід розуміти публічний показ у будь-якій формі продукції сексуального характеру або сценічні дії, метою яких є втілення сексуальних дій.

Група 3

ЛАНСАРОТСЬКА КОНВЕНЦІЯ. СТАТТЯ 22. РОЗБЕЩЕННЯ ДІТЕЙ

Кожна Сторона вживає необхідних законодавчих або інших заходів для забезпечення криміналізації умисного спонукання дитини, яка не досягла віку, передбаченого пунктом 2 статті 18 цієї Конвенції, спостерігати за сексуальним насильством або діяльністю сексуального характеру, навіть якщо вона не бере в цьому участі.

Роз'яснення: У статті 22 передбачено кримінальне правопорушення, здійснення якого спрямоване на змушення дитини спостерігати діяльність сексуального характеру або вчинення такої діяльності у присутності дітей, що може спричинити шкоду психологічному здоров'ю постраждалої особи, з ризиком завдання серйозної шкоди особистості, зокрема спотворене уявлення про секс та особисті стосунки.

У цій статті передбачається кримінальна відповідальність за умисне схиляння дитини, яка не досягла законного віку сексуальної згоди, до спостерігання сексуального насильства над іншими дітьми чи дорослими або діяльності сексуального характеру. Не обов'язково, щоб дитина яким-небудь чином брала участь у діяльності сексуального характеру. Злочин повинен бути здійснений умисно та «для сексуальних цілей». Конвенція залишає Сторонам можливість тлумачення терміну «спонукання» та воно може включати будь-який спосіб, з допомогою якого дитина змушена бути свідком такої діяльності, такий як сила, примушування, намовляння, обіцянка тощо. Кримінальне правопорушення виникає, коли дитина не досягла віку статевої згоди, відповідно до національної реєстрації (пункт 2 статті 18). Формулювання «сексуальне розбещення дитини онлайн» деколи застосовується у правових стандартах як термін, альтернативний до «приставання до дітей із сексуальною метою онлайн» («грумінг»).

КРИМІНАЛЬНИЙ КОДЕКС УКРАЇНИ

Стаття 156. Розбещення неповнолітніх.

1. Вчинення розпусних дій щодо особи, яка не досягла шістнадцятирічного віку, –

   караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк.

2. Ті самі дії, вчинені щодо малолітньої особи або вчинені членами сім'ї чи близькими родичами, особою, на яку покладено обов'язки щодо виховання потерпілого або піклування про нього, –

   караються позбавленням волі на строк від п'яти до восьми років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.

Науковий коментар:

Об'єкт злочину – статева недоторканість і нормальний фізичний, психічний і соціальний розвиток неповнолітніх. Потерпілим виступає особа чоловічої або жіночої статі, яка не досягла 16-річного віку. Не має значення, чи досягла потерпіла особа статевої зрілості, хто був ініціатором вчинення розпусних дій, а також характеристика потерпілої особи (попереднє ведення статевого життя, наявність сексуального досвіду тощо).

Об'єктивна сторона злочину. З об'єктивної сторони злочин виражається у вчиненні розпусних дій сексуального характеру, здатних викликати фізичне і моральне розбещення неповнолітніх.

Види розпусних дій:

- фізичні: оголення статевих органів винної чи потерпілої особи, непристойні доторкання до статевих органів, які викликають статеві збудження, навчання статевим збоченням, імітація статевого акту, схиляння або примушування потерпілих до вчинення певних сексуальних дій між собою, вчинення статевих зносин, акту онанізму у присутності потерпілої особи тощо;
- інтелектуальні: цинічні розмови з потерпілою особою на сексуальні теми, ознайомлення дитини із порнографічними зображеннями, відеофільмами тощо.

Злочин вважається закінченим з моменту вчинення розпусних дій.

Суб'єктивна сторона злочину. Суб'єктивна сторона злочину характеризується прямим умислом. Щодо віку потерпілої особи, то винна особа може достовірно знати або припускати, що така особа не досягла 16 років, або повинна була і могла це усвідомлювати.

Суб'єкт злочину. Суб'єктом злочину виступає особа чоловічої або жіночої статі, яка досягла 16-річного віку.

Кваліфікуючі ознаки. Кваліфікуючими ознаками злочину є вчинення розпусних дій:

- щодо малолітньої особи;
- членами сім'ї чи близькими родичами*, особою, на яку покладено обов'язки щодо виховання потерпілого або піклування про нього.

*близькі родичі та члени сім'ї – чоловік, дружина, батько, мати, вітчим, мачуха, син, дочка, пасинок, падчерка, рідний брат, рідна сестра, дід, баба, прадід, прабаба, внук, внучка, правнук, правнучка, усиновлювач чи усиновлений, опікун чи піклувальник, особа, яка перебуває під опікою або піклуванням, а також особи, які спільно проживають, пов'язані спільним побутом і мають взаємні права та обов'язки, у тому числі особи, які спільно проживають, але не перебувають у шлюбі (пункт 1 частина перша статті 3 Кримінального процесуального кодексу України).

Група 4

ЛАНСАРОТСЬКА КОНВЕНЦІЯ. СТАТТЯ 23. ДОМАГАННЯ ДИТИНИ ДЛЯ СЕКСУАЛЬНИХ ЦІЛЕЙ

Кожна Сторона вживає необхідних законодавчих або інших заходів для забезпечення криміналізації умисної пропозиції, зробленої дорослою людиною за допомогою інформаційно-комунікаційних технологій, зустрітися з дитиною, яка не досягла віку, передбаченого пунктом 2 статті 18 цієї Конвенції, для скоєння проти неї одного з правопорушень, передбачених підпунктом «а» пункту 1 статті 18 або підпунктом «а» пункту 1 статті 20 цієї Конвенції, якщо після цієї пропозиції відбулись істотні дії, що призвели до такої зустрічі.

Роз'яснення: Лансаротська конвенція є першим міжнародно-правовим документом, що дає визначення грумінгу. Конвенція визначає цю діяльність як «приставання до дітей у сексуальних цілях». Термін «грумінг» означає підготовку дитини до сексуального насильства. Ця підготовка мотивована бажанням використати дитину для сексуального задоволення. Це може включати дружбу з дитиною, часто з дорослою людиною, яка видає себе за іншу молоду людину, залучаючи дитину до обговорення інтимних питань, і поступово демонструючи дитині матеріали сексуального характеру для того, щоб зменшити опір або заборони стосовно сексу.

Дитина також може бути залучена до створення дитячої порнографії, методом надсилання компрометуючих особистих фотографій та із використанням цифрової камери, вебкамери або камери телефону, що забезпечує грумера засобами контролю над дитиною за допомогою погроз. Якщо організовується фізична зустріч, дитина може зазнати сексуального насильства чи іншої шкоди.

Приставання до дітей за допомогою інформаційно-комунікаційних технологій не обов'язково призводить до особистої зустрічі. Воно може тривати лише через мережу інтернет, утім завдати серйозної шкоди дитині. Злочини сексуального характеру, які навмисно вчиняються під час онлайн-зустрічі за допомогою комунікаційних технологій, часто пов'язані з виготовленням, володінням та передаванням дитячої порнографії.

КРИМІНАЛЬНИЙ КОДЕКС УКРАЇНИ

Стаття 156[1]. Домагання дитини для сексуальних цілей

1. Пропозиція зустрічі, зроблена повнолітньою особою, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, особі, яка не досягла шістнадцятирічного віку, з метою вчинення стосовно неї будь-яких дій сексуального характеру або розпусних дій, у разі, якщо після такої пропозиції було вчинено хоча б одну дію, спрямовану на те, щоб така зустріч відбулася, –

   карається обмеженням волі на строк до трьох років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

2. Пропозиція зустрічі, зроблена повнолітньою особою, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, неповнолітній особі з метою втягнення її у виготовлення дитячої порнографії, якщо після такої пропозиції було вчинено хоча б одну дію, спрямовану на те, щоб така зустріч відбулася, –

   карається позбавленням волі на строк від двох до п'яти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

3. Дії, передбачені частинами першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або щодо малолітньої особи, –

   караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Примітка.

1. Під зустріччю в цій статті слід розуміти, у тому числі, зустріч, проведення якої передбачає використання інформаційно-телекомунікаційних систем або технологій.
2. Під дитячою порнографією в цій статті та статті 301^1 цього Кодексу слід розуміти зображення у будь-який спосіб дитини чи особи, яка виглядає як дитина, у реальному чи змодельованому відверто сексуальному образі або задіяної у реальній чи змодельованій відверто сексуальній поведінці, або будь-яке зображення статевих органів дитини в сексуальних цілях.

Додаток 1.10.1.2

K.U. v. Finland 2 December 2008

Справа стосувалася реклами сексуального характеру, розміщеної про 12-річного хлопчика на сайті знайомств в інтернеті без його відома. У рекламі зазначався його вік, рік народження та детальний опис зовнішності. Крім того, було посилання на інтернет-сторінку К. У., де містився точний, крім однієї цифри, номер його телефону та фото. Реклама наголошувала, що він шукає інтимних стосунків з хлопцем його віку або старше.

Батько К. У. попросив поліцію ідентифікувати особу, яка розмісила рекламу, щоб притягнути до відповідальності. Провайдер послуг відмовив у наданні такої інформації. Згідно з фінським законодавством, яке діяло на той час, поліція та суди не могли вимагати від інтернет-провайдера ідентифікувати особу, яка розмістила повідомлення оголошення. Зокрема виконавець послуг відмовився встановити особу винну, стверджуючи, що це буде порушенням конфіденційності.

Суд постановив, що відбулося порушення статті 8 (право на повагу до приватного і сімейного життя) Конвенції. Він зазначив, що розміщення рекламної інформації було кримінальним актом, який зробив неповнолітнього об'єктом домагань з боку педофілів. Законодавцям слід забезпечити розроблення актів, які б враховували право на приватність в інтернеті, але водночас запобігали кримінальній поведінці та порушенню прав інших осіб, зокрема дітей.

Reklos and Davourlis v. Greece 15 January 2009

Справа стосувалася фотографій новонародженої дитини, зроблених у приватній клініці без попередньої згоди батьків, та зберігання негативів. Одразу після народження дитину помістили в стерильну палату, до якої лише медичний персонал клініки мав доступ. Наступного дня матері надали дві фотографії, на одній з яких дитина зображена обличчям до камери, зроблених на базі клініки.

Заявники скаржилися на фотографа за вторгнення в середовище, до якого повинен був мати доступ лише медичний персонал, а також можливе роздратування дитини через фотографування спереду.

Зіткнувшись з байдужістю клініки до їхніх скарг і відмовою надати негативи фотографій, заявники подали позов про відшкодування збитків, який був відхилено як необґрунтований.

Суд постановив, що відбулося порушення статті 8 (право на повагу до приватного і сімейного життя) Конвенції. Хоча на фотографіях малюк був лише спереду, а не в стані, який можна було б вважати таким, що принижує гідність, або іншим чином може завдати шкоди його особистості, головним міркуванням у цьому випадку було не те, чи фотографії були нешкідливими, але той факт, що фотограф їх зберіг без отримання згоди заявників. Отже, зображення дитини було збережено фотографом в ідентифікованому вигляді з можливістю подальшого використання всупереч бажанням дитини та/або її батьків. Національні суди недостатньо гарантували право дитини на захист її особистого життя.

Söderman v. Sweden 12 November 2013

Справа стосувалась чотирнадцятирічної станом на 2002 рік дівчини, яка виявила, що її вітчим намагався таємно зняти її оголеною – він сховав відеокамеру у кошику для білизни у ванній кімнаті, спрямовану на місце, де вона зазвичай роздягалася. Мати заявниці знищила відеозапис і повідомила про інцидент поліцію, яка притягнула вітчима до кримінальної відповідальності за сексуальні домагання. Вітчим був виправданий в апеляції в 2007 році, тому що, хоча він навмисно знімав неповнолітню, його поведінка не підпадала під положення про сексуальні розбещення, оскільки він не мав наміру, щоб заявниця дізналася про фільм. Крім

того, шведський апеляційний суд зазначив, що в шведському законодавстві немає загальної заборони знімати особу без її згоди, навіть якщо ця особа неповнолітня.

Велика палата винесла своє рішення, встановивши, що Швеція не виконала свого позитивного зобов'язання щодо захисту права заявника на повагу до приватного життя (стаття 8 ЄКПЛ). На думку Великої Палати, у шведському законодавстві не існувало ані кримінального, ані цивільного засобу правового захисту, який би дозволив заявниці отримати ефективний захист від порушення її особистої недоторканності. Вітчим був виправданий у сексуальних домаганнях не через відсутність доказів, а тому, що його дії на той час не вважалися сексуальними домаганнями. Положення про сексуальні розбещення були змінені в Швеції у 2005 році.

I.V.Ț. v. Romania 1 March 2022

Ця справа стосувалася телевізійного інтерв'ю неповнолітньої особи без згоди батьків або адекватних заходів для захисту її особистості. Інтерв'ю, яке стосувалося смерті однокласника, стало причиною знущань над нею та спричинило її емоційний стрес.

Суд постановив, що відбулося порушення статті 8 (право на повагу до приватного і сімейного життя) Конвенції, встановивши, що національні суди належним чином не врахували той факт, що особа була неповнолітньою, не виконавши їхній обов'язок захищати її право на приватне життя. Необхідно було врахувати вимогу батьківської згоди. Суд, зокрема, зазначив, що правила Національної аудіовізуальної ради передбачали «право неповнолітнього на своє приватне життя переважає над потребою в інформації». Суд зазначив, що національні суди встановили, що заявник зазнав сильних страждань після трансляції.

До уваги тренера/тренерки!

Коментуючи рішення Суду у справі «I.V.Ț. v. Romania», доцільно звернути увагу учасників на те, що наприкінці 2022 року в Україні було прийнято Закон України «Про медіа», згідно з ч. 10 ст.42 якого:

«Крім виняткових випадків, коли неможливо інакше забезпечити найкращі інтереси дитини, суб'єкти у сфері медіа не мають права без письмової згоди хоча б одного з батьків або інших законних представників дитини оприлюднювати фото дитини, яка зазнала фізичного чи сексуального насилля, а також розголошувати будь-яку інформацію, яка:

1) *може сприяти ідентифікації дитини, яка задіяна у провадженні у справах про адміністративні правопорушення, в кримінальному провадженні у будь-якому статусі або стосовно якої є інформація про здійснення нею правопорушення;*

2) *стосується факту самогубства дитини, при цьому ідентифікує її особу».*

Державне регулювання, нагляд та контроль у сфері медіа здійснює Національна рада України з питань телебачення і радіомовлення – незалежний постійно діючий колегіальний державний орган.

Додаток 1.10.1.3[2]

Фабула 1

Вчителька гімназії систематично протягом місяця вчиняла діяння, які полягали у нападках через надсилання великої кількості СМС–повідомлень, телефонних дзвінках.

До матеріалів справи долучено скріншоти листування у месенджерах Телеграм, Вайбер, яка відбувалася в період з жовтня по грудень між вчителькою та неповнолітнім. Зміст конкретних фраз, лексики та характеру використання мовних засобів, які вчителька застосовує у переписці з неповнолітнім, дає підстави для висновку, що вони можуть викликати у неповнолітнього побоювання за свою безпеку і завдати шкоду його психічному здоров`ю.

Інформація для тренера/тренерки:

Рішення суду міститься за посиланням: https://reyestr.court.gov.ua/Review/104244197.

Дії вчительки кваліфіковані за ст.173-4 «Булінг (цькування) учасника освітнього процесу» КУпАП.

Фабула 2

Юлія, дізнавшись про існування у мережі інтернет вебсайтів, на яких користувачі зі всього світу за допомогою комп`ютерної техніки з вебкамерами задовольняють свої статеві пристрасті через віртуальне спілкування з дівчатами, які оголюють своє тіло в режимі реального часу, та за демонстрування сексуальних дій здійснюють оплату грошовими коштами, котрі зараховуються на особистий рахунок на сайті, маючи корисливий мотив, з метою власного незаконного збагачення, вирішила організувати проведення таких діянь, задіявши до їх проведення неповнолітніх осіб. Реалізовуючи свій умисел, Юлія орендувала офісне приміщення та підготувала його для проведення відеотрансляцій в режимі реального часу на сайтах мережі інтернет за участю дівчат за грошову винагороду.

В подальшому Юлія, маючи корисливий мотив, діючи умисно, з метою отримання більшого прибутку від своєї злочинної діяльності, усвідомлюючи, що попит на отримання роботи у вказаній діяльності є більшим серед неповнолітніх осіб жіночої статті, організувала задіяння останніх до участі у проведенні таких заходів. З цією метою через соціальні мережі в інтернеті та мобільні застосунки, такий як Телеграм, підшукувала та підбирала дівчат, пропонуючи роботу в офісі «вебмоделями». Під час особистої зустрічі остання доводила до їхнього відома принципи роботи, а саме – спілкування з клієнтами на сексуальні теми в умовах реального часу із застосуванням вебкамер. Після чого під час виконання роботи, що полягала у спілкуванні з чоловіками, останні, спостерігаючи, що інші «вебмоделі» отримували більший заробіток, коли роздягались та оголювали своє тіло, водночас здійснюючи дотики до інтимних частин тіла, добровільно приймали рішення про вчинення вказаних вище дій, про що Юлії було достовірно відомо.

Надалі Юлія, отримавши від дівчини добровільну згоду, усвідомлюючи, що реєстрація у мережі інтернет на вебсайтах, де здійснюється спілкування між чоловіками та жінками, можлива лише повнолітньої особи, з метою приховання віку останніх, здійснювала виготовлення фальшивого паспорта громадянина України (ID-картки), схожого на справжній, в якому змінювала рік народження особи, і у такий спосіб організовувала участь неповнолітніх осіб. В подальшому «моделі», використовуючи ноутбуки, обладнані вебкамерами, авторизувалися на вищезазначених сайтах і в режимі онлайн спілкувалися з користувачами цих сайтів, на їхні побажання оголялися, здійснювали маніпуляції зі статевими органами, тобто вчиняли сценічні дії, метою яких є втілення сексуальних дій. За вчинення вказаних дій на відповідні акаунти неповнолітніх дівчат нараховувались грошові кошти, доступ до

[2] Всі імена в наведених в Додатку фабулах вигадані.

яких мала лише Юлія, оскільки під час реєстрації вказувала реквізити для отримання оплат, про які не повідомляла останніх, та здійснювала розрахунок з моделями особисто, через надання готівки або грошового переказу на картку.

Інформація для тренера/тренерки:

Рішення суду міститься за посиланням: https://reyestr.court.gov.ua/Review/108244485.

Дії Юлії кваліфіковані за ч. 1 ст. 301-2 КК.

Фабула 3

У квітні в Ігоря виник злочинний умисел на використання облікових записів в мобільному застосунку Телеграм мережі інтернет та подальшого відправлення приватних повідомлень користувачам системи миттєвого обміну повідомлень. З цією метою Ігор, користуючись послугами мережі інтернет, створив у мобільному застосунку Телеграм обліковий запис користувача, іменований «Король». У подальшому систематично за допомогою мобільного застосунку Телеграм, зокрема використовуючи можливості Телеграм-боту (анонімного чату), здійснював надсилання повідомлень користувачу мобільного застосунку Телеграм, який використовувала малолітня Вікторія, з висловлюваннями, які спрямовані на спонукання до дій сексуального характеру, спрямовані на задоволення своїх статевих потреб.

За допомогою програмного забезпечення, влаштованого на належному йому мобільному телефоні, Ігор умисно зберігав графічні файли та відеозаписи, які належать до дитячої порнографії, без мети збуту чи розповсюдження, доти, доки його мобільний телефон не був вилучений працівниками поліції під час проведення обшуку.

Інформація для тренера/тренерки:

Рішення суду міститься за посиланням: https://reyestr.court.gov.ua/Review/108348739.

Дії Ігоря кваліфіковані за ч. 2 ст. 156, ч. 1 ст. 301-1 КК України.

Фабула 4

Іван, маючи прямий умисел, направлений на задоволення статевої пристрасті неприродним способом, усвідомлюючи суспільно небезпечний характер свого діяння у вигляді порушення статевої недоторканості неповнолітньої потерпілої, передбачаючи його суспільно небезпечні наслідки і бажаючи їх настання, для якого він протягом останнього часу в застосунках-месенджерах спілкувався з неповнолітньою потерпілою Катериною, де через текстові повідомлення запропонував їй зустрітися, після чого пройшов з потерпілою за місцем свого проживання, куди запросив останню випити кави.

Зайшовши до приміщення квартири, Іван, продовжуючи свої дії, спрямовані на задоволення своєї статевої пристрасті, почав обіймати потерпілу, цілувати у шию та обличчя, потім взяв на руки та заніс до житлової кімнати, де став знімати її одяг, на що потерпіла висловлювала заперечення, та просила її не роздягати, не реагуючи на які він продовжував свої дії. Далі, поклавши останню на диван, обвинувачений Іван сам роздягнувся, та, будучи обізнаним про неповнолітній вік Катерини, став задовольняти свою статеву пристрасть за допомогою дотиків руками її оголеного тіла, грудей, зовнішніх статевих органів та у подальшому здійснив дії сексуального характеру орогенітальним способом, задовольнивши у такий спосіб свої статеві потреби і статеву пристрасть.

Інформація для тренера/тренерки:

Рішення суду міститься за посиланням: https://reyestr.court.gov.ua/Review/101584625.

Дії Івана кваліфіковані за ч. 3 ст. 153 КК України.

Додаткові рішення судів у справах, пов'язаних із вчиненням протиправних дій щодо дитини в мережі та з використанням мережі інтернет:

https://reyestr.court.gov.ua/Review/102937092

https://reyestr.court.gov.ua/Review/107942786

https://reyestr.court.gov.ua/Review/96986962

https://reyestr.court.gov.ua/Review/101461561

https://reyestr.court.gov.ua/Review/99979945

https://reyestr.court.gov.ua/Review/90385050

https://reyestr.court.gov.ua/Review/109894513

https://reyestr.court.gov.ua/Review/110197641

Заняття 1.10.2. Відповідальність за вчинення дітьми протиправних дій в мережі інтернет

Мета: надати учасникам інформацію про особливості відповідальності за вчинення протиправних дій дітьми в мережі інтернет та відпрацювати вміння кваліфікувати відповідні випадки.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Асоціації, пов'язані із вчиненням протиправних дій дітьми в мережі інтернет	Обговорення	10 хв	Фліпчарт та аркуші для фліпчарту, маркери (або мультимедійне обладнання)
2.	Відповідальність за вчинення дітьми протиправних дій в мережі інтернет	Інформаційне повідомлення	20 хв	Додаток 1.10.2.1, мультимедійне обладнання
3.	Легально чи нелегально?	Вправа	20 хв	Додаток 1.10.2.2, фліпчарт та аркуші для фліпчарту, маркери або мультимедійне обладнання
4.	Відповідальність за вчинення дітьми протиправних дій в мережі інтернет	Робота в групах	40 хв	Додаток 1.10.2.3, кулькові ручки

До уваги тренера/тренерки!

Доцільно це заняття проводити в межах курсів підвищення кваліфікації та службової підготовки або для випускних курсів здобувачів вищої освіти.

ХІД ЗАНЯТТЯ

1. Обговорення «Асоціації, пов'язані із вчиненням протиправних дій дітьми в мережі інтернет»

Мета: оцінити рівень інформованості учасників, актуалізувати основні поняття щодо протиправних дій, які вчиняються дітьми в мережі інтернет.

Час: 10 хв.

Необхідні матеріали: фліпчарт, аркуші для фліпчарту, маркери або мультимедійне обладнання.

Хід проведення:

Тренер/тренерка на аркуші фліпчарту пише словосполучення «*Протиправні дії, які вчиняються дітьми в мережі інтернет*» і пропонує учасникам озвучити асоціації, які виникають у них щодо цього словосполучення: «*Сьогодні ми з вами говоримо про відповідальність за вчинення протиправних дій дітьми в мережі інтернет, і я пропоную вам навести асоціації, пов'язані з цим словосполученням*».

Тренер/тренерка занотовує всі відповіді, які надають учасники.

До уваги тренера/тренерки!

Якщо дозволяє технічне обладнання, можна зробити опитування за допомогою програми «Mentimetr» у вигляді хмаринки думок.

Запитання для обговорення:

- *Чи складно було знайти відповідну асоціацію?*
- *Чи пов'язані якісь із цих асоціацій з вашим власним досвідом?*

2. Інформаційне повідомлення «Відповідальність за вчинення дітьми протиправних дій в мережі інтернет»

Мета: систематизувати знання учасників щодо особливостей відповідальності за вчинення протиправних дій дітьми в мережі інтернет.

Час: 20 хв.

Необхідні матеріали: Додаток 1.10.2.1, мультимедійне обладнання.

Хід проведення:

Тренер/тренерка зазначає: «*Якщо дитина, тобто особа віком до 18 років, вчиняє протиправні діяння у мережі інтернет, вона особисто несе відповідальність згідно з чинним законодавством, а у разі недосягнення нею встановленого віку, до відповідальності можуть бути притягнені її батьки або інші законні представники. В умовах дії правового режиму воєнного стану актуальними постають питання втягнення дітей у злочинну діяльність, зокрема в мережі інтернет*», після чого презентує інформацію із Додатка 1.10.2.1.

До уваги тренера/тренерки!

Під час підготовки до заняття слід перевірити актуальність інформації, яка міститься у Додатку 1.10.2.1, та підготувати мультимедійну презентацію. Під час підготовки змісту інформаційного повідомлення та презентації слід враховувати категорію учасників, чи обізнані вони із загальними засадами відповідальності дітей. Якщо ні, то доцільно зосередити увагу спочатку на цих питаннях. Для підготовки можна використовувати матеріали навчально-методичного посібника «Підготовка працівників Національної поліції України у частині забезпечення та захисту прав дітей».

Запитання для обговорення:

- *Чи відрізняються загальні правила настання відповідальності дітей у разі вчинення ними протиправних дій у мережі інтернет?*
- *Чи необхідно і чому враховувати Керівні принципи Ради Європи щодо правосуддя, дружнього до дітей, у випадках вчинення дітьми протиправних дій в мережі інтернет?*
- *Які із вашого досвіду найбільш поширені протиправні дії вчиняють діти у мережі інтернет?*

До уваги тренера/тренерки!

Слід нагадати учасникам, що втягнення неповнолітнього в правопорушення є обтяжуючою адміністративну відповідальність обставиною (п.3 ч.1 ст.35 КУпАП).

3. Вправа «Легально чи нелегально?»

Мета: формування вміння ідентифікувати протиправні дії, які вчиняються дітьми в мережі інтернет.

Час: 20 хв.

Необхідні матеріали: Додаток 1.10.2.2, фліпчарт та аркуші для фліпчарту, маркери або мультимедійне обладнання.

Хід проведення:

Тренер/тренерка по черзі зачитує ситуації із Додатка 1.10.2.2 та запрошує учасників відповісти на питання: «*Чи легальні ці дії?*», яке доцільно записати формулювання питання на аркуші фліпчарту або вивести на екран.

Тренер/тренерка пропонує такі варіанти для відповіді: «Так», «Ні», «Не знаю».

До уваги тренера/тренерки!

Можна підготувати завчасно аркуші з відповідними написами та розмістити їх в різних частинах аудиторії. Після зачитування тренером/тренеркою ситуації здобувачі освіти мають перейти до того аркуша, який відповідає їхній думці.

За результатами відповідей тренер/тренерка просить учасників з різними позиціями навести аргументи чи коментарі, чому вони обрали саме таку відповідь. Після цього тренер/тренерка коментує ситуацію, використовуючи матеріали з Додатка 1.10.2.2 та переходить до наступної ситуації.

До уваги тренера/тренерки!

Можна дану вправу провести також за допомогою об'єднання учасників у групи та надання кожній із них однієї ситуаційної задачі з Додатка 1.10.2.2. Завдання для груп: протягом десяти хвилин визначити, чи є в цій ситуації протиправне діяння. Якщо так, то як можна кваліфікувати це діяння, та настання якого виду відповідальності передбачено за його вчинення? Після закінчення часу на роботу в групах учасники протягом двох хвилин презентують свої напрацювання. Тренер/тренерка надає коментарі відповідно до матеріалів, які містяться у Додатку 1.10.2.2.

Запитання для обговорення:

- *Яка ситуація була найскладніша, а яка найлегша для обговорення? Чому?*
- *Чи можете ви навести приклади вчинення протиправних дій дітьми в мережі інтернет з власної практики?*

4. Робота в групах «Відповідальність за вчинення дітьми протиправних дій в мережі інтернет»

Мета: формування вміння ідентифікувати протиправні дії дітей в мережі інтернет та здійснювати їх кваліфікацію.

Час: 40 хв.

Необхідні матеріали: Додаток 1.10.2.3, кулькові ручки.

Хід проведення:

Тренер/тренерка об'єднує учасників у чотири групи та надає кожній із них ситуаційну задачу із Додатка 1.10.2.3. Завдання для груп: протягом десяти хвилин проаналізувати ситуацію,

визначити, склад яких правопорушень наявний у цій ситуації, та яку кваліфікацію можна надати з врахуванням наявної в умові інформації.

Після завершення роботи в групах учасники презентують напрацювання до п'яти хвилин, а тренер/тренерка доповнює їхні відповіді, спираючись на судові рішення, з яких були взяті фабули.

До уваги тренера/тренерки!

Під час підготовки до заняття можна самостійно знайти фабули протиправних діянь, які були вчинені дітьми в мережі інтернет чи за допомогою мережі інтернет», або скористатись запропонованими у Додатку 1.10.2.3. Для пошуку судових рішень доцільно використовувати Єдиний державний реєстр судових рішень: https://reyestr.court.gov.ua/.

Запитання для обговорення:

- *Чи погоджуєтесь ви з кваліфікацією діянь та рішеннями судів у розглянутих справах?*
- *Чи були у вашій практичній діяльності або особистому житті випадки, пов'язані із вчиненням дитиною протиправних дій в мережі інтернет?*

Тестові питання до заняття:

1. За якою статтею якого нормативно-правового акту притягаються до відповідальності батьки або законні представники дитини у разі вчинення малолітньою дитиною кібер-булінгу?

А) 173-4 КУпАП;

Б) 184 КУпАП;

В) 166 ККУ;

Г) не притягаються до відповідальності в такому випадку.

2. Розміщення дитиною особистих фотографій на власній сторінці в соціальній мережі може бути протиправною дією?

А) ні;

Б) так, якщо батьки не дали дозвіл на публікацію;

В) так, якщо вони містять заборонений контент;

Г) складно відповісти.

3. За загальним правилом адміністративній та кримінальній відповідальності підлягають особи, які досягли на момент вчинення правопорушення:

А) 14 років;

Б) 16 років;

В) 18 років;

Г) 21 року.

4. Який принцип Комітету міністрів Ради Європи щодо правосуддя, дружнього до дітей, включає в себе надання належної уваги думці дітей:

А) захисту від дискримінації (недискримінації);

Б) участі;

В) гідності;

Г) верховенства права.

5. Під час втягнення дітей у протиправну діяльність доросла особа може здійснювати психологічний вплив через:

А) переконання;

Б) залякування;

В) підкуп;

Г) всі відповіді правильні.

Ключі-відповіді:

1. А; 2. В; 3. Б; 4. Б; 5. Г.

Додаток 1.10.2.1

Відповідальність за вчинення дітьми протиправних дій в мережі інтернет

Для виокремлення правопорушень, за які діти підлягають притягненню до юридичної відповідальності, слід передусім враховувати **вік настання відповідальності**. За загальним правилом адміністративній та кримінальній відповідальності підлягають особи, які досягли на момент вчинення правопорушення *шістнадцятирічного віку*. Однак за низку правопорушень, визначених в ч. 2 ст. 22 ККУ, можуть підлягати кримінальній відповідальності діти у віці *з 14 до 16 років*. У разі, якщо протиправне діяння щодо дитини було вчинено особою, яка не досягла віку відповідальності, *до адміністративної відповідальності можуть бути притягнені батьки останньої або особи, що їх замінюють,* відповідно до:

- ч. 3 ст. 184 КУпАП – у випадку вчинення неповнолітніми віком від чотирнадцяти до шістнадцяти років адміністративних правопорушень, крім булінгу;
- ч. 4 ст. 184 КУпАП – у випадку вчинення неповнолітніми, які не досягли віку настання кримінальної відповідальності, діянь, що містять ознаки кримінального правопорушення;
- ч. 3 ст. 173-4 – у випадку вчинення дитиною віком до 16 років булінгу, зокрема із застосуванням засобів електронних комунікацій;
- ч. 4 ст. 173-4 – у випадку вчинення дитиною віком до 16 років булінгу, зокрема із застосуванням засобів електронних комунікацій, групою осіб або повторно.

До неповнолітніх, які вчинили суспільно-небезпечні діяння, що підпадають під ознаки діяння, передбаченого ККУ, у віці, коли їм виповнилося 11 років, але до досягнення віку, з якого згідно з кримінальним законом можливе настання кримінальної відповідальності, судами застосовуються примусові заходи виховного характеру, передбачені ст.105 ККУ.

Серед адміністративних правопорушень, які можуть вчиняти діти у мережі інтернет або за допомогою засобів ІКТ, є:

- поширювання неправдивих чуток (ст. 173-1 КУпАП);
- вчинення домашнього насильства (ст. 173-2 КУпАП);
- булінг (цькування) учасника освітнього процесу (ст. 173-4 КУпАП);
- мобінг (цькування) працівника (ст. 173-5 КУпАП).

До уваги тренера/тренерки!

Враховуючи категорію учасників, слід проаналізувати, чи доцільно приділити окрему увагу питанням кібербулінгу, як правопорушенню, яке доволі часто вчиняється дітьми в мережі інтернет. Якщо учасники необізнані з цього питання та мають відповідний запит, доцільно більш детально розкрити це питання.

Кібербулінг – це один із різновидів булінгу (цькування).

Відмінності кібербулінгу від офлайн-булінгу зумовлюються особливостями інтернет-середовища: анонімністю, можливістю підмінити ідентичність, охоплювати велику аудиторію одночасно (особливо дієво для поширення пліток), тероризувати та тримати у напрузі постраждалу особу будь-де і будь-коли. Кібербулінг може мати ширші масштаби та поширюватися швидше, аніж в офлайн-середовищі. Кібербулінг може здійснюватися у будь-який час – вдень чи вночі, порушуючи межі «простору», який донедавна вважався безпечним, і може мати анонімний характер.

Відповідно до *Рекомендації для директивних органів щодо захисту дитини в цифровому середовищі,* **кібербулінг** – це навмисна агресивна дія, що неодноразово

вчиняється групою осіб або окремою особою за допомогою цифрових технологій та спрямована проти особи, який важко захиститися. Зазвичай передбачає «*використання цифрових технологій та інтернету для розміщення чутливої інформації про будь-кого, навмисне поширення відомостей особистого характеру, небажаних світлин або відео, надсилання повідомлень із погрозами чи образами (електронною поштою, у форматі миттєвого обміну повідомленнями, в чатах і текстових повідомленнях), поширення пліток та неправдивої інформації про постраждалу особу або навмисне виключення її з онлайн-спілкування*». Може відбуватися безпосередньо (в чатах або текстових повідомленнях), у межах спільноти з обмеженим доступом (розсилання постів та дратівливих повідомлень за списком електронних адрес) або ж у громадському доступі (наприклад створення сайтів для навмисного знущання з постраждалої особи).

Ознаки кібербулінгу такі самі, як і у булінгу загалом:

- систематичність (повторюваність) діяння;
- наявність сторін – кривдник (булер), потерпілий (постраждала від булінгу), спостерігачі (за наявності);
- дії або бездіяльність кривдника, наслідком яких є заподіяння психічної та/або фізичної шкоди, приниження, страх, тривога, підпорядкування потерпілого інтересам кривдника та/або спричинення соціальної ізоляції потерпілого.

Якщо висловлювання, поширення картинок тощо в мережі інтернет щодо певної особи сприймається нею як жарт, не мають систематичного характеру та не спричиняють негативних емоційних реакцій, такі дії не вважаються кібербулінгом.

Сторони кібербулінгу та їхні ролі.

Кривдник (булер) – учасник освітнього процесу, зокрема малолітня чи неповнолітня особа, яка вчиняє булінг (цькування) щодо іншого учасника освітнього процесу.

Потерпілий (постраждала особа) – учасник освітнього процесу, зокрема малолітня чи неповнолітня особа, щодо якої було вчинено булінг (цькування).

Спостерігач – свідки та (або) безпосередні очевидці випадку булінгу (цькування).

Відповідальність за вчинення булінгу передбачена ст.173-4 КУпАП.

Стаття 173⁴. Булінг (цькування) учасника освітнього процесу

Булінг (цькування), тобто діяння учасників освітнього процесу, які полягають у психологічному, фізичному, економічному, сексуальному насильстві, зокрема із застосуванням засобів електронних комунікацій, що вчиняються стосовно малолітньої чи неповнолітньої особи або такою особою стосовно інших учасників освітнього процесу, внаслідок чого могла бути чи була заподіяна шкода психічному або фізичному здоров'ю потерпілого, –

тягне за собою накладення штрафу від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або громадські роботи на строк від двадцяти до сорока годин.

Діяння, передбачене частиною першою цієї статті, вчинене групою осіб або повторно протягом року після накладення адміністративного стягнення, –

тягне за собою накладення штрафу від ста до двохсот неоподатковуваних мінімумів доходів громадян або громадські роботи на строк від сорока до шістдесяти годин.

Діяння, передбачене частиною першою цієї статті, вчинене малолітніми або неповнолітніми особами віком від чотирнадцяти до шістнадцяти років, –

тягне за собою накладення штрафу на батьків або осіб, які їх замінюють, від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або громадські роботи на строк від двадцяти до сорока годин.

Діяння, передбачене частиною першою цієї статті, вчинене малолітньою або неповнолітньою особою віком від чотирнадцяти до шістнадцяти років, –

тягне за собою накладення штрафу на батьків або осіб, які їх замінюють, від ста до двохсот неоподатковуваних мінімумів доходів громадян або громадські роботи на строк від сорока до шістдесяти годин.

Неповідомлення керівником закладу освіти уповноваженим підрозділам органів Національної поліції України про випадки булінгу (цькування) учасника освітнього процесу –

тягне за собою накладення штрафу від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або виправні роботи на строк до одного місяця з відрахуванням до двадцяти процентів заробітку.

Серед кримінальних правопорушень, які можуть вчиняти діти у мережі інтернет або за допомогою ІКТ, є:

- несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану (стаття 114-2 ККУ);
- вчинення домашнього насильства (ст. 126-1 ККУ);
- порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163 ККУ);
- порушення авторського права і суміжних прав (ст. 176 ККУ);
- порушення недоторканності приватного життя (ст. 182 ККУ);
- розповсюдження порнографічних предметів, зокрема дитячої порнографії (ст. 301 – 301-1 ККУ);
- проведення видовищного заходу сексуального характеру за участю неповнолітньої особи (ст.301-2 ККУ);
- публічні заклики до агресивної війни або до розв'язування воєнного конфлікту (ст. 436 ККУ).

Перелік перерахованих правопорушень, безумовно, не є вичерпним.

Одним з факторів, які сприяють протиправним діям дітей в інтернеті, є вплив підбурювачів та організаторів з числа дорослих осіб, які самі прагнуть залишатися в стороні та уникнути кримінальної відповідальності. Слід пам'ятати, що за **втягнення неповнолітніх у протиправну діяльність** (як онлайн, так і офлайн) передбачена кримінальна відповідальність (ст. 304 ККУ). Під час втягнення дітей у протиправну діяльність доросла особа зазвичай здійснює фізичне насильство або психологічний вплив через:

- переконання (про можливість без покарання вчинити правопорушення, отримання певних благ, втіх, про романтизм та героїзм антигромадської, злочинної поведінки тощо);
- залякування (погроза нанесення побоїв, розголошення відомостей, що ганьблять особу, позбавлення певних благ тощо);

- підкупу (надання матеріальної винагороди, надання певних благ тощо);
- обману (надання неправдивої інформації, створення удаваних ілюзій та уявлень);
- збудження почуття помсти (стимуляція фізичної та духовної розправи тощо);
- збудження заздрості або інших почуттів (переконання отримати або придбати певну річ, зайняти престижне місце в групі тощо);
- обіцянки придбати або продати крадене, надання порад про спосіб скоєння або укриття слідів правопорушення, розпиття спиртних напоїв з дітьми з метою полегшення схиляння їх до скоєння злочину та інше.

Протидія залученню дітей російськими військовими до протиправної діяльності через інтернет є ще одним сучасним викликом. Непоодинокі випадки, коли діти готові виконувати протиправні дії, зокрема адміністрування каналів в соціальних мережах та месенджерах, що підбурюють їх до протиправних, зокрема хуліганських дій (як, наприклад, ЧВК «Редан»), або спрямованих на доведення дитини до самогубства (як, наприклад, «Синій кит»). Також вони можуть надавати координати розташування українських військових тощо.

Які б протиправні дії не вчинила дитина, зокрема з використанням мережі інтернет, під час здійснення провадження слід враховувати Керівні принципи Комітету міністрів Ради Європи щодо правосуддя, дружнього до дітей, 2010 р. До основоположних принципів поводження з дитиною, закріплених у Керівних принципах Комітету Ради Європи щодо правосуддя, дружнього до дітей, зокрема належать такі:

✔ *Принцип захисту від дискримінації (недискримінації).*

Права дитини повинні забезпечуватись без жодної дискримінації за ознакою статі, раси, кольору шкіри, етнічного походження, віку, мови, релігії, політичних або інших переконань, національного або соціального походження, соціально-економічного стану, статусу одного з їхніх батьків або обох батьків, належності до національних меншин, майнового стану, народження, сексуальної орієнтації, ґендерної ідентичності або іншого статусу. У разі потреби повинні бути гарантовані конкретні засоби захисту та допомоги дітям у більш уразливому становищі, наприклад, дітям мігрантів, дітям-біженцям та дітям-шукачам притулку, дітям без супроводу, дітям з інвалідністю, безпритульним дітям, а також дітям ромського походження та дітям, які перебувають у спеціалізованих закладах.

✔ *Принцип найкращих інтересів дитини.*

Держави зобов'язані гарантувати ефективне здійснення прав дитини, щоб їхні найкращі інтереси мали першочергову увагу в усіх аспектах, що стосується або зачіпає їхні інтереси. В оцінці інтересів залучених або постраждалих дітей важливо приділяти належну увагу їхнім поглядам та думкам. Хоча судові органи мають кінцеву компетенцію і відповідальність за прийняття остаточного рішення, держави повинні спрямувати спільні зусилля на створення міждисциплінарних підходів для оцінки найкращих інтересів дітей під час процедур, пов'язаних з ними. Водночас найкращі інтереси всіх дітей, які беруть участь в тій самій процедурі чи справі, мають бути окремо оцінені та збалансовані з метою узгодження можливого конфлікту інтересів дітей.

✔ *Принцип участі.*

Слід поважати право всіх дітей на отримання інформації про свої права, а також на доступ до правосуддя та консультування. Діти мають право бути почутими під час розглядів, що стосуються або впливають на їхнє життя. Це включає надання належної уваги думкам дитини з урахуванням її зрілості та можливих труднощів у спілкуванні, щоб забезпечити ефективну участь. Хоча це не означає, що їхній думці завжди будуть відповідати, принцип участі вима-

гає серйозного та поважного розгляду їхньої позиції, залежно від віку, зрілості та обставин справи, з урахуванням процесуальних норм національного законодавства. Діти повинні вважатися повноправними носіями прав і мати змогу здійснювати всі свої права з урахуванням їхньої здатності формувати власні погляди та обставин справи. Замість того, щоб занадто швидко припускати, що дитина не може сформувати думку, державам слід вважати, що у дитини насправді є така здатність. Водночас державам не рекомендується встановлювати стандартизовані вікові обмеження.

- *Принцип гідності.*

До дітей слід ставитися з обережністю, чутливістю, справедливістю та повагою під час будь-якої процедури або справи. Особливу увагу потрібно приділяти їхній особистій ситуації, добробуту та конкретним потребам, забезпечуючи повагу до їхньої фізичної та психологічної недоторканності. Таке ставлення повинно бути надане незалежно від того, як вони вступають в контакт із судовим або не судовим розглядом, або іншими заходами, а також незалежно від їхнього правового статусу і потенціалу під час будь-якої процедури або справи. Діти не повинні зазнавати катувань, нелюдського або такого, що принижує гідність, ставлення чи покарання.

- *Принцип верховенства права.*

Принцип верховенства права має повною мірою застосовуватися як до дітей, так і до дорослих. Елементи належної правової процедури, такі як принципи законності та пропорційності, презумпція невинності, право на справедливий судовий розгляд, право на юридичну допомогу, право на доступ до судів і право на апеляцію, повинні бути гарантовані дітям так само, як і дорослим, і не можуть бути зведені до мінімуму або заборонені під приводом захисту «кращих інтересів дитини». Це стосується всіх судових, позасудових і адміністративних розглядів. Діти повинні мати право на доступ до відповідних незалежних та ефективних механізмів розгляду скарг.

Додаток 1.10.2.2

Ситуація 1.

Хлопець час від часу розміщує відеоролики порнографічного змісту на своїй сторінці в соціальній мережі.

Ситуація 2.

Хлопець розмістив на своїй сторінці в соціальній мережі скріншот листування з однокласником, який ділився з ним своїми почуттями до дівчини з тієї самої школи.

Ситуація 3.

Хлопець підібрав пароль від скайпу свого знайомого та від його імені веде листування з іншими людьми.

Ситуація 4.

Дівчина розмістила фотографії зі святкування 2-річчя своєї молодшої сестри. На фото в домі її батьків були зображені її дорослі родичі, молодші брати та сестри. Фотографії «лайкнули» понад 80 друзів.

Ситуація 5.

Неповнолітня дівчина поширює образливі чутки щодо малолітньої в інтернет-мережі «Інстаграм».

Матеріал для тренера

Ситуація 1.

В ситуації йдеться про судову справу, що проходила в Україні у 2012 році. Дії обвинуваченого було кваліфіковано як розповсюдження продукції порнографічного характеру, тобто як злочин, передбачений статтею 301 Кримінального кодексу України.

Ситуація 2.

В ситуації йдеться про порушення права на приватність, зокрема конфіденційність кореспонденції та можливе розголошення певних обставин приватного життя іншої особи, що є порушенням статей 31 і 32 Конституції України. За такі протиправні діяння може наставати цивільно-правова відповідальність, можливе призначення компенсації завданої моральної шкоди за рішенням суду.

Ситуація 3.

В ситуації йдеться про втручання у роботу комп'ютерних систем, що є злочином, за яке передбачається кримінальна відповідальність за статтею 361 Кримінального кодексу України.

Ситуація 4.

В ситуації йдеться про порушення права на приватність через поширення інформації про сімейне життя (конфіденційної інформації) без згоди особи. Стаття 32 Конституції України забороняє такі дії, а Закон України «Про захист персональних даних» передбачає судовий захист від незаконного збирання та поширення персональних даних, незалежно від носія та форми зберігання інформації.

Ситуація 5.

В ситуації йдеться про вчинення булінгу, що є адміністративним правопорушенням, за яке передбачається адміністративна відповідальність за статтею 173-4 Кодексу України про адміністративні правопорушення.

Всі ситуації, наведені у Додатку, відображають реальні дії і є або кримінальними правопорушеннями (1, 3), або адміністративним правопорушенням (5), або порушеннями прав людини (2, 4), за які може наставати цивільно-правова відповідальність у вигляді відшкодування потерпілій стороні завданої моральної шкоди у розмірі, визначеному судом.

Додаток 1.10.2.3

Фабула 1

Вчителька історії в КЗ «Ліцей №5» заявила, що учень 8-Б класу періодично надсилає їй домашні завдання з образливими підписами: «дура», «крейзі», «ракушка» та картинки із побажанням смерті. Пізніше з такими ж підписами він почав відправляти домашні завдання і класному керівникові.

Інформація для тренера/тренерки:

Рішення суду міститься за посиланням: https://reyestr.court.gov.ua/Review/110140657.

Дії учня кваліфіковані за ч. 3 ст. 173-4 «Булінг (цькування) учасника освітнього процесу» КУпАП.

Фабула 2

27 лютого 2023 року близько 22:23, 15-річний Петро, перебуваючи за місцем проживання, у месенджері Телеграм підбурював учасників субкультури «Редан» до масових зборів.

Інформація для тренера/тренерки:

Рішення суду міститься за посиланням: https://reyestr.court.gov.ua/Review/109916653.

Дії кваліфіковані за ч. 1 ст. 184 «Невиконання батьками або особами, що їх замінюють, обов'язків щодо виховання дітей» КУпАП.

Фабула 3

14-річний Максим, перебуваючи вдома, в навчальній групі в месенджері Телеграм виклав фото порнографічного характеру.

Інформація для тренера/тренерки:

Рішення суду міститься за посиланням: https://reyestr.court.gov.ua/Review/102808845.

Дії Максима кваліфіковані поліцейськими за ст. 173 КУпАП, на матір склали протокол за ч. 3 ст. 184. Суд закрив провадження у зв`язку з відсутністю в її діях складу адміністративного правопорушення.

Фабула 4

Неповнолітня Оксана, перебуваючи за місцем свого фактичного місця проживання, діючи умисно, з корисливих мотивів, з метою протиправного збагачення, створила та адмініструвала акаунти на сайті, де розмістила декілька фіктивних оголошень про продаж собак породи «Коргі» та «Мопс». Не маючи водночас на меті виконати взяті на себе зобов`язання, ввела в оману декілька осіб, під час спілкування через месенджер Вайбер, заволоділа їхніми грошовими коштами, які отримала електронним переказом на банківську картку на своє ім`я, як завдаток за собак породи «Коргі» та «Мопс».

Інформація для тренера/тренерки:

Рішення суду міститься за посиланням: https://reyestr.court.gov.ua/Review/111777999.

Дії кваліфіковані за ч. 1 та ч. 2 ст. 190 «Шахрайство» ККУ.

ТЕМА 1.11. Особливості проведення опитування дитини різного віку, яка постраждала від насильства в кіберпросторі

Заняття 1.11.1. Психологічні особливості дітей різного віку, які необхідно враховувати під час проведення опитування

Мета: оцінити рівень знань вікових особливостей дітей, сформувати розуміння щодо особливостей комунікації з дитиною.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Асоціація	Обговорення	20 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, стікери, кулькові ручки
2.	Вікові особливості дітей	Робота в групах	40 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, Додатки 1.11.1.1 та 1.11.1.2
3.	Як встановити контакт з дитиною	Мозковий штурм	20 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери або мультимедійне обладнання
4.	Правда чи міф	Гра	10 хв	Кольорові аркуші (зеленого та червоного кольору) на кожного учасника/учасницю, Додаток 1.11.1.3

ХІД ЗАНЯТТЯ

1. Обговорення «Асоціація»

Мета: актуалізація та визначення знань учасників про психологічні особливості дітей.

Час: 20 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, стікери, кулькові ручки.

Хід проведення:

Тренер/тренерка роздає кожному учаснику/учасниці по стікеру та просить написати на ньому характеристику дітей або асоціацію, яка виникає на слово «Дитина». Після цього учасники по черзі виходять та закріплюють свої стікери на аркуші паперу для фліпчарту, пояснюючи свою асоціацію.

До уваги тренера/тренерки!

Якщо є час, можна роздати учасникам/учасницям ще по одному стікеру, на якому вони мають зазначити асоціацію до словосполучення «Дитина у контакті із законом».

Підсумовуючи відповіді учасників, тренеру/тренерці варто зауважити: «*Діти – це особлива категорія. Кожний віковий період має свої особливості, на які ми маємо спиратись, щоб забезпечити комфортні психологічні умови для дитини з метою сприяти її розповіді про обставини події*».

2. Робота в групах «Вікові особливості дітей»

Мета: сформувати розуміння особливостей дітей відповідно до віку.

Час: 40 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додатки 1.11.1.1, 1.11.1.2.

Хід проведення:

Тренер/тренерка об'єднує учасників у три групи та просить обговорити вікові особливості дітей за схемою, зазначеною в Додатку 1.11.1.1:

група 1 – діти дошкільного віку (від 3 до 6 років);

група 2 – діти молодшого шкільного віку (від 6 до 10 років);

група 3 – підлітки (від 10 до 18 років).

Після завершення виконання завдання по одному представнику/представниці від кожної групи презентують напрацьовані результати до п'яти хвилин.

Запитання для обговорення:

- *З чим вдалось легко впоратися під час визначення вікових особливостей?*
- *Що було складно визначити?*
- *Навіщо нам знати про вікові особливості дітей? Як ми їх застосовуємо?*
- *Які висновки можна зробити за результатами виконаної вправи?*

До уваги тренера/тренерки!

Підбиваючи підсумки результатів напрацювань груп, можна використовувати додаткову інформацію із Додатка 1.11.1.2.

3. Мозковий штурм «Як встановити контакт з дитиною»

Мета: ознайомити учасників з методикою «Зелена кімната», сформувати розуміння встановлення контакту із дитиною.

Час: 20 хв.

Необхідні матеріали: фліпчарт, аркуші альбому для фліпчарту, маркери або мультимедійне обладнання.

Хід проведення:

Тренер/тренерка зазначає: *«Під час взаємодії з дитиною, зокрема, яка зазнала насильства, важливо дотримуватись такої формули: «Безпечний дорослий + Безпечне місце = Дитина у безпеці». Тож спробуймо зрозуміти, що в себе включає кожен компонент формули».*

До уваги тренера/тренерки!

Можна занотувати формулу на аркуші для фліпчарту або підготувати презентацію та вивести на екран.

Запитання для обговорення:

- *Що в себе включає поняття «Безпечний дорослий»?*
- *Що в себе включає поняття «Безпечне місце»?*
- *Що в себе включає поняття «Дитина у безпеці?*

Після завершення обговорення тренер/тренерка зазначає:

*«**Безпечне місце»** означає, що:*

- *воно є передбачуваним для дитини.*

Дитина отримує повну інформацію про те, де й чому вона знаходиться, і що з нею відбуватиметься; які вона має права, який приблизно час займе опитування, де вона може задовольнити власні потреби. Наприклад, якщо це місце – нове для неї, їй слід показати, де можна випити води, сходити в туалет тощо. Також дитина має знати, хто буде присутній на опитуванні та з якою метою. Так вона володітиме повним об'ємом інформації і розумітиме, що й як відбуватиметься. Така поінформованість додаватиме їй спокою і впевненості, що дасть змогу свідчити про події, які з нею сталися.

- *унеможливлює будь-які прояви насильства над дитиною, тиск на неї, підвищення голосу, погрози, примус, маніпулювання тощо – неприпустимі;*
- *відповідає усім вимогам, необхідним для роботи з дітьми (зручні дитячі меблі, декілька іграшок, олівці, папір тощо). Там відсутні сторонні, помірна температура повітря і комфортне освітлення.*

***«Безпечний дорослий»** – це особа, яка під час опитування перебуває поруч з дитиною, а також:*

- *знає, розуміє та враховує її психологічний стан, вікові й індивідуальні особливості;*
- *взаємодіє з нею з позиції рівності, зокрема фізичної, підтримуючи контакт очі в очі, а не зверху донизу;*
- *вміє розпізнавати актуальні потреби дитини та стабілізувати її психоемоційний стан під час опитування та загалом;*
- *забезпечує дотримання усіх процедур, необхідних для захисту прав та найкращих інтересів дитини;*
- *ініціює контакт, виявляє доброзичливість, надає підтримку.*

До уваги тренера/тренерки!

Емпатійна поведінка безпечного дорослого передбачає розуміння власних емоцій та чутливе сприйняття емоційних реакцій дитини, що ґрунтується на прийнятті її почуттів і потреб, на делікатному спілкуванні з нею зрозумілою для дитини мовою, без оцінювання й осуду, з повагою, турботою, дотриманням її прав та врахуванням інтересів.

***«Дитина у безпеці»** означає, що дитина:*

- *розуміє відсутність прямої загрози, спроможна усвідомлювати те, що відбуватиметься;*
- *відчуває захищеність та фізично перебуває у стані спокою;*
- *розуміє, де вона знаходиться й до кого може звернутися по допомогу та підтримку;*
- *знає, що в будь-який момент може попросити перерву, щоби вийти в туалет або випити води;*
- *може безпечно пригадувати і відтворювати події минулого та вільно виявляти власні емоції;*
- *розуміє, що поруч – безпечний, а отже уважний та турботливий дорослий;*
- *з власної ініціативи вносить корективи до своїх свідчень (наприклад «ой, це було не вихідного дня, я була тоді вдома, бо в школі скасували заняття»).*

4. Гра «Правда чи міф»

Мета: закріплення знань про вікові особливості дітей, сприяння зміні стереотипних поглядів учасників.

Час: 10 хв.

Необхідні матеріали: кольорові аркуші (зеленого та червоного кольору) на кожного учасника/учасницю, Додаток 1.11.1.3.

Хід проведення:

Тренер/тренерка зазначає: «*А тепер, спробуймо закріпити інформацію, яку ми з вами розбирали у попередніх вправах. У вас є дві картки – зелена та червона. Я буду зачитувати твердження, якщо ви з ним погоджуєтесь, то підіймаєте зелений аркуш, якщо не погоджуєтесь – червоний. За бажанням можете обґрунтувати власну відповідь*», та по черзі зачитує твердження із Додатка 1.11.1.3.

Тестові питання до заняття:

1. Діти – це…

А) категорія осіб, які часто фантазують про події, які з ними трапились;

Б) особи, які не мають суттєвих відмінностей від дорослих;

В) особлива категорія, кожний віковий період має свої особливості та потреби.

2. Особливістю відтворення підлітками обставин подій є:

А) описують подію через емоційну реакцію, тактильні відчуття, але плутають факти у розповіді у часовому проміжку;

Б) розповідають про обставини події через зіставлення історій;

В) мають труднощі із вербалізацією понять.

3. Безпечний дорослий…

А) може торкатись або обіймати дитину за бажанням;

Б) взаємодіє з дитиною, з урахуванням її потреб та інтересів;

В) особа, яка виконує функції суду.

4. Безпечне місце – це…

А) місце, яке є прогнозоване дитиною;

Б) місце суб'єктів, які захищають права дитини;

В) у дитини вдома.

5. Як впливає присутність батьків під час опитування/допиту дитини?

А) ніяким чином не впливає;

Б) впливає на користь підтримки дитини батьками, і тому вона може надати максимально детальну інформацію про обставини події;

В) у присутності батьків дитина орієнтується на їхню реакцію, що може вплинути на її свідчення та зменшити кількість важливих деталей про обставини події.

Ключі-відповіді: 1. В; 2. А; 3. Б; 4. А; 5. В.

Додаток 1.11.1.1

Схема до вправи «Вікові особливості»

Характеристика	Вікова особливість
Провідна діяльність	
Орієнтування у просторі та часі	
Особливості запам'ятовування та відтворення подій	
Способи відтворення обставин подій	
Здатність надавати описову характеристику	
Якими знаннями володіє	
Що вміє дитина	
Які потреби є у дитини (відповідно до віку)	

Додаток 1.11.1.2

Вікові особливості дітей

Діти дошкільного віку (від 3 до 6 років).

Орієнтація у часі.

Діти дошкільного віку запам'ятовують емоційно забарвлені події, такі як свято, день народження, Новий рік, змагання тощо. Вони орієнтуються у часі доби та порах року через такі описи, як «було світло» (ранок) або «було темно» (ніч), «на вулиці було холодно» (зима) тощо.

Опис події.

Діти дошкільного віку покладаються на тактильні відчуття та пояснюють явища через дії, підкріплюючи їх тактильними рухами. Водночас у них можуть виникати труднощі з вербалізацією та поясненням подій, які відбулися. Діти у цьому віці здатні описати предмети та їх властивості, відповідаючи на запитання: «якого кольору?», «якої форми?», «як працює?», «що ним роблять?» До кінця дошкільного віку в них з'являється тенденція до узагальнення і встановлення зав'язків. Наприклад, діти можуть описувати процеси, що відбулися з ними, у вигляді гри та правил, які пропонував дорослий, але ще не здатні зрозуміти та пояснити ці дії.

Молодший шкільний вік (від 6 до 10 років).

Орієнтація у часі.

Дитина молодшого шкільного віку орієнтується в часі та днях тижня, але не завджи усвідомлює самові проміжки; може згадати події, які відбулись кілька тижнів тому.

Опис події.

У дітей молодшого шкільного віку розвивається абстрактне мислення, здатність логічно міркувати, уважно слухати, спостерігати, запам'ятовувати, аналізувати і робити висновки. Вони можуть визначати позицію предметів (праворуч, попереду, позаду тощо). Дитина молодшого шкільного віку точно сприймає предмети, події і взаємозв'язок між ними, якщо можна дослідити їх особисто. Дитина молодшого дошкільного віку здатна описувати час події, орієнтуючись на розкдлад і шкільний графік занять, кажучи, наприклад, «це було після уроків», «на уроці фізкультури», «коли я йшла на танці», «я робила уроки і тут…». У дитини молодшого дошкільного віку актуалізується робота всіх аналізаторів, тому вона відтворює події, описуючи те, що бачила, що чула, яке було на дотик та на смак.

Підлітки (від 10 до 18 років).

Орієнтація у часі.

Діти підліткового віку достатньо добре орієнтуються у часі, однак частіше, ніж дорослі, помиляються у визначенні відстані, тривалості часу, послідовності дій.

Опис події.

Підлітки здатні описувати події через емоційні реакції та тактильні відчуття, але можуть плутають факти у розповіді за часовими проміжками. Підлітки спочатку виражають свої почуття та переживання, а потім за допомогою дорослого можуть деталізувати подію. Вони можуть здійснювати опис події, покладаючись на власні переживання, наприклад: «Мені було страшно, я не могла закричати та втекти, ноги були як ватні». У процесі розповіді підліток часто слідує не за перебігом подій, а своїм асоціаціям. Проте його не можна квапити, обривати чи договорювати за нього. Якщо підліток перебуває у стані збудження або пригнічений через подією злочину чи затримання, доцільно обмежитися допитом лише в обсязі, необхідному

для невідкладних слідчих дій, а детальний допит варто відкласти на деякий час. Важливим є етап запитань і відповідей під час допиту, тому доцільно ґрунтуватись на асоціаціях, які відповідають обсягу знань та колу інтересів допитуваного. Підліткам легше впізнати предмет або місце, ніж описати його. Також підлітки частіше помиляються у визначенні відстані, тривалості часу та послідовності дій. Вони можуть використовувати терміни і поняття, які вживають дорослі, нерідко перекручуючи їх та не розуміючи справжнього змісту, водночас соромлячись запитати чи попросити пояснень.

Додаток 1.11.1.3

Твердження:

1. Діти дошкільного віку вважаються найщирішими свідками (правда).

Пояснення: оскільки у дітей ще не сформовані причинно-наслідкові зв'язки, вони відтворюють те, що бачать.

2. Діти самі провокують насильство у відповідь на їхню поведінку (міф).

Пояснення: діти, враховуючи свої вікові особливості та вразливості, не можуть бути відповідальними за вчинений над ними акт.

3. Діти молодшого шкільного віку відчувають сором, що може призвести до небажання розповідати про обставини події (правда).

Пояснення: на відміну від дітей дошкільного віку, у молодших школярів вже з'являється почуття сорому, що може стати причиною відмови від розповідей про обставини події.

4. Під час взаємодії з дитиною важливо враховувати її вікові особливості (правда).

Пояснення: врахування вікових особливостей сприяє формуванню у дитини довіри до вас та відчуття безпеки.

5. Безпечне місце створює дорослий (правда).

Пояснення: показуючи дитині приміщення та розказуючи, де що знаходиться, дорослий допомагає дитині їй відчувати себе у безпеці.

6. Якщо підліток під час надання свідчень плутає факти – це означає, що він/вона говорить неправду (міф).

Пояснення: плутання фактів є характерним для підліткового віку; однієї ознаки недостатньо, щоб робити висновок, що дитина не пережила досвід насильства.

7. Не має значення, чи дитина розповідає обставини події у присутності батьків, чи ні (міф).

Пояснення: це має суттєве значення, оскільки у присутності батьків дитина може відчувати себе скутою і зазнавати їхнього впливу. В найкращих інтересах дитини бажано проводити опитування дитини із застосуванням дружніх методик опитування дітей, наприклад методики «Зелена кімната» або моделі «Барнахус».

Заняття 1.11.2. Алгоритм проведення опитування дитини, яка постраждала від насильства у кіберпросторі

Мета: надати інформацію щодо методики «Зелена кімната», сформувати розуміння особливостей формулювання запитань, залежно від вікових особливостей дітей.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Особливості проведення опитування дитини	Мозковий штурм	30 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.11.2.1
2.	Підготовка питань до опитування дитини	Робота у групах	20 хв	Аркуші паперу для фліпчарту, маркери, Додаток 1.11.2.2
3.	Акваріум	Гра	40 хв	Додаток 1.11.2.2 та напрацьовані групами питання із попередньої вправи

ХІД ЗАНЯТТЯ

1. Мозковий штурм «Особливості проведення опитування дитини»

Мета: актуалізація знань на формування уявлення та розуміння процедури проведення опитування дитини.

Час: 30 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 1.11.2.1.

Хід проведення:

Тренер/тренерка зазначає: «*Для того, щоб зрозуміти, як має відбуватися процес опитування, спочатку важливо сформувати уявлення, як цей процес має виглядати. Отже, спробуймо разом поміркувати над тим, як має відбуватися цей процес. Уявіть, що ви маєте провести опитування дитини, постраждалої від насильства у кіберпросторі, та з'ясувати деталі обставин подій».*

Запитання для обговорення:

- *Із чого почнете опитування?*
- *Як побудуєте опитування дитини?*

Тренер/тренерка фіксує відповіді учасників на фліпчарті, після чого підсумовує: «*Одним із головних завдань, окрім отримання від дитини інформації про обставини події, є збереження самостійності її розповіді з мінімізацією стороннього впливу. Також ми повинні пам'ятати, що в процесі опитування важливо не нашкодити дитині додатковим травмуванням і реалізувати всі завдання, поєднуючи їх юридичне та психологічне значення. Попередня підготовка, поетапність процесу опитування важливі для фахівця/фахівчині, який/яка його проводитиме, тож він/вона має зібрати необхідну інформацію для побудови взаємодії з дитиною, наприклад, застосувавши методику «Зелена кімната», яка полягає в отриманні достовірних свідчень в умовах мінімізації негативного впливу на дитину та*

недопущення її повторного травмування. Ця методика, окрім згаданої вище формули, передбачає 5 фаз опитування:

- попередню;
- вступну;
- фазу вільної розповіді;
- детальних запитань;
- завершальну.

Тож тепер попрошу вас об'єднатися у 5 груп, відповідно до фаз, та обговорити, в чому полягає ваша фаза».

Після завершення роботи у групах учасники презентують свої напрацювання, а тренер/тренерка підбиває підсумок, використовуючи інформацію із Додатка 1.11.2.1.

До уваги тренера/тренерки!

Залежно від категорії учасників та рівня їх підготовки, для виконання завдання можна їм дати посилання на Методичні рекомендації щодо організації роботи з дітьми за методикою «Зелена кімната» для слідчих та ювенальних поліцейських.

2. Робота у групах «Підготовка питань до опитування дитини»

Мета: сприяти формуванню навичок підготовки запитань дитині, яка постраждала від насильства у кіберпросторі.

Час: 20 хв.

Необхідні матеріали: аркуші паперу для фліпчарту, маркери, Додаток 1.11.2.2.

Хід проведення:

Тренер/тренерка об'єднує учасників у три групи та просить, відповідно до кейсів, викладених у Додатку 1.11.2.2, сформувати перелік запитань до опитування дитини. Після завершення виконання групами завдання один представник/представниця презентує напрацьовані результати до п'яти хвилин на групу.

Запитання для обговорення:

- *Чи складно було створювати перелік запитань?*
- *Із чим вдалося легко впоратися?*
- *Які висновки можна зробити за результатами виконаної вправи?*

3. Гра «Акваріум»

Мета: сприяти формуванню навичок ставлення запитань дитині.

Час: 40 хв.

Необхідні матеріали: Додаток 1.11.2.2 та напрацьовані групами питання із попередньої вправи.

Хід проведення:

Тренер/тренерка пропонує по одному бажаючому із груп відпрацювати навички ставлення запитань. Тренер/тренерка грає роль дитини, а учасники – інтерв'юєра. У процесі відпрацювання опитування дитини інші учасники фіксують:

- що вдалось інтерв'юєру/інтерв'юерці найкраще;
- які питання допомагали розповідати, а які ускладнювали розповідь дитини;

- які питання були не коректними та чому;
- як би інакше вони поставили запитання дитині;
- які питання додатково поставили б дитині;
- чи вдалось досягнути поставленої мети інтерв'юєру/інтерв'юерці (дізнатись детально обставини події).

Після кожного інтерв'юєра учасники групи надають зворотний зв'язок.

До уваги тренера/тренерки!

Головним завданням під час отримання зворотного зв'язку для інтерв'юєра є отримання підтримки від групи, тому, якщо група це зробила на недостатньому рівні, тренер/тренерка має зробити це самостійно, висловивши вдячність за сміливість та за роботу тощо.

Головним завданням групи у процесі спостереження – це сформувати спостережливість та вміння оперативно аналізувати поставлені запитання. Адже учасники не завжди будуть проводити самостійно опитування дитини, цю функцію може бути передано психологу, тому у процесі опитування їм буде необхідно корегувати та направляти психолога щодо елементів подій, які необхідно з'ясувати.

Після завершення виконання вправи відбувається загальне обговорення, під час якого учасники за бажанням висловлюють свою думку.

Запитання для обговорення:

- *Чим корисною була вправа?*
- *Які висновки ви можете зробити за результатами виконання цієї вправи?*

Тестові питання до заняття:

1. Завдання використання методики «Зелена кімната» поліцейськими:

А) отримання достовірних свідчень дитини в умовах, дружніх до дитини, та з дотриманням принципів правосуддя, дружнього до дитини;

Б) мінімізація та недопущення повторної травматизації дитини, блокування гострих стресових реакцій, що можуть виникнути під час її допиту/опитування;

В) обидві відповіді правильні.

2. Попередня фаза опитування дитини полягає:

А) у детальному вивченні інформації про дитину та складанні переліку запитань до опитування;

Б) у встановленні контакту з дитиною та роз'ясненню їй ролей учасників, які беруть участь в опитуванні;

В) деталізації розповіді дитини про обставини події.

3. Фаза вільної розповіді передбачає:

А) ставлення додаткових запитань, які необхідно встановити;

Б) дитина самостійно, у власному темпі розповідає про обставини події;

В) встановлення контакту з дитиною та ведення бесіди на вільні теми.

4. У процесі складання переліку запитання для опитування дитини важливо орієнтуватись на:

А) вікові особливості дитини;

Б) особливості батьків;

В) власний розсуд.

5. Яке питання НЕ рекомендується ставити дитині під час опитування?

А) Де?

Б) Коли?

В) Чому?

Ключі-відповіді:

1. В; 2. А; 3. Б; 4. А; 5. В.

Додаток 1.11.2.1

Фази опитування дитини

1. **Попередня фаза** охоплює дії, що передують контакту з дитиною, і полягає в детальному вивченні інформації, яка так чи інакше її стосується, – вік, індивідуальні та сімейні особливості, обставини подій (хто що й де вчиняв, за яких обставин, як виявлено тощо). Якщо це не перше опитування дитини, то необхідно детально ознайомитись з матеріалами попереднього, висновками психологів, експертів та інших спеціалістів, якщо такі були. На цьому етапі також важливо скласти перелік запитань, які ви поставите дитині під час опитування, з урахуванням його мети, а саме: які вікові й індивідуальні особливості характерні для дитини, яку інформацію необхідно отримати від неї, які ознаки події є кваліфікуючими, чи є й які саме невідповідності в показаннях та поясненнях щодо них.

2. **Вступна фаза** є безпосереднім знайомством з дитиною, коли пояснюють її права, розказують, що відбуватиметься, яка роль осіб, присутніх на опитуванні. Суттєвою складовою частиною фази є встановлення контакту з дитиною. Вкрай важливо, щоб усі учасники опитування (якщо їх декілька) відповідали критеріям безпечного дорослого. Перед тим, як розпочати опитування, важливо чітко роз'яснити дитині, що вона може не знати відповідей на всі запитання або може не розуміти деяких з них. У такому разі слід пояснити дитині, що це цілком нормально, і що вона може про це вільно повідомити. Також важливо сказати, що вона має право не відповідати на запитання, якщо того не бажає. Слід установити, чи в змозі дитина відрізнити правду від обману, та пояснити їй важливість говорити саме правду так, як вона це розуміє.

3. **Фаза вільної розповіді** є етапом, коли дитина розповідає про перебіг подій довільно у характерному для неї темпі. Важливо розпочати цю фазу із запитання, яке спонукатиме до розмови. Не слід перебивати дитину, навіть якщо вона відхиляється від суті справи. Не слід виправляти, уточнювати та/або корегувати сказане нею, а також порівнювати з інформацією з інших джерел. Це може обмежити вільне викладення спогадів, завадить перебігу думок або змінить порядок окремих деталей, згадуваних дитиною.

4. **Фаза детальних запитань** має на меті деталізацію подій, описаних дитиною під час фази вільної розповіді, та їх впорядкування для з'ясування обставин справи. Дорослий має подбати про те, щоби перехід до фази детальних запитань відбувся плавно, природно і не викликав занепокоєння у дитини, пов'язаного з тим, що вона може не впоратися з відповідями. Слід пам'ятати, що цей етап повинен мати таку форму розмови, яка обирається з урахуванням вікових та психологічних особливостей дитини. Слід пояснити, що заради безпеки дитини дорослі хочуть дізнатися більше про подію, а тому може бути й більше запитань. Це робиться з метою доповнення, пояснення, уточнення і узгодження сказаного дитиною. Питання для деталізації можна формулювати в порядку від першого до четвертого: Де? Коли? Як? Хто?

Важливо! Питання, які починаються з «Чому», «Навіщо», НЕ застосовувати!
Зауважимо, що на етапі детальних запитань спочатку зосереджуються на інформації, яку надає дитина, і лише згодом – на даних, отриманих з інших джерел.

5. **Заключна фаза** – підсумкова, на якій дитина зазвичай відчуває себе розслабленою, і цьому є пояснення. На психологічному та фізичному рівнях вона витрачає багато сил на згадування та виклад інформації, пов'язаної з подіями. Психіка намагається від цього вивільнитись, аби дитина надалі могла гармонійно розвиватися. У розповіді про подію задіяні всі канали сприйняття та відтворення інформації: думки, спогади, емоції, а також фізичні відчуття в тілі внаслідок пережитого та поведінка в період, коли усе відбувалося. Полегшення настає після «опрацювання» події. Навіть якщо дитина плакала або була

засмученою, на рівні тіла її напруга зменшилася. Зовні можна спостерігати, як вона схилила голову, сперлася на стінку стільчика. Як сиділа мовчки, а потім захотіла погратися або поїсти. Ці та подібні ознаки свідчать про природне відновлення взаємодії зі світом, що є цілком нормальним. Однак буває й так, що дитина після надання свідчень стає знервованою, неспокійною через свої висловлювання або через їх оцінку іншими. Слід дати їй час заспокоїтися, показати, що ви розумієте її емоції. Важливо подякувати за взаємодію та готовність розповісти все, що знає, навіть якщо в її показаннях не буде суттєвої інформації для справи, подякувати за допомогу і готовність спілкуватися. Завершити бесіду слід на нейтральній темі, щоби знизити напругу дитини. Заключна фаза є важливою для захисту психіки, тому слід переключити дитину з тяжких для неї спогадів на повсякденне життя, спитавши, що вона робитиме після зустрічі, куди піде, з ким зустрінеться, тощо.

Додаток 1.11.2.2

Кейси до вправи

Група 1

Дівчина, 16 років. Було виявлено, що вона створювала дитячий порнографічний контент та розповсюджувала його у мережі Телеграм-каналу. У процесі відпрацювання матеріалу працівниками кіберполіції було встановлено, що кошти за продані матеріали отримував її 20-річний хлопець. Під час обшуку в квартирі, де проживає дівчинка, вона розповіла, що створювала контент за допомогою фотошопу. Сама дівчина кошти від свого хлопця або «покупців» не отримувала. Кошти надходили її хлопцю, оскільки у неї не було власної банківської картки.

Ви маєте провести опитування 16-річної дитини.

Запитання мають бути з урахуванням вікових та психологічних особливостей дитини. Передусім це стосується питань, які є предметом доказування:

1. Про час події.
2. Про місце події.
3. Про кількість, багатократність подій.
4. Про саму дитину, можливих співучасників.

Також можна використовувати таку схему запитань:

- Де?
- Коли?
- Хто?
- Що саме відбувалось/як?

Уникати питання «Чому?»

Група 2

Хлопець, 15 років. Коли йому було 14 років, у соціальній мережі познайомився із дівчиною. Вони певний час листувалися, після чого вона почала називати його своїм хлопцем. Надалі вона попросила надсилати його фото: спочатку звичайні фото, поступово переходячи до фото інтимного характеру (оголений торс, фото у білизні), потім фото його статевого органу, а далі відео, як він мастурбує. Якось, коли він сказав, що більше не буде цього робити, вона пригрозила, що викладе його фото в інтернеті. Після чого хлопець заблокував її. Через рік працівники кіберполіції виявили особу, яка здійснювала листування із неповнолітніми хлопцями у різних соціальних мережах. Так було виявлено потерпілого хлопця.

Ви маєте провести опитування 14-річного хлопця.

Запитання мають бути з урахуванням вікових та психологічних особливостей дитини. Передусім це стосується питань, які є предметом доказування:

1. Про час події.
2. Про місце події.
3. Про кількість, багатократність подій.
4. Про саму дитину, можливих співучасників.

Також можна використовувати таку схему запитань:

- Де?
- Коли?
- Хто?
- Що саме відбувалось/як?

Уникати питання «Чому?»

Група 3

Троє 14-річних дівчат П., Ж., С. із 9-го класу створили групу в Телеграм-каналі, в якій викладали відео дівчини К. 12-річного віку, 6-го класу, на якому міститься дитячий порнографічний контент. Контент створювався так: у групі надсилалось повідомлення із запитанням: «Що б ви хотіли, щоб К. зробила у наступному відео?», учасники групи писали свої варіанти, після чого С. писала К., що вона має знімати, та надіслати їй. Коли мама К. у телефоні дівчини побачила ці відео, вона запитала, для чого вона їх знімала, на що К. відповіла, що так їй сказала зробити С. та надіслати їй. Після цього батьки К. звернулись із заявою до кіберполіції.

Ви маєте провести опитування 12-річної дівчини.

Запитання мають бути з урахуванням вікових та психологічних особливостей дитини. Передусім це стосується питань, які є предметом доказування:

1. Про час події.
2. Про місце події.
3. Про кількість, багатократність подій.
4. Про саму дитину, можливих співучасників.

Також можна використовувати таку схему запитань:

- Де?
- Коли?
- Хто?
- Що саме відбувалось/як?

Уникати питання «Чому?»

ТЕМА 1.12. Взаємодія підрозділів поліції під час реагування на випадки онлайн-насильства над дітьми

Заняття 1.12.1. Взаємодія між підрозділами поліції під час реагування на випадки онлайн-насильства над дітьми

Мета: систематизувати знання учасників щодо повноважень різних підрозділів поліції та особливостей їх взаємодії під час реагування на випадки онлайн-насильства над дітьми.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Підрозділи поліції, які уповноважені на реагування на випадки онлайн-насильства над дітьми	Мозковий штурм	10 хв	Фліпчарт, аркуші для фліпчарту, маркери
2.	Роль підрозділів поліції у реагуванні на випадки онлайн-насильства над дітьми	Робота в групах	40 хв	Фліпчарт, аркуші для фліпчарту, маркери
3.	Алгоритм взаємодії поліцейських під час реагування на випадки онлайн-насильства над дітьми	Робота в групах	40 хв	Фліпчарт, аркуші для фліпчарту, маркери

ХІД ЗАНЯТТЯ

1. Мозковий штурм «Підрозділи поліції, які уповноважені на реагування на випадки онлайн-насильства над дітьми»

Мета: актуалізувати знання учасників щодо кола підрозділів поліції, уповноважених на реагування на випадки онлайн-насильства над дітьми.

Час: 10 хв.

Необхідні матеріали: фліпчарт, аркуші для фліпчарту, маркери.

Хід проведення:

Тренер/тренерка звертається до учасників із запитанням: «*Які підрозділи поліції, на вашу думку, можуть бути задіяні під час реагування на випадки онлайн-насильства над дітьми та з якою метою?*». Відповіді учасників слід зафіксувати на аркуші фліпчарту.

До уваги тренера/тренерки!

Слід звернути увагу учасників, що коло підрозділів поліції, які можуть бути задіяні до реагування на випадки онлайн-насильства над дітьми, досить широке. Водночас кожен підрозділ поліції має свої повноваження та свою роль у цій діяльності.

Запитання для обговорення:

- *Чи мали ви досвід реагування на випадки онлайн-насильства над дітьми? З якими підрозділами поліції ви тоді взаємодіяли?*
- *Від чого, на вашу думку, залежить ефективність взаємодії між підрозділами поліції під час реагування на випадки онлайн-насильства над дітьми?*

2. Робота в групах «Роль підрозділів поліції у реагуванні на випадки онлайн-насильства над дітьми»

Мета: систематизувати знання учасників щодо повноважень різних підрозділів поліції щодо реагування на випадки онлайн-насильства над дітьми.

Час: 40 хв.

Необхідні матеріали: фліпчарт, аркуші для фліпчарту, маркери.

Хід проведення:

Тренер/тренерка об'єднує учасників у чотири групи, кожна з яких має проаналізувати роль одного із підрозділів поліції стосовно реагування на випадки онлайн-насильства над дітьми за напрямами: *запобігання/профілактики; притягнення до відповідальності; надання допомоги постраждалій дитині*:

група 1 – підрозділи ювенальної превенції/служба освітньої безпеки;

група 2 – підрозділи кіберполіції;

група 3 – підрозділи дільничних офіцерів поліції/поліцейських офіцерів громади;

група 4 – підрозділи слідства/дізнання.

Для роботи в групах учасники можуть використовувати як власні знання та досвід, так і нормативно-правові акти, які регламентують діяльність підрозділів поліції.

Час на роботу в групах – 15 хвилин, презентація напрацювань груп – до п'яти хвилин.

Запитання для обговорення:

- *Чи можемо ми виокремити підрозділ, який відіграє найважливішу роль у реагуванні на випадки онлайн-насильства над дітьми?*
- *Який підрозділ поліції має серед завдань завчасне інформування населення про появу нових кіберзлочинів?*
- *До завдань якого підрозділу поліції належить профілактична діяльність, спрямована на запобігання вчиненню дітьми правопорушень, зокрема онлайн, виявлення причин і умов, які цьому сприяють, вжиття в межах своєї компетенції заходів для їх усунення?*
- *Сприяння іншим підрозділам Національної поліції у запобіганні, виявленні та припиненні кримінальних правопорушень, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є завданням якого підрозділу поліції?*
- *Які підрозділи поліції організовують роботу з дітьми за методикою «Зелена кімната»?*

До уваги тренера/тренерки!

У разі проведення заняття в межах курсів підвищення кваліфікації або службової підготовки, доцільно дати учасникам достатньо часу для обміну власним досвідом взаємодії з іншими підрозділами поліції.

3. Робота в групах «Алгоритм взаємодії поліцейських під час реагування на випадки онлайн-насильства над дітьми»

Мета: відпрацювати можливі алгоритми взаємодії поліцейських різних підрозділів під час реагування на випадки онлайн-насильства над дітьми.

Час: 40 хв.

Необхідні матеріали: фліпчарт, аркуші для фліпчарту, маркери.

Хід проведення:

Тренер/тренерка об'єднує учасників у п'ять груп, які протягом десяти хвилин мають обговорити та зобразити на аркушах альбому для фліпчарту алгоритм взаємодії поліцейських під час реагування на випадки онлайн-насильства щодо дітей:

Група 1 – до шкільного офіцера поліції після профілактичного заходу щодо безпеки в інтернеті підійшов учень 6-го класу та повідомив, що його друг хоче вийти із групи «Синій кит», проте адміністратор групи погрожує завдати шкоди його батькам та молодшій сестрі у такому разі.

Група 2 – до дільничного офіцера поліції звернулась мама учениці 5-го класу, якій в месенджері Вайбер систематично надходять з різних облікових записів повідомлення на кшталт: «Я все всім розкажу», «Зустрічаємось у парку о 18.00», «Ти жахлива подруга».

Група 3 – до поліцейського ювенальної превенції під час батьківських зборів у закладі освіти звернулась мати учня 8-го класу з повідомленням про власну стурбованість поведінкою сина, який останнім часом знаходиться в пригніченому настрої, по ночам «зависає» в телефоні, а коли вона погрожує забрати телефон, у сина починається істерика, він кричить, що йому тоді «кінець, він мусить бути завжди на зв'язку».

Група 4 – до поліцейського ювенальної превенції звернулась мати, яка виявила у телефоні 10-річної доньки її оголені фото та фото оголеного статевого органу невідомого чоловіка.

Група 5 – до чергової частини відділу поліції звернулась мати 7-річної Софії, яка повідомила, що однокласниця її доньки в загальній групі класу пише на адресу доньки образливі слова та надала як докази близько трьох скріншотів повідомлень.

До уваги тренера/тренерки!

Під час підготовки до заняття можна обрати інші ситуації. Доцільно, щоб кейси були реальні та тренер/тренерка міг/могла пояснити, чим закінчилися ситуації, над якими працювали учасники.

Час на презентацію напрацювань групи та обговорення – до п'яти хвилин.

Запитання для обговорення:

- *Від чого залежить ефективність взаємодії між підрозділами поліції під час реагування на випадки онлайн-насильства щодо дітей?*
- *Чи впливає особистісний фактор на реагування на випадки онлайн-насильства щодо дітей? Як?*

Тестові питання до заняття:

1. Який підрозділ поліції має серед завдань завчасне інформування населення про появу нових кіберзлочинів?

А) слідство/дізнання;

Б) ювенальна превенція;

В) кіберполіція;

Г) всі відповіді правильні.

2. До завдань якого підрозділу поліції належить профілактична діяльність, спрямована на запобігання вчиненню дітьми правопорушень, зокрема онлайн, виявлення причин і умов, які цьому сприяють, вжиття в межах своєї компетенції заходів для їх усунення?

А) ювенальна превенція;

Б) слідство/дізнання;

В) патрульна поліція;

Г) кіберполіція.

3. Які підрозділи поліції організовують роботу з дітьми за методикою «Зелена кімната» відповідно до Методичних рекомендацій, затверджених Головою Національної поліції України в 2021 році?

А) ювенальна превенція;

Б) слідство/дізнання;

В) кіберполіція;

Г) правильні відповіді А та Б.

4. Сприяння іншим підрозділам Національної поліції у запобіганні, виявленні та припиненні кримінальних правопорушень, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є завданням:

А) Укрбюро Інтерполу;

Б) кіберполіції;

В) слідства/дізнання;

Г) ювенальної превенції.

5. Основна роль органів Національної поліції у реагуванні на ситуації онлайн-насильства щодо дітей полягає у:

А) притягненні правопорушників до відповідальності;

Б) запобіганні та профілактиці онлайн-насильства щодо дітей;

В) наданні допомоги та підтримки постраждалій дитині;

Г) всі відповіді правильні.

Ключі-відповіді:

1. В; 2. А; 3. Г; 4. Б; 5. Г.

Заняття 1.12.2. Взаємодія підрозділів поліції з іншими суб'єктами під час реагування на випадки онлайн-насильства щодо дітей

Мета: сформувати у учасників розуміння важливості взаємодії з іншими суб'єктами під час реагування на випадки онлайн-насильства щодо дітей.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Коло суб'єктів, з якими взаємодіють поліцейські під час реагування на випадки онлайн-насильства щодо дітей	Мозковий штурм	20 хв	Фліпчарт, аркуші для фліпчарту, маркери або мультимедійне обладнання та доступ до інтернету
2.	Перешкоди для ефективного реагування на випадки онлайн-насильства щодо дітей та взаємодії між суб'єктами у цих випадках	Робота в парах Рольова гра	40 хв	Додаток 1.12.2.1, мотузка, ножиці; фліпчарт, аркуші для фліпчарту, маркери, кулькові ручки, блокноти або мультимедійне обладнання та доступ до інтернету
3.	Алгоритм взаємодії поліцейських з іншими суб'єктами під час реагування на випадки онлайн-насильства щодо дітей	Робота в групах	30 хв	Фліпчарт, аркуші для фліпчарту, маркери

До уваги тренера/тренерки!

Заняття з цієї теми доцільно проводити після вивчення учасниками/учасницями тем, присвячених питанням правових засад протидії онлайн-насильству щодо дітей та відповідальності за ці діяння.

ХІД ЗАНЯТТЯ

1. Мозковий штурм «Коло суб'єктів, з якими взаємодіють поліцейські під час реагування на випадки онлайн-насильства щодо дітей»

Мета: актуалізувати знання учасників щодо кола суб'єктів, з якими взаємодіють поліцейські під час реагування на випадки онлайн-насильства щодо дітей.

Час: 20 хв.

Необхідні матеріали: фліпчарт, аркуші для фліпчарту, маркери або мультимедійне обладнання та доступ до інтернету.

Хід проведення:

Тренер/тренерка звертається до учасників з питанням: «*З якими суб'єктами взаємодіють поліцейські під час реагування на випадки онлайн-насильства щодо дітей та у яких нормативно-правових актах визначено порядок їх взаємодії?*».

До уваги тренера/тренерки!

Відповіді учасників доцільно зазначати на аркуші паперу для фліпчарту.

Для виконання цієї вправи також можна використати Mentimetr або Slido.

Запитання для обговорення:

- *Чи відрізняється коло суб'єктів реагування на випадки онлайн-насильства над дітьми від випадків офлайн?*
- *Яким нормативно-правовим актом затверджено порядок забезпечення соціального захисту дітей, які зазнали онлайн-насильства?*
- *У який строк поліцейські мають повідомити службу у справах дітей про випадки виявлення онлайн-насильства щодо дітей? Який підрозділ поліції зобов'язаний це робити?*
- *Чи зобов'язаний керівник закладу освіти у разі отримання заяви або повідомлення про випадок кібербулінгу повідомити територіальний орган (підрозділ) Національної поліції України? Якщо так, у який строк?*

2. Робота в парах. Рольова гра. «Перешкоди для ефективного реагування на випадки онлайн-насильства щодо дітей та взаємодії між суб'єктами у цих випадках»

Мета: сприяти усвідомленню учасниками важливості небайдужого ставлення кожним із суб'єктів до постраждалих від онлайн-насильства дітей, наслідків упередженого ставлення з боку суб'єктів та необхідності руйнування наявних в суспільстві стереотипів.

Час: 40 хв.

Необхідні матеріали: Додаток 1.12.2.1, мотузка, ножиці; фліпчарт, аркуші для фліпчарту, маркери, кулькові ручки, блокноти або мультимедійне обладнання та доступ до інтернету.

Хід проведення:

На першому етапі тренер/тренерка об'єднує учасників у пари та просить кожну пару протягом п'яти хвилин занотувати у блокноті перелік перешкод, які можуть заважати ефективному реагуванню суб'єктів на випадки онлайн-насильства щодо дітей та взаємодії між ними у цих випадках.

Після закінчення часу на виконання завдання пари учасників по черзі називають по одній із зафіксованих перешкод, тренер/тренерка фіксує перелік на аркуші фліпчарту та звертається до учасників з пропозицією запропонувати способи усунення цих перешкод.

До уваги тренера/тренерки!

Альтернативне проведення цієї вправи може передбачити використання для опитування Mentimetr або Slido. В такому разі учасники/учасниці працюють не в парах, а надають індивідуальні відповіді.

На другому етапі тренер/тренерка зазначає: «*Стереотипи, які панують у суспільстві, є однією із найбільш розповсюджених перешкод для ефективного реагування на випадки насильства щодо дітей загалом та онлайн-насильства зокрема. Вони можуть заважати правильній оцінці ситуації та прийняттю необхідних заходів. Важливо усвідомлювати ці стереотипи та працювати на їх подолання, з метою створення безпечного середовища для всіх дітей*», після чого проводить вправу відповідно до Додатка 1.12.2.1.

До уваги тренера/тренерки!

Важливо наголосити, що не слід недооцінювати серйозність загрози для дитини у разі поширення її інтимного зображення в інтернеті. Навіть якщо вжити всіх заходів для видалення такого контенту, він може з'являтися знову, завдаючи дитині повторних травм. У 2018 році IWF відстежив, як часто з'являються зображення дитини, врятованої в 2013 році. За три місяці аналітики IWF зафіксували 347 появ зображення – 25 разів на тиждень. Щоразу, коли зображення дитини, яка зазнала насильства, потрапляє в мережу або завантажується злочинцем, ця дитина знову зазнає експлуатації. Постраждалі змушені жити з усвідомленням того, що ці зображення можуть існувати та поширюватись решту їхнього життя.

Щойно з'являється матеріал, що містить елементи сексуальних зловживань щодо дітей, або вебхостинг, де розміщено подібні матеріали, важливо якомога швидше видалити чи заблокувати контент. Невідкладне втручання з боку відповідних суб'єктів, а також їхнє небайдуже та неупереджене ставлення ще на етапі загроз є вкрай важливими. Проте ще більш важливим є формування в суспільстві нульової толерантності до будь-яких проявів насильства стосовно дітей як офлайн, так і онлайн.

Формування нульової толерантності до насильства у суб'єктів, які реагують на подібні випадки, є надзвичайно важливим. Міфи та стереотипи перешкоджають своєчасному виявленню та документуванню випадків насильства, що призводить до його посилення, подовження, формування відчуття безкарності у кривдника та безпорадності у постраждалої особи.

Запитання для обговорення:

- *Який вплив має стереотипне мислення суб'єктів на дитину, яка постраждала або може постраждати від насильства в кіберпросторі?*
- *З якими перешкодами у взаємодії з іншими суб'єктами ви стикаєтесь частіше всього?*
- *Якщо оцінювати рівень взаємодії за 10-бальною шкалою, на який бал ви оціните вашу взаємодію у питаннях реагування на випадки онлайн-насильства щодо дітей з: а) службою у справах дітей, б) центрами надання безоплатної правничої допомоги, в) центрами соціальних служб, г) судом, д) прокуратурою е) громадськими організаціями?*
- *Які фактори ви враховували під час оцінювання?*

До уваги тренера/тренерки!

Для більш наочного оцінювання поліцейськими рівня взаємодії між суб'єктами можна використати Mentimetr.

Якщо достатньо часу, доцільно вивести на екран та обговорити з учасниками перелік рекомендацій Комітету міністрів Ради Європи (CM/Rec (2018)7) державам-членам про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі щодо співпраці та координації діяльності суб'єктів на національному рівні:

- ✔ призначити орган влади або створити координаційний механізм для оцінки розвитку цифрового середовища, який може вплинути на права дитини, залучаючи дітей у процеси ухвалення рішень, та забезпечити належну увагу їхньої національної політики до таких змін;
- ✔ створити межі співпраці, процедури та процеси між компетентними державними органами, незалежними органами влади, громадянським суспільством і підприємствами, враховуючи їх відповідні ролі, обов'язки, можливості та ресурси;

- вимагати від платформ або постачальників послуг зв'язку швидких та ефективних заходів у відповідь на скарги щодо насильства чи жорстокого поводження між користувачами в інтернеті, а також забезпечити співпрацю з національними органами влади;
- залучати підприємства, такі як інтернет-провайдери і постачальники соціальних мереж, до активної участі у запобіганні та видаленні нелегального контенту згідно із законодавством чи рішеннями компетентних органів;
- заохочувати зацікавлені сторони громадянського суспільства як ключових каталізаторів у популяризації аспектів прав людини в цифровому середовищі. Вони мають активно відслідковувати, оцінювати і розвивати навички дітей, їхній добробут та інформаційну грамотність, а також ініціативи з навчання. Поширювати свої висновки й результати;
- заохочувати всі професійні засоби масової інформації, особливо, суспільні медіа до приділення уваги своїй ролі як важливого джерела інформації та рекомендацій для дітей, батьків, опікунів і вихователів щодо прав дитини, беручи до уваги міжнародні та європейські стандарти свободи слова та інформації й свободи медіа.

3. Робота в групах «Алгоритм взаємодії поліцейських з іншими суб'єктами під час реагування на випадки онлайн-насильства щодо дітей»

Мета: відпрацювати можливі алгоритми взаємодії поліцейських з іншими суб'єктами під час реагування на випадки онлайн-насильства над дітьми.

Час: 30 хв.

Необхідні матеріали: фліпчарт, аркуші для фліпчарту, маркери.

Хід проведення:

Тренер/тренерка об'єднує учасників у три групи, які протягом десяти хвилин мають обговорити в групах та зобразити на аркушах альбому для фліпчарту алгоритм взаємодії поліцейських з іншими суб'єктами під час реагування на випадки онлайн-насильства щодо дітей:

Група 1 – в закладі освіти класна керівниця виявила вчинення кібербулінгу з боку учениць 7-го та 8-го класу щодо учня 6-го класу місцевої школи.

Група 2 – до служби у справах дітей звернулась бабуся 6-річної дівчинки та повідомила, що онука «по секрету» розповіла їй, що вітчим, коли мама відсутня вдома, «знімає доросле кіно з нею у головній ролі», раніше їй це подобалось, проте іноді вітчим робить боляче. Мати дівчинки все заперечує й говорить, що донька все вигадала.

Група 3 – до поліції звернулась психолог місцевої школи, яка повідомила, що керівництво закладу освіти пропонує батькам перевести доньку в іншу школу, оскільки дівчинка надсилала свої інтимні фото хлопцю, з яким познайомилась в дитячому таборі, після чого ці фото з'явились у шкільних групах дітей в месенджері Телеграм. Батьки дівчини погодились забрати документи та перевести доньку до іншої школи. Доньку насварили та заборонили користуватись інтернетом. Психолог хвилюється, що дівчинка може вчинити суїцид.

Час на презентацію напрацювань групи – до п'яти хвилин.

Запитання для обговорення:

- *Які є важелі впливу на фахівців, які не виконують або неналежним чином виконують повноваження під час реагування на випадки онлайн-насильства щодо дітей?*

Тестові питання до заняття:

1. Забезпечення соціального захисту дітей, які зазнали онлайн-насильства, здійснюється у порядку, затвердженому:

А) Законом України «Про охорону дитинства»;

Б) Постановою Кабінету Міністрів України від 01.06.2020 року № 585;

В) Постановою Кабінету Міністрів України від 22.08.2018 року № 658;

Г) усі відповіді правильні.

2. У який строк поліцейські мають повідомити службу у справах дітей про випадки виявлення онлайн-насильства щодо дітей?

А) протягом десяти діб;

Б) протягом трьох діб;

В) не пізніше однієї доби;

Г) поліцейські не зобов'язані повідомляти службу у справах дітей.

3. У який строк керівник закладу освіти у разі отримання заяви або повідомлення про випадок кібербулінгу має повідомити територіальний орган (підрозділ) Національної поліції України?

А) протягом трьох робочих діб;

Б) строк такого повідомлення не визначений;

В) невідкладно у строк, що не перевищує однієї доби;

Г) він не зобов'язаний повідомляти поліцію.

4. Виявлення дитини, яка постраждала від онлайн-насильства, можливе через:

А) самозвернення дитини (в усній та (або) письмовій формі, зокрема із застосуванням засобів електронної комунікації) до будь-якого суб'єкта;

Б) звернення та надсилання повідомлень підприємств, установ, організацій незалежно від форми власності (в усній та (або) письмовій формі, зокрема із застосуванням засобів електронної комунікації) до будь-якого суб'єкта;

В) отримання інформації про дитину під час виконання професійних чи службових обов'язків посадовими особами, працівниками суб'єктів;

Г) усі відповіді правильні.

5. До суб'єктів, з якими взаємодіють підрозділи Національної поліції у разі вчинення онлайн-насильства щодо дитини, належать:

А) служба у справах дітей;

Б) установи освіти;

В) центри соціальних служб;

Г) усі відповіді правильні.

Ключі-відповіді:

1. Б; 2. В; 3. В; 4. Г; 5. Г.

Додаток 1.12.2.1

ВПРАВА «СТРУНА»

Тренер/тренерка пропонує семи учасникам взяти участь у вправі, яка призначена для ілюстрації досвіду постраждалих від онлайн-насильства дітей.

Після обрання учасників тренер/тренерка пропонує кожному з них обрати одне із посвідчень (*Додаток до вправи*) та просить їх стати в напівколо навколо людини, що грає роль постраждалої від онлайн-насильства дитини. Після чого тренер/тренерка роздає кожному учаснику/учасниці шматочок мотузки та просить «постраждалу дитину» тримати інший кінець кожної мотузки разом в її руках. «Постраждала» повинна бути зв'язана з кожною людиною, включно з кривдником, довжиною струни. Кривдник повинен бути останньою особою у півколі ліворуч від постраждалої дитини.

Тренер/тренерка просить «постраждалу дитину» прочитати її посвідчення особи та заяву. Потім вона звертається до особи праворуч від неї, яка читає свою відповідь, не називаючи свою роль. Інші учасники, які спостерігають, мають здогадатись, хто міг так відповісти. Після цього тренер/тренерка перерізає струну, що з'єднує цих двох осіб. Далі «постраждала дитина» звертається до наступної людини і повторює свій рядок: «Мій інтернет-знайомий погрожує розіслати мої інтимні фото всім знайомим, якщо я відмовлюсь надалі надсилати йому більш відверті зображення, ти можеш мені допомогти?». Так само кожна людина в півколі зачитує свою відповідь, а тренер/тренерка перерізає струну, що з'єднує їх. Це триває доти, поки не залишиться єдиний зв'язок, який залишився у постраждалої дитини і кривдника. Потім кривдник повідомляє свою особу та озвучує: «Я сказав, що ніхто тобі не повірить і не допоможе. Лише на мене ти можеш покластись».

Під час обговорення вправи тренер/тренерка запитує «постраждалу дитину», як вона почувалася після кожної відповіді. Можна поставити такі питання:

- чи відчували ви, що можете отримати допомогу?
- чи відчували ви, що хтось звинувачує вас у тому, що з вами сталося?
- чи відчували ви, що хтось звинувачував кривдника за його дії?

На загальну аудиторію слід поставити питання:

- чому нам вдавалось вгадувати, хто саме міг дати таку відповідь?
- які міфи та стереотипи лунали під час рольової гри?
- який синдром може сформуватись у постраждалої дитини в результаті, та як суб'єкти під час своєї діяльності можуть стикнутись з його проявом?

Додаток до вправи

ПОЛІЦЕЙСЬКА

Це ж тільки погрози.
Ось якщо викладе фото, то тоді і приходь.

СУСІДКА/СУСІД

Дорогенька, як то кажуть, моя хата скраю… Не хочу в чужому бруді нишпорити. Та й чого ти очікувала, якщо так відверто одягаєшся, напевно і фото відповідні сама в інтернет викладаєш.

ПОЛІЦЕЙСЬКИЙ

Ви впевнені, що хочете подати заяву про це? Доказів немає, злочинець незрозуміло де, це марне витрачання часу поки що. Якщо викладе фото, то ми його видалимо, не турбуйтесь. Та й фото в інтернеті – це не так вже й серйозно. Це ж не реальне насильство.

МАТИ/БАТЬКО

Я ж казала (-в), що твоє постійне «зависання» в інтернеті до добра не доведе. Не послухалась мене, тепер будеш знати. Мені ще цієї ганьби не вистачало. З цієї хвилини жодного доступу до інтернету! На майбутнє будеш думати, перш ніж щось робити.

ПОДРУГА/ДРУГ

Я думаю, ти перебільшуєш. Ти напевно щось не так зрозуміла. Та й навіть якщо так, подумаєш! Може з цього фото почнеться твоя кар'єра моделі. Та й фігура в тебе класна, чого соромитися.

ПОСТРАЖДАЛА ОСОБА

Мій інтернет-знайомий погрожує розіслати мої інтимні фото всім знайомим, якщо я відмовлюсь надалі надсилати йому більш відверті зображення, ти можеш мені допомогти?

КРИВДНИК

Я ж казав, що тобі ніхто не повірить і не допоможе. Лише на мене ти можеш покластись.

ІІ. ОСОБЛИВА ЧАСТИНА

2.1. ОСОБЛИВОСТІ ДІЯЛЬНОСТІ ПОЛІЦЕЙСЬКИХ ПІДРОЗДІЛІВ ПРЕВЕНТИВНОЇ ДІЯЛЬНОСТІ

ТЕМА 2.1.1. Інструменти виявлення шкідливого для дітей онлайн-контенту, зокрема насильства у кіберпросторі

Мета: навчитися здійснювати територіальний моніторинг інформаційних ресурсів для виявлення онлайн-контенту, шкідливого для дітей.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Як ефективно виявляти шкідливий контент на території обслуговування	Інформаційне повідомлення	20 хв	Мультимедійне обладнання, Додаток 2.1.1.1
2.	Територіальний моніторинг інформаційних ресурсів	Індивідуальна робота	70 хв	Комп'ютери для учасників з доступом до інтернету

ХІД ЗАНЯТТЯ

1. Інформаційне повідомлення «Як ефективно виявляти шкідливий контент на території обслуговування»

Мета: вивчити окремі способи швидкого виявлення контенту, деструктивного для дітей, в мережі інтернет, ознайомитись з роботою відповідних інструментів.

Час: 20 хв.

Необхідні матеріали: мультимедійне обладнання.

Хід проведення:

Тренер/тренерка звертається до учасників: «*Оскільки правоохоронні органи здебільшого працюють за територіальним принципом, перед ними постає проблема ефективної профілактики злочинності та виявлення протиправної активності на підконтрольній території. Протиправний контент, пов'язаний зі злочинами проти дітей, може бути розміщений на території, яка підпадає під юрисдикцію правоохоронного органу, а також зберігатися та розповсюджуватися із використанням ресурсів місцевих провайдерів. Водночас простий пошук у пошукових системах нерідко не дає бажаних результатів, оскільки значна частина протиправних ресурсів не індексується. В таких умовах правоохоронцям необхідно використовувати спеціалізоване програмне забезпечення. Крім того, важливо володіти інформацією про пул IP-адрес, асоційованих з місцевими провайдерами та операторами зв'язку*», після чого презентує інформацію із Додатка 2.1.1.1.

2. Індивідуальна робота «Територіальний моніторинг інформаційних ресурсів»

Мета: відпрацювати роботу інструментів пошуку неправомірного контенту на території функціонування правоохоронного органу.

Час: 70 хв.

Необхідні матеріали: комп'ютери для учасників з доступом до інтернету.

Хід проведення:

Тренер/тренерка звертається до учасників з проханням відкрити відповідний сайт, після чого пропонує виконати такі практичні завдання:

1) здійснити відпрацювання сервісів Network Scanner та Selka для діапазону IP-адрес поточного провайдера (дізнатися через зовнішню IP-адресу) та проаналізувати одержані дані;
2) зареєструватися у сервісі ICACCOPS;
3) за допомогою сервісів Google Alerts, Awario, Social Searcher та Visualping налаштувати спостереження з урахуванням поточних оперативно-службових завдань. Обґрунтувати свою відповідь.

Запитання для обговорення:

- *Що важливого ви сьогодні зрозуміли для себе?*
- *Чому новому навчились?*
- *Як будете використовувати набуті знання?*

Тестові питання до теми:

1. За допомогою якої з наведених утиліт можна визначити запущені на комп'ютері сервіси HTTP та FTP?

А) Microsoft Word;

Б) Microsoft Excel;

В) Network Scanner від LizardSystems;

Г) IBM i2 Analyst's Notebook.

2. Як називається банк даних, що містить інформацію про правопорушників і постраждалих від злочинів у сфері дитячої порнографії?

А) Europol's Sexual database;

Б) Interpol's International Child Sexual Exploitation (ICSE) database;

В) Child Sexual Abuse Victims database;

Г) Social Searcher database.

3. За допомогою якого ресурсу можна здійснити точкове спостереження за окремими сайтами або їх елементами?

А) Tracert;

Б) Whois;

В) VisualPing;

Г) Get.

4. Який з наведених сервісів дозволяє відстежувати завантаження контенту з пірінгових мереж за IP-адресою?

А) I KNOW (https://iknowwhatyoudownload.com/ru/peer/);

Б) Awario (https://awario.com/);

В) Mention (https://mention.com/en/);

Г) Social Searcher (https://www.social-searcher.com/).

5. Який альтернативний спосіб доставки сповіщень, крім каналу RSS, передбачає сервіс Google Alerts?

А) електронна пошта;

Б) месенджер;

В) хмарне сховище;

Г) підключення до мережної служби.

Ключі-відповіді:

1. В; 2. Б; 3. В; 4. А; 5. А.

Додаток 2.1.1.1

Як ефективно виявляти шкідливий контент на території обслуговування

Одним з простих та безоплатних (з некомерційною метою) застосунків, який дає змогу визначити запущені сервіси на певних IP-адресах, є програма Network Scanner від LizardSystems. За її допомогою серед іншого можна визначити запущені на комп'ютері сервіси HTTP та FTP (Рис. 1).

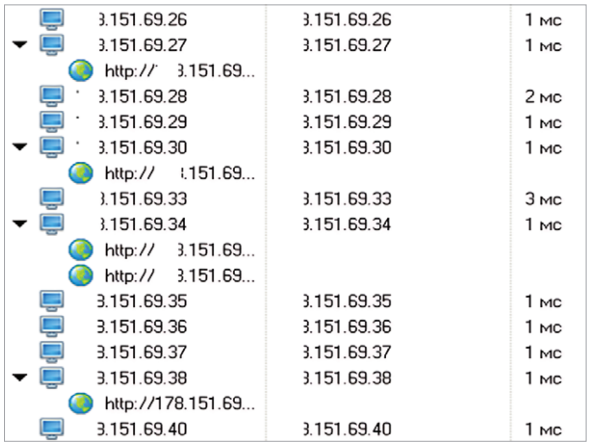


Рис. 1. Сканування діапазону IP-адрес

Більш докладний пошук за адресами, які становлять інтерес, можна здійснити за допомогою безоплатного парсера Selka (Рис. 2). Ця програма дасть змогу здійснити пошук інформації про те, де і коли зустрічалися визначені IP-адреси.

.23	www.bestchange.ru	/obmenpm-exchanger-2.html
.23	www.lookup-ip-address.info	/ip-address-range/:
.23	geoiplookup.net	/ip-addresses/(
.23	whoislookupdb.com	/iplist/:
9.24	**linuxcorral.com**	**/bitcoin/index.php**
.24	www.iplocationtools.com	/: 5.html
.24	geoiplookup.net	/ip-addresses/: :1.255

Рис. 2. Результат роботи парсера Selka

Крім застосування описаних методів, також необхідно здійснювати моніторинг завантажень протиправного контенту у своєму регіоні. Для цього у нагоді стануть сервіси I KNOW (https://iknowwhatyoudownload.com/ru/peer/) та більш професійний – ICACCOPS (Рис. 3).

IP	All Networks	Location	FOI	Last Seen (UTC)
193 8.69	B	UA, 26, Zaporozhye	99340	20.03.2017
77.9 186	B	UA, 26, Zaporozhye	85827	20.03.2017
91.1 .246	B	UA, 26, Zaporozhye	76222	19.03.2017
77.9 138	B	UA, 26, Zaporozhye	72321	20.03.2017
46.2 5.79	B E	UA, 26, Zaporozhye	59671	18.03.2017
89.2 103	B	UA, 26, Zaporozhye	57168	17.03.2017
194 .9	B	UA, 26, Zaporozhye	56474	19.03.2017
46.1 4.127	B	UA, 26, Zaporozhye	55803	20.03.2017
95.4 .4	B	UA, 26, Berdyansk	55459	15.03.2017
46.1 8.231	B	UA, 26, Zaporozhye	55308	18.03.2017

Рис. 3. Сервіс ICACCOPS

Для роботи з останнім потрібно зареєструватися з використанням службової електронної поштової скриньки за адресою https://www.icaccops.com/users/login.aspx (Рис. 4).

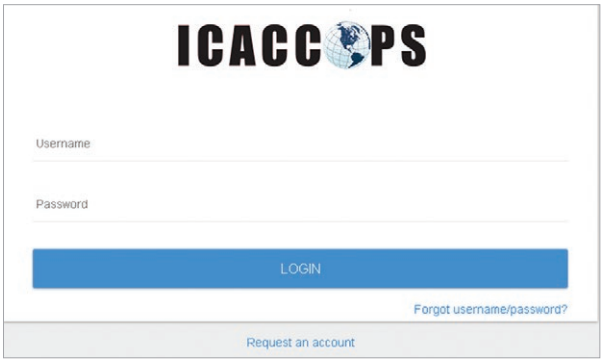


Рис. 4. Реєстраційна форма сервісу ICACCOPS

У результаті застосування цих сервісів серед іншого можна знайти IP-адреси, з яких завантажувалася (Рис. 5) та вивантажувалася дитяча порнографія.

FIRST SEEN (UTC)	LAST SEEN (UTC)	CATEGORY	TITLE	SIZE
5 квіт. 2023 р., 22:11:02	6 квіт. 2023 р., 11:20:17		LS Studios Collection - LS Land 16-22	7.09GB
5 квіт. 2023 р., 23:27:47	5 квіт. 2023 р., 23:27:47	Child porn	Incoming	
1 квіт. 2023 р., 14:35:52	6 квіт. 2023 р., 00:07:37	Child porn	ls-magazine	
30 бер. 2023 р., 16:36:14	6 квіт. 2023 р., 06:40:34		欧幼	74.47GB
30 бер. 2023 р., 10:35:27	6 квіт. 2023 р., 00:43:25	Child porn	хоум мейд намба три	
30 бер. 2023 р., 19:38:13	31 бер. 2023 р., 08:46:46		swordmaster	27.55GB

Рис. 5. Результат роботи сервісу «I KNOW»

Подібний до наведених проєкт Police2Peer функціонує і в Європолі. Більш докладно з ним можна ознайомитись за адресою: https://www.europol.europa.eu/partners-agreements/police2peer.

В Інтерполі також функціонує банк даних, що містить інформацію про правопорушників і постраждалих від злочинів у сфері дитячої порнографії (INTERPOL's International Child Sexual Exploitation (ICSE) database). На теперішній час ідентифіковано понад 32 тисяч відповідних осіб (https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database). Для використання цього банку даних (Рис. 6) потрібно отримати доступ до мережі Інтерпол через Департамент міжнародного поліцейського співробітництва Національної поліції України.

Рис. 6. Робота з ICSE database (за матеріалами сайту https://www.interpol.int/News-and-Events/News/2017/INTERPOL-network-identifies-10-000-child-sexual-abuse-victims)

Для виявлення нового тематичного контенту також можуть бути застосовані різні інструменти, зокрема https://www.google.com/alerts, користування яким не потребує облікового запису Google. Достатньо лише налаштувати параметри пошуку, зокрема із застосуванням спеціалізованих операторів, та зберегти сповіщення (Рис. 7). Якщо на позначку «Автоматично» клацнути двічі, то будуть обрані всі категорії джерел пошуку. Щоб виключити непотрібні, слід додати мінус («-»), а не «NOT».

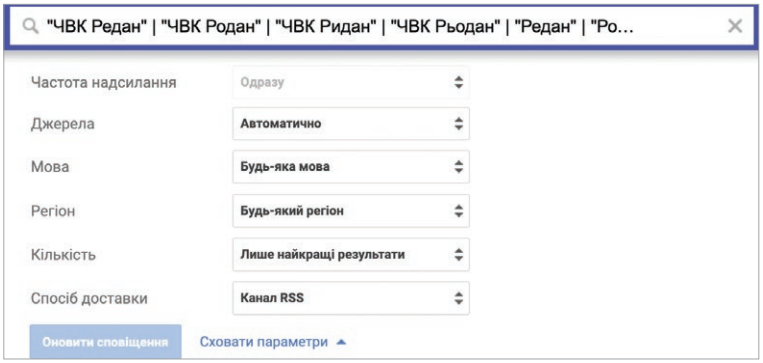


Рис. 7. Налаштування параметрів сповіщення Google Alerts

Серед альтернатив Google Alerts, які є безоплатними або мають пробний період використання, варто згадати:

- Awario (https://awario.com/)
- Mention (https://mention.com/en/)
- Talkwalker Alerts (https://www.talkwalker.com/alerts)
- Hootsuite (https://hootsuite.com/)
- Social Searcher (https://www.social-searcher.com/)
- Brand24 (https://brand24.com/).

Приклад налаштування сервісу Awario показано на Рис. 8, а результату пошуку сервісу Social Searcher – на Рис. 9.

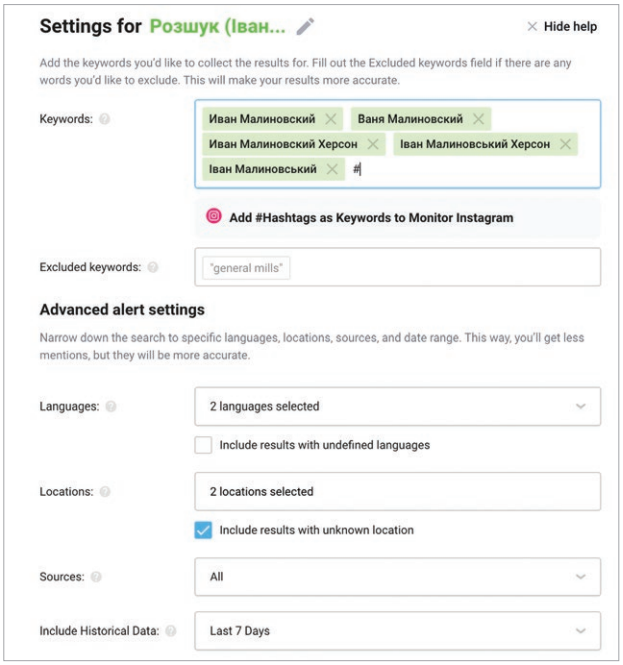


Рис. 8. Налаштування параметрів сервісу Awario

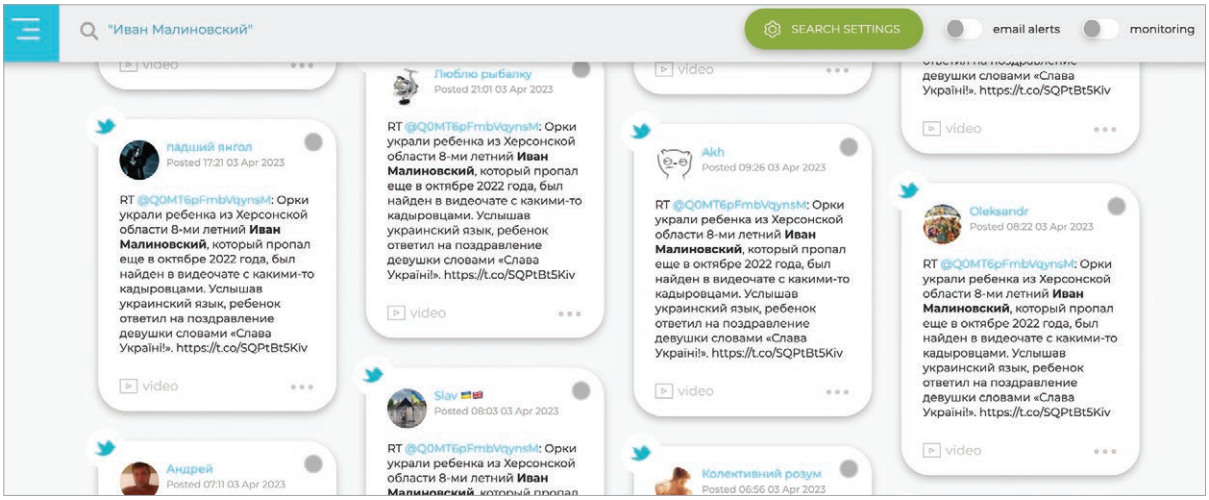


Рис. 9. Результат пошуку за допомогою сервісу Social Searcher

За потреби **точкового спостереження за окремими сайтами або їх елементами** слід скористатися **Visualping**(visualping.io), що дасть змогу налаштувати відстеження візуальних, текстових або програмних змін на певних ресурсах (Рис. 10).

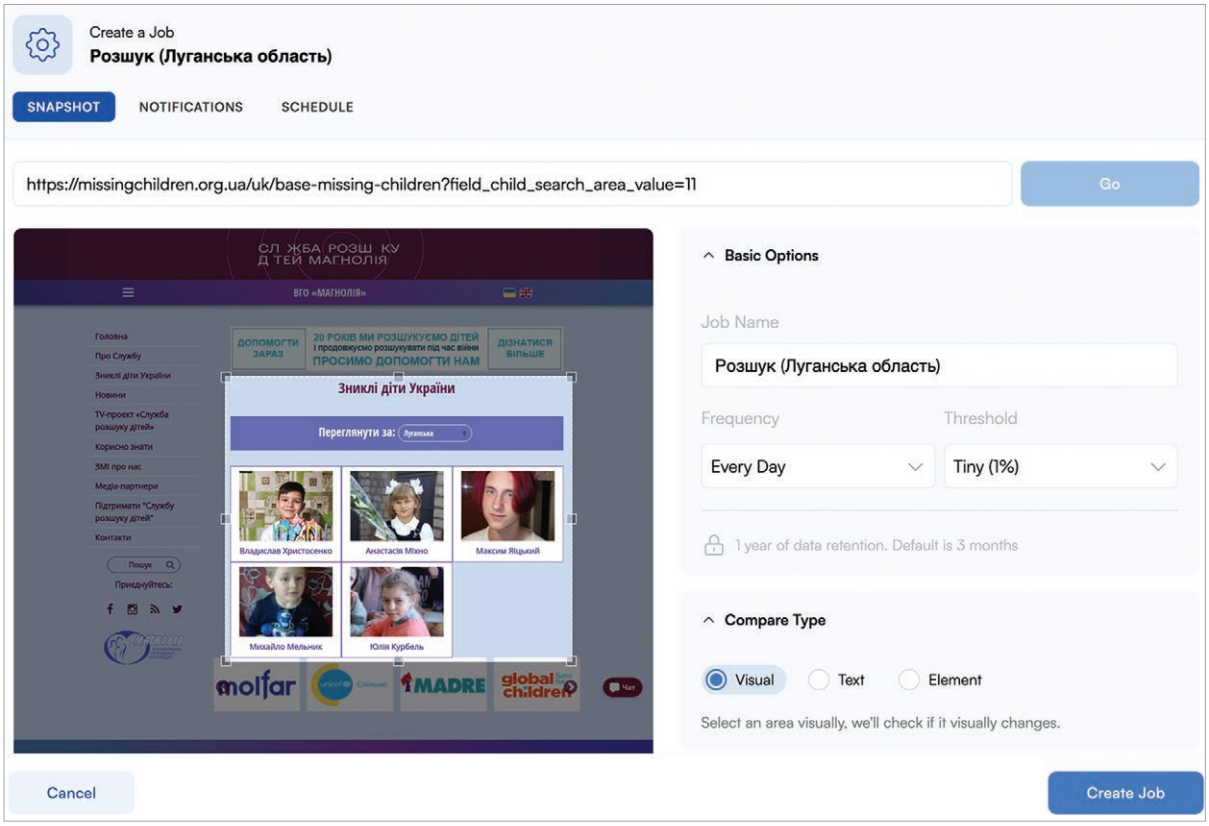


Рис. 10. Налаштування параметрів сервісу Visualping

ТЕМА 2.1.2. Профілактика втягнення дітей у протиправну діяльність в кіберпросторі

Заняття 2.1.2.1. Поняття та види профілактичної роботи. Особливості інтернет-залежності дитини

Мета: актуалізація знань учасників стосовно особливостей, рівнів та видів профілактики в діяльності поліцейських та змісту поняття інтернет-залежність дитини.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Профілактика: визначення та види	Інформаційне повідомлення Робота в групах	45 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 2.1.2.1.1
2.	Інтернет-залежність: що, чому, як?	Інтерактивна вправа	45 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 2.1.2.1.2

ХІД ЗАНЯТТЯ

1. Інформаційне повідомлення та робота в групах «Профілактика: визначення та види»

Мета: надати учасникам інформацію та актуалізувати знання щодо сутності поняття «профілактика», рівнів та видів профілактики.

Час: 45 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 2.1.2.1.1.

Хід проведення:

Тренер/тренерка ознайомлює учасників з поняттям «профілактика», видами та рівнями профілактики, відповідно до Додатка 2.1.2.1.1, а також наводить приклади (практичні кейси) проведення профілактичних заходів поліцейськими та іншими дотичними суб'єктами.

Після інформаційного повідомлення тренер/тренерка об'єднує учасників у три групи, кожна з яких отримує завдання – протягом десяти хвилин розкрити значення профілактики втягнення дітей у злочинну та іншу протиправну діяльність в кіберпросторі на певному рівні та визначити підрозділи поліції та інші органи й установи, які можуть бути задіяними у профілактичних заходах цього рівня:

група 1 – первинна;

група 2 – вторинна;

група 3 – третинна.

Результати роботи в групах учасники викладають на аркуші фліпчарту за зразком:

Вид профілактики

Зміст профілактичної роботи	Структурний підрозділ Національної поліції, інші органи та установи, які можуть бути задіяні

Запитання для обговорення:

- *Чим була корисна ця вправа?*
- *Яким аспектам профілактичної роботі на кожному рівні необхідно приділяти більше уваги підрозділам поліції та соціальним службам?*
- *Як розподілити сфери впливу та відповідальність між партнерськими організаціями, залученими до профілактичної діяльності?*
- *На якому з трьох рівнів профілактична поліцейська діяльність може бути найбільш ефективною, а на якому – менш ефективною? З чим це може бути пов'язане?*

2. Інтерактивна вправа «Інтернет-залежність: що, чому, як?»

Мета: актуалізація знань стосовно розуміння сутності поняття інтернет-залежності дитини, її ознак, причин та наслідків.

Час: 45 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 2.1.2.1.2.

Хід проведення:

Перший етап (5-10 хвилин). Тренер/тренерка об'єднує учасників у чотири групи. Кожна група отримує аркуш паперу для фліпчарту, на якому необхідно закінчити речення «Інтернет-залежність – це…». Після виконання завдання групи передають по колу аркуші фліпчарту та доповнюють визначень інших груп. Кожна група має опрацювати всі визначення інших груп, після чого отримує свій аркуш із доповненнями.

Другий етап (10 хвилин). Кожна група отримує завдання визначити:

- ознаки інтернет-залежності дитини;
- психологічні особливості дітей, що роблять їх вразливими для впливу інтернет-загроз;
- чим приваблює дитину інтернет;
- наслідки інтернет-залежності.

Третій етап. Тренер/тренерка пропонує групам представити напрацювання. Час на виступ кожній групі – 5 хвилин.

Після представлення напрацювань учасників тренер/тренерка підбиває підсумок вправи (5 хвилин), звертаючи увагу учасників на Додаток 2.1.2.1.2.

До уваги тренера/тренерки!

Підбиваючи підсумки, тренер/тренерка наголошує, що ключовою ознакою залежності є поступове збільшення часу, проведеного людиною в інтернет-мережі або гаджетах, за рахунок іншої життєвоважливої діяльності на фоні загострення її проблем і конфліктів.

Залежність від інтернету може мати чимало шкідливих наслідків для людини як у соціальній, психологічній, так у фізичній сферах життя, адже надмірне використання електронних пристроїв спричиняє звикання, а частина життєвих сфер потерпає від дефіциту уваги і здорових стосунків: сім'я, навчання, спілкування з друзями тощо.

Запитання для обговорення:

- *Чим була корисна ця вправа?*
- *В чому, на вашу думку, можуть виникати труднощі у визначенні ознак того, що у дитини сформувалася інтернет-залежність ?*
- *Як ви вважаєте, які наслідки інтернет-залежності є віддаленими, а які можуть проявитися достатньо швидко?*

Тестові питання до заняття:

1. Який вид профілактики передбачає звернення до фахової психологічної допомоги для корекції адиктивної поведінки?

А) первинна профілактика;

Б) вторинна профілактика;

В) третинна профілактика.

2. Який вид профілактики передбачає раннє виявлення й коригування несприятливих індивідуальних і соціальних факторів, які з великою ймовірністю можуть спричиняти деструктивну поведінку?

А) первинна профілактика;

Б) вторинна профілактика;

В) третинна профілактика.

3. Який вид профілактики передбачає організацію зустрічі з учнями шкіл та тему захисту від небезпек, з якими можна стикнутися в інтернеті та соціальних мережах?

А) первинна профілактика;

Б) вторинна профілактика;

В) третинна профілактика.

4. Що можна віднести до ознак інтернет-залежності дитини? (можна обрати декілька варіантів відповідей)

А) тривалий час перебуває у пригніченому або агресивному стані, не може зосередитись на іншій справі, коли втрачає можливість перебувати в інтернеті;

Б) систематично забуває поїсти, виконати гігієнічні процедури, скаржиться на погане самопочуття;

В) проводить в інтернеті дедалі більше часу без об'єктивної потреби, пов'язаної з роботою, навчанням, не спілкується з друзями у звичний спосіб.

5. Що можна віднести до наслідків інтернет-залежності дитини? (можна обрати декілька варіантів відповідей)

А) погіршення спілкування з однолітками; ігнорування, ізоляція або відторгнення ними;

Б) прокрастинація;

В) збільшення або втрата ваги.

Ключі-відповіді:

1. В; 2. Б; 3. А; 4. А,Б,В; 5. А,Б.

Додаток 2.1.2.1.1

Поняття, рівні та види профілактики

У поліцейській діяльності є терміни «превенція» та «профілактика».

Превенція (від пізньолат. *praeventio* – випереджаю, попереджаю; англ. *prevention*) – це процес попередження негативних явищ і станів особистості.

Профілактика (від грец. *prophylaktikos* – попереджувальний) – це комплекс заходів, спрямованих на попередження будь-якого негативного явища та/або усунення ризиків його виникнення, що ґрунтується на своєчасному виявленні та виправленні негативних факторів, які зумовлюють протиправну поведінку особистості.

Незважаючи на різноманітність підходів до визначення профілактики, її основною характеристикою є спрямованість на попередження та мінімізацію негативних наслідків для дитини і суспільства.

Визначають первинну, вторинну і третинну профілактику.

Первинна профілактика негативних явищ **є універсальною** для застосування в дитячому та підлітковому середовищі (для всіх без винятку) і **спрямована на формування усвідомлено активного та адаптивного способу життя** (в контексті кібербезпеки – це здатність пристосуватися до змін для забезпечення безпеки в онлайн-просторі та захисту інформації)**, орієнтованого на відповідальну поведінку**.

Основною метою первинної профілактики в контексті кібербезпеки є зміцнення захищеності дітей, розвиток їхньої обізнаності та формування навичок, які їм допоможуть убезпечити себе від потенційних онлайн-небезпек і загроз.

Основні **завдання первинної профілактики**, що здійснюється поліцейськими, можуть включати:

1. надання дітям та батькам інформації про онлайн-загрози та небезпеки (наприклад віруси, спам, шахрайство, фішинг, злам особистих сторінок особи, кібербулінг, секстинг, онлайн-грумінг тощо);
2. навчання дітей правил безпеки в інтернеті (наприклад категорично не давати згоди на зустріч з особою, з котрою познайомився/познайомилася онлайн, дбати про безпеку персональних даних, вміти розпізнавати ситуації ризику і повідомляти дорослим про будь-які небезпечні ситуації в мережі тощо);
3. спонукати дітей до використання програм та платформ, які обмежують або блокують неприйнятний контент;
4. розвиток у дітей медіаграмотності та вміння відрізняти правдиву інформацію від фальшивої;
5. залучення батьків та освітян до проведення навчальних заходів з питань безпеки дітей у мережі, надання їм інструментів та ресурсів для створення безпечного онлайн-середовища;
6. розроблення та впровадження ефективних стратегій та заходів, спрямованих на запобігання онлайн-ризиків та небезпек, зокрема кібербулінгу, експлуатації та інших форм онлайн-насильства щодо дітей;
7. співпраця з громадськими організаціями, навчальними закладами для розроблення і впровадження програм та ініціатив з попередження онлайн-небезпек серед дітей.

Вторинна профілактика спрямована на зменшення ризиків і передбачає **раннє виявлення й коригування несприятливих індивідуальних і соціальних факторів**, які з великою ймовірністю можуть спричинити деструктивні наслідки.

Цей вид профілактики передбачає роботу з категоріями осіб, найбільш уразливих до потрапляння в ситуації онлайн-насильства, або тих, хто вже зазнав певних ризиків або схильний до

девіантної поведінки. За своєю спрямованістю вторинна профілактика є специфічною як така, що спрямована на групу й водночас стосується конкретної особи, тобто є індивідуальною.

Основною метою вторинної профілактики в контексті кібербезпеки дітей є виявлення небезпеки в онлайн-просторі та реагування на неї, а також надання підтримки та захисту дітям як найбільш уразливим до таких загроз або таким, що можуть практикувати ризиковану поведінку в мережі.

Основні **завдання вторинної профілактики** у цьому контексті можуть включати:

1. моніторинг та виявлення онлайн-небезпек та реагування на них;
2. проведення практичних навчальних заходів для дітей щодо вміння розпізнавати небезпечні ситуації та вчасно реагувати на них, засвоївши правила і стратегії захисту;
3 співпраця з громадськими організаціями й навчальними закладами для розбудови системи реагування та забезпечення безпеки дітей в мережі.

Третинна профілактика переважно є індивідуальною і спрямована на убезпечення та підтримку дітей, котрі постраждали від онлайн-загроз, зазнали наслідків ризикованої поведінки або самі здійснюють насильство у кіберпросторі.

Основною метою третинної профілактики в контексті кібербезпеки є створення стійкої системи захисту та підтримки дітей, які постраждали від онлайн-небезпек, запобігання подібним ситуаціям у майбутньому, а також робота з дітьми, які самі вчиняють такі правопорушення.

Основні **завдання третинної профілактики** можуть включати:

1. виконання необхідних заходів для притягнення винних осіб до відповідальності;
2. консультування з питань безпечної поведінки в кіберпросторі, забезпечення доступу до ресурсів та інформації для дітей, які постраждали або самі вчиняли такі правопорушення, а також їхніх батьків;
3. співпраця з психологами, соціальними педагогами, соціальними працівниками для надання психологічної підтримки та консультування дітей, які постраждали від онлайн-загроз або самі практикували насильницьку поведінку онлайн.

Варто звернути увагу, що робота з дітьми, які постраждали від онлайн-загроз, та дітьми, які практикували насильницьку поведінку онлайн та, наприклад, перебувають на обліку ювенальної превенції, проводиться ОКРЕМО!

Профілактична діяльність поліцейських також поділяється на загальну та індивідуальну.

Загальна профілактика є виконанням комплексу заходів інформаційно-роз'яснювального та просвітницького змісту, що спрямовані на підвищення обізнаності з певних питань, формування усвідомлення цінності життя і здоров'я та необхідних якостей особистості, а також навичок, що допоможуть відмовитися від негативних звичок та певних стандартів поведінки.

Заходи загальної профілактики можуть проводитись у закладах освіти, в громадських організаціях, які працюють з дітьми, соціальних службах, під час групових та масових заходів у громаді.

На заходах загальної профілактики бувають випадки виявлення дітей, котрі є постраждалими особами або вчиняють правопорушення. Важливо не залишати їх без уваги та діяти відповідно до вимог чинного законодавства.

Індивідуальна профілактика – це комплекс організаційно-практичних заходів із запобігання вчиненню, фіксації та припинення правопорушень, контролю за поведінкою осіб з метою недопущення повторного щодо них або вчинених ними правопорушень.

Додаток 2.1.2.1.2

Ключові ознаки, що вказують на перехід від зловживання інтернетом до залежності (К. Янг, Дж. Леменс, А. Джентайл, Е. Сарда та ін.)

I стадія – нетривалий час перебування в мережі.

II стадія – виявлення зацікавлення використанням інтернету для роботи і розваг.

III стадія – перебування в мережі із втратою відліку часу і контролю.

IV стадія – наявність залежності, руйнування взаємодії з навколишнім світом.

1. **Надмірна стурбованість** – підліток може бути зосереджений на певних активностях в інтернеті, постійно думає про те, що робитиме в мережі, чекає, коли зможе зануритися в спілкування або гру, і не може сконцентруватися на інших справах.
2. **Потреба у збільшенні часу** для улюблених активностей в інтернеті – підліток хоче довше перебувати в мережі, частіше грати або читати повідомлення, перевіряти статуси. Він може бути незадоволений через те, що хоче грати чи спілкуватися більше, ніж це можливо.
3. **Негативні переживання** – виникають, коли бажана активність в інтернеті стає недоступною. Підліток відчуває неспокій, напругу, роздратування та нещастя, що посилюється з часом.
4. **«Втеча» в інтернет від негараздів** – підліток занурюється у вебсерфінг, соціальні мережі або ігри, щоб забути про проблеми, уникнути неприємних думок або позбутися негативних переживань.
5. **Проблеми через надмірну активність** в інтернеті – підліток не може своєчасно зупинитися, відчуває недосипання тощо. Він систематично не виконує домашні завдання, пропускає заняття в школі, має непорозуміння з оточенням, але це не призводить до поліпшення його поведінки.
6. **Невдалі спроби контролю** над активностями в інтернеті – підліток намагається скоротити час або частоту перебування в мережі, але не може через неприємності та конфлікти, спричинені цією активністю.
7. **Приховування активності** в інтернеті – підліток приховує від інших час, витрачений на інтернет; у відповідь на запитання може говорити неправду; переглядає ресурси, спілкується або грає таємно.
8. **Втрата альтернативних інтересів** – з посиленням активності в інтернеті підліток втрачає інтерес до того, що раніше його цікавило; проводить менше часу з друзями і нехтує іншими видами діяльності.
9. **Конфлікти та руйнування стосунків** через активність в інтернеті – суттєві конфлікти з батьками та іншими членами сім'ї, втрата друзів та нехтування значущими відносинами.

Людина вважається інтернет-залежною, якщо протягом року у неї систематично спостерігається не менш ніж п'ять із вищезазначених ознак. Не всі з цих ознак можуть бути своєчасно помічені оточенням дитини, тому занепокоєння має виникати, якщо дитина:

1. проводить дедалі більше часу в інтернеті без об'єктивної потреби, пов'язаної з роботою чи навчанням, або якщо не спілкується з друзями у звичний спосіб;
2. не може відволіктися від інтернету на дійсно важливі справи;
3. систематично залишається в інтернеті або користується гаджетами вночі, незважаючи на необхідність рано йти до школи;

4. має кардинальні зміни настрою після заглиблення в інтернет;
5. без об'єктивних причин забуває про усталені інтереси;
6. демонструє погіршення успішності в навчанні, хоча залишає таку ж активність в інтернеті;
7. постійно «втікає» до інтернету від неприємностей, конфліктів чи зауважень батьків;
8. тривалий час перебуває у пригніченому або агресивному стані, не може зосередитися на інших справах, коли втрачає змогу користуватися інтернетом;
9. систематично забуває поїсти, виконати гігієнічні процедури та скаржиться на погане самопочуття.

Діти проявляють підвищену цікавість до всього нового, яскравого, незвичного; вони легко підпадають під вплив зовнішнього середовища і є більш допитливими, ніж дорослі. Тому вони використовують інтернет як універсальний спосіб дослідження та пізнання навколишнього світу. Однак такі психологічні особливості, як недостатня розвиненість механізмів саморегуляції, слабкий вольовий та емоційний контроль, а також імпульсивність поведінки, роблять дітей особливо вразливими під впливом інформаційних і програмно-технічних загроз.

Чим же приваблює інтернет дітей?

- відкрите та різноманітне спілкування з «будь-ким, з будь-якого куточка світу»;
- можливість втамувати інформаційний голод;
- пошук нових форм для самовираження (можливість робити те, чого раніше не робив, або дозволити собі те, що зазвичай заборонено в реальному житті);
- анонімність і віртуальна свобода (можливість бути «не собою» у «безпечних умовах»);
- відчуття спільності та належності до чогось більшого, ніж те, що є в реальному житті.

Окрім того, «втеча» в інтернет є одним зі способів уникнення середовища, наповненого проблемами і труднощами, що часто здаються набридлими і нездоланними. Через складнощі в оточенні підліток шукає безпечніші способи взаємодії і намагається уникати неприємних ситуацій.

Активність в інтернеті також дає змогу дитині захиститися від поганого настрою, болю або приниження. Діти, які мають залежність від інтернету, часто почуваються самотніми у реальному житті, мають незадоволені комунікативні потреби, що призводить до проблем у спілкуванні з близькими та ровесниками. Вони можуть відчувати нерозуміння або зазнавати емоційного тиску з боку близьких людей, переживати емоційну напруженість і тривогу.

Одна з найпопулярніших теорій щодо природи адиктивної поведінки (Ц. Короленко) вказує на те, що її причиною є прагнення людини «втекти» від неприємної реальності за допомогою штучної зміни свого емоційного стану та концентрації уваги на діяльності, що дає змогу переживати яскраві емоції. Саме це і забезпечують різноманітні активності в інтернеті, такі як перегляд відео, створення нового образу, спілкування в соціальних мережах, покупки, електронні ігри тощо.

Наслідки інтернет-залежності

Соціальні наслідки інтернет-залежності:

- **сімейні проблеми** – погіршення стосунків з батьками, іншими членами сім'ї та родичами;
- **погіршення спілкування з однолітками** – ігнорування, ізоляція або відторгнення з їхнього боку;
- **проблеми в школі,** зокрема погіршення успішності через непродуктивне використання часу на пошук інформації натомість, щоб виконувати домашні завдання; часто завдання

залишаються незавершеними або неповними, що призводить до погіршення комунікації з однокласниками та вчителями.

Психологічні наслідки інтернет-залежності можуть включати:

1. розлади вольових процесів;
2. розлади спілкування;
3. зниження показників пам'яті;
4. погіршення пізнавальних процесів;
5. схильність до отримання швидких результатів і негайного задоволення, що впливає на амбіції дитини, зменшує її вольові ресурси та знижує мотивацію до наполегливої праці і концентрації на виконанні складних завдань;
6. неспроможність зосереджуватися;
7. схильність до обману;
8. почуття провини;
9. тривожність, загострення страхів аж до фобій;
10. часті перепади настрою, дратівливість, агресивність як реакція на відключення від мережі;
11. втрата відчуття часу;
12. неможливість визначати пріоритети або дотримуватися графіків і планів;
13. соціальна ізоляція, почуття самотності;
14. постійне відкладання важливих справ, завдань та доручень, що призводить до негативних наслідків (прокрастинація).

Фізичні наслідки інтернет-залежності можуть виявлятися в таких симптомах:

1. біль у спині та шиї;
2. синдром зап'ястного каналу (защемлення та запалення нерва, що призводить до оніміння руки та зниження її рухової активності);
3. головні болі;
4. розлади сну, безсоння;
5. зміни в харчуванні (недоїдання або, навпаки, надмірне споживання їжі як спосіб «заїдання» стресу через віддалення від комп'ютера); збільшення або втрата ваги;
6. погіршення особистої гігієни (небажання приймати душ, щоб продовжити перебування в мережі);
7. сухість очей та інші проблеми із зором.

Заняття 2.1.2.2. Особливості профілактичної діяльності поліцейських підрозділів превентивної діяльності щодо втягнення дітей у протиправну діяльність в кіберпросторі

Мета: розглянути особливості профілактичної діяльності поліцейських підрозділів превентивної діяльності щодо втягнення дітей у злочинну діяльність в кіберпросторі на різних рівнях.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Особливості профілактичної діяльності підрозділів превентивної діяльності	Робота в групах	45 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 2.1.2.2.1
2.	Індивідуальна профілактична діяльність поліцейського з дитиною	Робота в групах	45 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 2.1.2.2.2

ХІД ЗАНЯТТЯ

1. Робота в групах «Особливості профілактичної діяльності підрозділів превентивної діяльності»

Мета: проаналізувати особливості профілактичної діяльності працівників поліції з дітьми на кожному з рівнів профілактики.

Час: 45 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 2.1.2.2.1.

Хід проведення:

Тренер/тренерка нагадує учасникам про те, що структура профілактики складається з трьох рівнів, де на першому – макрорівні: розробляються комплексні профілактичні програми, інформаційні кампанії у засобах масової інформації, масові заходи; на другому – мікрорівні: профілактика здійснюється у вигляді спеціальних програм, заходів та окремих активностей у межах закладів та організацій, а також за місцем проживання; на третьому – індивідуальному: робота здійснюється з окремими особами.

Після цього тренер/тренерка об'єднує учасників у три групи та озвучує завдання: проаналізувати які профілактичні заходи первинної, вторинної та третинної профілактики можуть використовувати поліцейські:

група 1 – профілактичні заходи першого рівня;

група 2 – профілактичні заходи другого рівня;

група 3– профілактичні заходи третього рівня.

Час на роботу в групах – 20 хвилин.

Результати роботи в групах учасники мають викласти в таблицю за зразком:

№ з/п	Рівень профілактичних заходів	Перелік заходів, які можуть здійснюватися на зазначеному рівні	Суб'єкти, яких можна залучити до реалізації профілактичних засобів	Необхідні інструменти, засоби, матеріали тощо
1.	Профілактичні заходи першого рівня			
2.	Профілактичні заходи другого рівня			
3.	Профілактичні заходи третього рівня			

Після завершення виконання завдання кожна група презентує напрацьовані результати по 5 хвилин на групу, а тренер/тренерка доповнює їхні відповіді з врахуванням інформації, викладеної в Додатку 2.1.2.2.1.

До уваги тренера/тренерки!

Якщо заняття проводиться в межах первинної підготовки або учасники не мають достатніх знань та досвіду проведення профілактичної діяльності, для виконання цієї вправи доцільно завчасно підготувати та надати їм узагальнений перелік можливих профілактичних заходів, з якого учасники можуть обирати заходи для конкретного рівня профілактики.

Додатково до підготоки до заняття можна використовувати розділ 4 «Зміст і форми профілактики девіантної поведінки дітей» навчального посібника «Психолого-педагогічні та правові засади діяльності поліції із захисту прав дитини».

Запитання для обговорення:

- *Чим була корисна ця вправа?*
- *Які заходи профілактики на кожному рівні, на вашу думку, є найбільш ефективними? У якій формі доцільно їх проводити? Прокоментуйте, чому саме.*
- *На якому з рівнів найбільш потрібною може бути підтримка партнерських закладів, організацій та установ? З яких питань?*
- *Які особливості профілактичної діяльності втягнення дітей у злочинну та іншу протиправну діяльність в кіберпросторі ви можете визначити?*
- *Чи існують відмінності у здійсненні профілактичних заходів на різних рівнях профілактики? Визначте їх суть та особливості.*
- *Чи варто залучати до планування заходів дітей та молодь як суб'єктів профілактичної діяльності, наприклад за методом «рівний-рівному»?*

2. Робота в групах «Індивідуальна профілактична діяльність поліцейського з дитиною»

Мета: відпрацювати навички планування індивідуальної профілактичної діяльності поліцейського з дитиною.

Час: 45 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 2.1.2.2.2.

Хід проведення:

Тренер/тренерка об'єднує учасників у чотири групи. Кожна група отримує картку з ситуацією, в якій головною діючою особою є дитина, яка втягнена у злочинну діяльність в кіберпросторі. Протягом 20 хвилин учасники мають в групах розробити план проведення індивідуальної профілактичної діяльності поліцейського з дитиною за схемою: «захід-мета-очікуваний результат-залучені фахівці» та презентувати розроблений план.

- групи 1 та 3 працюють над ситуацією 1;
- групи 2 та 4 працюють над ситуацією 2.

Після закінчення презентацій тренер/тренерка ініціює обговорення.

Запитання для обговорення:

- *Чим корисна була ця вправа?*
- *Хто може бути об'єктом профілактичної діяльності?*
- *Фахівці яких підрозділів поліції та установ можуть бути залучені до профілактичної діяльності?*
- *Що необхідно враховувати в процесі здійснення профілактичної поліцейської діяльності з дитиною?*
- *Що допомагало, а що заважало плануванню заходів? А як би це було в режимі реального часу?*

Тестові питання до заняття:

1. До заходів профілактики втягнення дітей у злочинну та іншу протиправну діяльність в кіберпросторі можна віднести:

А) виявлення причин й умов, що сприяють втягненню дітей у злочинну та іншу протиправну діяльність у кіберпросторі та впровадження організаційних і практичних заходів для їх усунення;

Б) проведення тематичних зустрічей з адміністрацією закладів освіти та представниками батьківської громадськості;

В) проведення у закладах освіти, за місцем проживання дітей профілактичних заходів, спрямованих на формування безпечної поведінки в інтернеті.

Г) усі відповіді правильні.

2. Під час здійснення профілактики втягнення дітей у злочинну та іншу протиправну діяльність в кіберпросторі поліцейські:

А) планують профілактичні заходи з урахуванням потреб осіб, щодо яких вони здійснюються;

Б) можуть застосовувати різні форми та методи профілактичної роботи;

В) взаємодіють з іншими суб'єктами: соціальними службами, закладами освіти, громадськими організаціями тощо;

Г) вживають усі вищеперераховані заходи.

3. Скільки існує рівнів профілактики?

А) 2 рівні;

Б) 3 рівні;

В) 4 рівні;

Г) 5 рівнів.

4. Найбільш ефективними формами роботи з дітьми під час проведення профілактичної роботи щодо втягнення дітей у злочинну та іншу протиправну діяльність в кіберпросторі є:

А) активні форми;

Б) пасивні форми;

В) інтерактивні форми;

Г) усі перераховані форми.

5. До інтерактивних форм профілактичної діяльності належить:

А) лекція;

Б) бесіда;

В) відеолекторій;

Г) тренінг.

Ключі-відповіді:

1. Г; 2. Г; 3. Б; 4. Г; 5. Г.

Додаток 2.1.2.2.1

Особливості профілактичної діяльності підрозділів поліції щодо втягнення дітей у протиправну діяльність в кіберпросторі

Загальновизнано, що профілактична діяльність поліцейських підрозділів превентивної діяльності щодо втягнення дітей у злочинну та іншу протиправну діяльність є складним комплексом заходів, спрямованих на усунення або нейтралізацію конкретних криміногенних факторів, що сприяють цим правопорушенням. Це також включає виправлення й перевиховання осіб, які вчинили правопорушення. Як видно, така діяльність може здійснюватися як щодо правопорушників, так і щодо дітей, які потенційно можуть стати постраждалими від злочинних посягань.

Профілактична діяльність поліцейських підрозділів у кіберпросторі має свої особливості. Працівники поліції не можуть безпосередньо впливати на осіб, які здійснюють протиправні дії щодо залучення дітей у злочинну та іншу протиправну діяльність в інтернеті. Саме тому в цьому випадку доречно говорити про **віктимологічну профілактику**.

Віктимологічна профілактика визначається як сукупність державних і громадських заходів, спрямованих на запобігання злочинам через зниження ризику (схильності) у населення, зокрема у окремих громадян, стати постраждалими від злочинних посягань. Екстраполюючи це визначення, можна стверджувати, що віктимологічна профілактика щодо втягнення дітей у злочинну та іншу протиправну діяльність в кіберпросторі передбачає сукупність заходів, спрямованих на запобігання такій діяльності через зниження ризику (схильності) дітей стати постраждалими особами.

Ця робота є цілеспрямованою та плановану діяльністю, що має правову регламентацію і повинна виконуватися відповідно до норм закону, а також враховувати знання в галузі психології та педагогіки. Профілактичні заходи застосовуються з метою зміни як соціальних умов існування осіб, так і особистісних якостей суб'єкта, у нашому випадку – дітей.

У віктимологічній профілактиці виділяють два основні напрями запобіжних заходів, об'єктами яких є віктимологічні ситуації:

Індивідуальна віктимологічна профілактика спрямована безпосередньо на потенційних і реальних постраждалих.

Загальна або індивідуально-групова віктимологічна профілактика спрямована на груповий рівень.

З огляду на це, плануючи профілактичні заходи щодо втягнення дітей у злочинну та іншу протиправну діяльність у кіберпросторі, працівники підрозділів поліції повинні враховувати потреби в проведенні таких заходів залежно від рівня профілактики. Вони мають брати до уваги особливості ефективної просвітницько-профілактичної роботи, з урахуванням вікових характеристик дітей, наявні можливості та власну обізнаність у специфіці реалізації цих заходів.

Авторами методичних рекомендацій «Твоя безпека в інтернеті: попередження насильства щодо дітей в інтернеті та формування безпечної поведінки в мережі» виокремлено такі ефективні форми роботи з дітьми під час проведення просвітницько-профілактичної роботи:

Пасивні форми передбачають взаємодію учасників і ведучих, в якій ведучі є основними дійовими особами заходу, а учасники є лише слухачами. Класичний приклад пасивної форми взаємодії з групою – лекція.

Недоліком пасивних форм взаємодії з аудиторією є обмеження зворотного зв'язку, адже запитання не передбачені, й неможливо визначити, чи зрозуміли слухачі лектора/лекторку, чи вдалося йому/їй досягти поставленої мети. Низький рівень уваги впродовж зустрічі (учас-

ники, зазвичай, втрачають увагу через 15-20 хвилин після того, як лекція почалася); низький рівень сприйняття та запам'ятовування почутого, особливо якщо інформація для учасників була новою і не використовувалась жодна наочність (прикладами наочності, що підвищує ефективність роботи, є плакати, буклети, презентації, відео) – теж є характерними недоліками такої форми взаємодії. Отже, **пасивні форми вважаються найменш ефективними** для якісного засвоєння матеріалу.

Однак, незважаючи на вищевикладене, вони мають деякі переваги. По-перше, підготовка до них порівняно проста; по-друге, вони дають змогу довести до відома слухачів максимальну кількість матеріалів в обмеженому часі; по-третє, охоплюють упродовж однієї зустрічі значну кількість учасників.

Активні форми – це форми взаємодії учасників і ведучих, залучених до заняття, коли обидві сторони можуть і запитувати, і відповідати на запитання.

Вони вважаються більш ефективними, ніж пасивні, проте менш ефективними, ніж інтерактивні форми організації просвітницько-профілактичної роботи.

Інтерактивні форми – це форми, в межах яких учасники взаємодіють не лише з ведучими, а й між собою, обмінюючись думками, успішним або невдалим досвідом, напрацьовуючи правильні та безпечні стратегії поведінки, тощо.

Ведучі в інтерактивних заняттях спрямовують діяльність учасників на досягнення цілей, роз'яснюють ситуації та виступають у ролі експертів. Отже, **найбільш продуктивними є інтерактивні заняття.**

Відповідно до форм роботи обираються й методи навчання.

Метод у загальному значенні – це спосіб досягнення мети і діяльність, впорядковані певним чином.

Методи навчання – сукупність прийомів та підходів, які відображають форму взаємодії учасників з ведучими у процесі навчання.

Не всі методи роботи з групою є однаково ефективними. Так звана «піраміда пізнання» показує, що чим більший ступінь участі в процесі пізнання тих, хто навчається, тим більше інформації й навичок вони засвоюють.

Піраміда пізнання

У практиці щоденної роботи не існує ідеальних форм і методів профілактики. **Ефективність залежить від професійної компетентності фахівців, доцільності обраних ними форм та методів у конкретній ситуації, а також наявних ресурсів та умов, в яких вони будуть запроваджуватись. Бажано, щоби інформаційно-просвітницькі заходи з дітьми були інтерактивними.** Використовуйте різноманітні методи: роботу в малих групах, мозковий штурм, обговорення, моделювання, демонстрацію, рольові та інші ігри, ілюстрації, приклади, розгляд історій тощо.

Під час проведення просвітницько-профілактичних заходів/програм важливо:

1. говорити доступною для дітей мовою, уникати складних термінів, пояснювати на прикладах, забезпечувати зворотний зв'язок з аудиторією для взаєморозуміння;
2. встановити спільно з учасниками правила проведення занять, наприклад, хочеш висловитися — підніми руку; дотримуйся часу, відведеного на виконання завдань у групі; будь активним і залучайся до обговорення; поважай тих, хто поруч, тощо;
3. розказати про зміст і ціль заняття та як воно відбуватиметься, які результати очікуються, а також як набуті знання та навички знадобляться кожному з учасників у подальшому;
4. робити паузи між інформаційними блоками, щоби полегшити їх сприйняття учасниками заходу та дати їм змогу обдумати почуте. Не варто поспішати та ставити за мету розгляд якомога більшої кількості аспектів теми;
5. зупинятися за потреби, відповідати на запитання, які виникають, збільшувати час для розуміння й усвідомлення інформації та/або відпрацювання навичок;
6. спостерігати за поведінкою та активністю учасників, намагатися їх зацікавити запитаннями чи завданнями замість зауважень;
7. активізувати їх відкритими запитаннями, що вимагають розгорнутої відповіді, ідеальної для двохсторонньої комунікації: «Як ви вважаєте...», «Чому, на вашу думку,...», «Навіщо...» тощо;
8. перевіряти, чи зрозуміли учасники інформацію, закритими запитаннями, які передбачають відповіді «так» або «ні», наприклад, «Якщо людина вчинила правопорушення, вона має понести за це покарання?» тощо;
9. бути чесними, щирими й демонструвати повагу у спілкуванні з дітьми, віддавати перевагу порадам, а не вимогам, дослухатися до їхніх думок;
10. контролювати вираз свого обличчя і жести, які мають бути коректними і відповідати змісту вашої розповіді;
11. заздалегідь готувати наочні й роздатковий матеріали, технічні засоби тощо, використовувати власні творчі можливості.

Чітко сплановане й цікаве за змістом емоційне заняття є запорукою його успішного проведення та найкращим способом налагодження доброзичливих взаємин з учнями.

Під час планування та проведення заходів загальної профілактики серед дітей слід використовувати матеріали, рекомендовані Міністерством освіти і науки України (https://mon.gov.ua/osvita-2/pozashkilna-osvita/vikhovna-robota-ta-zakhist-prav-ditini/bezpeka-ditey-v-interneti).

Для **проведення профілактичних заходів** з дітьми також можуть бути використані матеріали, схвалені до використання рішенням відповідної комісії Науково-методичної ради з питань освіти Міністерства освіти і науки України. Зокрема:

1. **просвітницько-профілактична програма «Твоя безпека в інтернеті: попередження насильства щодо дітей в інтернеті та формування безпечної поведінки у мережі»**,

яка спрямована на формування у дітей та молоді (1-11 класів) базових компетентностей (знань, умінь та навичок) безпечної поведінки в інтернеті з урахуванням їхніх вікових можливостей розвитку: https://drive.google.com/file/d/12DhKid5L3dHtsT19Wr6kIJSj4TXcP4rz/view?usp=share_link;

2. **лифлети та стікерпаки** для дітей 1-11 класів з правил безпеки в мережі: https://drive.google.com/drive/folders/1BQhiaXMAftqzORJxtjvRIhHdq2tQlH3G?usp=share_link;
3. пакет інструментів із запобігання насильству в інтернеті щодо дівчат-підлітків — **Toolkit з профілактики сексуального онлайн-насильства щодо дівчат-підлітків**: https://lhsi.org.ua/s430-instrumentariy-iz-zapobigannya-onlayn-nasilstvu-schodo-divchat-pidlitkiv;
4. **матеріали для підлітків** (картки з правилами безпечної поведінки офлайн та онлайн) **Школи безпеки ТЯМ:** https://childfund.org.ua/diialnist/shkola-bezpeki-tyam;
5. **навчальний посібник із безпеки дітей в інтернеті**, розроблений компанією Google у співпраці з організаціями The Net Safety Collaborative та Internet Keep Safe Coalition: https://rescentre.org.ua/bezpeka-ditei-v-interneti/navchalnyi-posibnyk-iz-bezpeky-ditei-v-interneti;
6. **онлайн-курс та уроки для школярів 1-11 класів про приватність в інтернеті**: https://minzmin.org.ua/projects/;
7. **освітні серіали на платформі «Дія»** (наприклад «Про кібербулінг для підлітків»: https://osvita.diia.gov.ua/courses/cyberbullying; «Персональні дані»: https://osvita.diia.gov.ua/courses/personaldata; «Кіберняні»: https://osvita.diia.gov.ua/courses/cybernanny тощо);
8. **онлайн-курси** (наприклад «Кіберпростір та кібербезпека»: https://cyber.volunteer.kiev.ua; «VeryVerified: онлайн-курс з медіаграмотності»: https://verified.ed-era.com/ua#rec129945142; «Основи інформаційної кібербезпеки»: https://courses.prometheus.org.ua тощо);
9. **навчальні та освітні відео** (наприклад «П'ятихвилинка медіаграмотності»: https://www.youtube.com/watch?v=tMQudmwJUf8);
10. **ігри та онлайн-ігри** («МедіаДрайвер»: http://mediadriver.online/about/; «365° за шкалою медіаграмотності»: https://www.aup.com.ua/365-game/; «Медіазнайко»: https://www.aup.com.ua/Game/index.html);
11. **матеріали інформаційно-освітньої кампанії #stop_sextинг:** https://stop-sexting.in.ua/about.

Додаткова інформація

У 2022 році командою експертів МГО «Соціальні ініціативи з охорони праці та здоров'я» було проведено оцінку ситуації щодо кібербезпеки дітей 10-18 років, за результатами якої встановлено, що більшість дітей та батьків не ідентифікують безпеку в інтернеті як проблему і не визнають нагальних потреб у змінах. Водночас батьки визнають потребу в додатковій інформації та покращення знань про те, як захистити свою дитину від небезпечного контенту та контакту в інтернеті. Водночас експерти дійшли єдиної думки щодо необхідності привертати більше уваги до питань кібербезпеки дітей в інтернеті саме зараз, під час війни та вимушеного переміщення великої кількості осіб. Це демонструє, що експерти ознайомлені та знають про загрози для дітей в інтернет-просторі більше, аніж батьки, та частіше стикаються вже із наслідками небезпечного впливу насильницького контексту, кібербулінгу та небезпечної поведінки дітей в мережі інтернет. Ними вироблено рекомендації для подальшої роботи проєкту та розроблення пріоритетного плану дій для ефективної профілактики та реагування на загрози безпеці дітей 10-18 років в інтернеті, які можна розділити на національний та місцевий рівні.

Національний рівень. Переглянути чинні нормативно-правові акти в контексті воєнної агресії росії проти України та розробити національний механізм профілактики та реагування на випадки насильства над дітьми в мережі інтернет. Надати експертні висновки та долучитися до перегляду Національної стратегії захисту прав дітей у цифровому середовищі, надати консультаційну підтримку та сприяти її подальшому затвердженню; розробити рекомендації та план її втілення, що допоможе скоординувати дії усіх зацікавлених державних і недержавних органів і партнерів.

Провести інформаційно-навчальну кампанію для батьків і вихователів про можливість насильства та потенційні ризики, з якими дитина стикається у мережі інтернет, з особливим фокусом на можливі загрози насильства щодо дітей в інтернет-просторі, які збільшуються та поглиблюються під час війни.

Провести навчання або підвищення кваліфікації, застосовуючи найкращий міжнародний досвід, представників Національної поліції, ювенальної превенції, шкільних офіцерів поліції для підвищення рівня їхніх знань про сучасні ризики насильства в інтернеті, включно з булінгом, секстингом, онлайн-грумінгом і втягуванням дітей (особливо дівчат) до комерційного сексу та порнографії.

Для всіх державних і недержавних установ, які відповідають за захист прав дітей, підвищити потенціал та розробити керівництво щодо навичок спілкування з дітьми різних вікових категорій та соціальних груп, для ефективної протидії залученню дітей 10-18 років у насильницько-деструктивні групи.

Напрацювати та розробити механізми моніторингу випадків насильства над дітьми в мережі інтернет, розглянути та апробувати механізми реагування на скарги з боку дітей.

Місцевий рівень. У зв'язку з реформою децентралізації та функціями місцевої влади зі створення безпечного середовища для дітей переглянути місцеві стратегії профілактики насильства над дітьми, зокрема в інтернет-середовищі, та розробити плани інформування дітей та батьків щодо своєчасної профілактики ризиків можливого насильства в інтернеті.

Працівники соціальних служб, служб у справах дітей, закладів освіти та неурядових організацій, які працюють у сфері захисту прав дітей, мають пройти підвищення кваліфікації щодо роботи з дітьми з профілактики насильства в інтернеті.

Зібрати та адаптувати найкращі міжнародні практики щодо профілактики насильства над дітьми в інтернеті, апробувати (протестувати) міжнародні інструменти роботи та співпраці на місцевому рівні в Україні.

Залучати молодь і дітей до навчання та до інформаційної кампанії з розроблення цифрових повідомлень щодо профілактики онлайн-насильства. Надавати та розповсюджувати інформацію щодо наявних ресурсів надання допомоги дітям щодо насильства («гарячі лінії», чат-боти, телефони довіри, сайти та чати тощо).

У зв'язку зі внутрішнім переміщенням і переміщенням багатьох сімей з дітьми за кордон розробити механізми інформування родин щодо небезпеки насильства й торгівлі людьми через небезпечні контакти дітей в інтернеті та в соціальних мережах.

Практичні приклади запобігання віктимності дітей

- У 2019 році поліцією Донеччини розроблено Регіональну програму профілактики правопорушень серед дітей на території Донецької області на 2019-2022 роки. Під час реалізації заходів Програми запроваджено низку безпекових проєктів.
- «Відновні практики: прості рішення складних питань» – це спільний проєкт ювенальної превенції та ГО «Молодіжна ліга майбутніх поліцейських», метою якого є: профілактика

правопорушень, зниження рівня злочинності серед неповнолітніх, подолання та вирішення конфліктів серед дітей, зокрема запобігання булінгу у школах. В межах проєкту у загальноосвітніх закладах створено 108 шкільних служб порозуміння, проведено 14 тренінгів для отримання навичок медіації, якими охоплено 120 учнів та 30 вчителів. З використанням відновних практик з дітьми та батьками проведено понад 300 профілактичних заходів.

- Інформаційний простір «Дитячий коп» – спільний проєкт поліції та ГО «Рада жінок Донеччини», мета якого полягає у створенні інформаційного простору «дитячий коп» у соціальній мережі Instagram для дітей та молоді Донеччини, що містить у собі корисний інтернет-контент (фото та відео блог) на правову тематику, а також поширення їх через свій сервіс і низку інших соціальних мереж, що дає змогу дітям, підліткам та їхнім батькам більше дізнатися про свої права та обов'язки, вміти захистити свої законні інтереси.
- «Діти + поліція = безпека та мир» – є спільним проєктом поліції та ГО «Азовський патріот» через створення громадської платформи ініціатив для захисту неповнолітніх від насильства (сексуального, фізичного, економічного, психологічного), булінгу, зокрема внутрішньо переміщених дітей та тих, які проживають у зоні збройного конфлікту.
- «Простір миру та безпеки» також є спільним проєктом поліції та ГО «Молодіжна ліга майбутніх поліцейських», метою якого є запобігання злочинності проти неповнолітніх. Упродовж трьох етапів професійними тренерами ювенальної превенції – медіаторами було сформовано 11 команд медіаторів серед учнів. Загалом було охоплено понад 6 000 учнів. У навчальних закладах за підтримки Програми ООН із відновлення та розбудови миру облаштовано 11 кімнат шкільної служби порозуміння.

Додаток 2.1.2.2.2

Ситуація 1

На день народження батьки подарували Катрусі (14 років) комп'ютер та підключили до мережі інтернет, тепер у неї з'явилося більше можливостей для спілкування. Спілкуючись в соціальній мережі з друзями, одного разу вона отримала цікаве повідомлення від незнайомого хлопця, який незабаром запропонував їй дружбу. З кожним днем спілкування Катя розуміла, що в них багато спільного, та й за віком хлопець був лише на два роки старшим за неї. На фото, яке вона отримала, він був дивовижно гарним і добрим хлопцем, тому в неї не виникло сумнівів щодо зустрічі з ним. Але говорити про це батькам дівчинка не стала, бо вважала себе вже дорослою та думала, що повернеться додому раніше, ніж вони прийдуть з роботи. Вона уявляла, що з новим другом прийде на дискотеку, і всі подруги будуть їй заздрити.

Коли ж дівчина прийшла на призначене місце зустрічі, там було темно і безлюдно, проте це її зовсім не турбувало, адже її новий знайомий хотів, щоб їм ніхто не заважав. Пройшов деякий час і, раптом перед нею з'явився неохайно вдягнений дорослий чоловік. Як з'ясувалося – це був той, хто видавав себе в інтернеті за чемного і доброго хлопця, якому 16 років. Чоловік відібрав сумку і мобільний телефон, побив дівчину та почав погрожувати їй насиллям, якщо вона розповість про нього. Дівчинка дуже злякалась, вирвалась з ціпких рук чоловіка та втекла додому.

Ситуація 2

Саша (13 років) цікавиться інтернет-квестами. Він уже не один раз брав у них участь. Але цього разу хлопець знайшов квест на невідомому йому сайті, це його насторожило, але не зупинило, тому в кінці проходження змагання учасникам обіцяли дорогоцінні призи. Перші завдання мали зміст такий, як у звичайних інтернет-квестах, проте зміст наступних його налякав. Саші давали завдання зняти відео з небезпечними трюками, для його життя та здоров'я. Коли хлопець хотів вийти з гри, то організатори квесту почали йому погрожувати, що вб'ють його батьків, якщо він не буде виконувати завдання. Саша дуже переживав за батьків, адже на початку квесту під час реєстрації він заповнив форму, в якій зазначив свою домашню адресу, і дозволив простежувати свої географічні дані на телефоні. Хлопець розгублений і звернувся до друга.

ТЕМА 2.1.3. Профілактичні заходи для захисту дітей від насильства і експлуатації в кіберпросторі. Запобігання потраплянню дітей в небезпечні ситуації

Заняття 2.1.3.1. Профілактичні заходи для захисту дітей від насильства і експлуатації в кіберпросторі

Мета: надати учасникам інформацію про особливості організації та реалізації профілактичних заходів для захисту дітей від насильства і експлуатації в кіберпросторі.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Сутність та види профілактики насильства та експлуатації дітей в кіберпросторі	Інформаційне повідомлення	20 хв	Додаток 2.1.3.1.1, мультимедійне обладнання
2.	Сучасні форми та ресурси для планування профілактичних заходів з питань захисту дітей від насильства і експлуатації в кіберпросторі	Обговорення	20 хв	Додаток 2.1.3.1.2, мультимедійне обладнання, фліпчарт, аркуші для фліпчарту, маркери
3.	Online сексуальне насильство над дітьми (онлайн-грумінг)	Відеолекторій	20 хв	Відео «Online сексуальне насильство над дітьми (кібергрумінг)» https://www.youtube.com/watch?v=b-gaa9ZI2JE&ab_channel=StopSextingUkraine, мультимедійне обладнання, Додаток 2.1.3.1.3
4.	Які принципи слід враховувати під час планування та проведення профілактичних заходів з питань безпеки в інтернеті?	Робота в парах	30 хв	Додаток 2.1.3.1.4, аркуші А4, маркери

До уваги тренера/тренерки!

Доцільно проводити заняття з цієї теми після вивчення учасниками/учасницями теми, присвяченій питанням ризиків та загроз для дітей в кіберпросторі.

ХІД ЗАНЯТТЯ

1. Інформаційне повідомлення «Сутність та види профілактики насильства і експлуатації дітей в кіберпросторі»

Мета: актуалізувати знання учасників щодо сутності та видів профілактики взагалі, а також сприяти усвідомленню ними важливості комплексного підходу до питань профілактики насильства та експлуатації дітей в кіберпросторі, спрямованого не лише на запобігання потраплянню дітей в небезпечні ситуації, а й виявлення та усунення його причин та умов.

Час: 20 хв.

Необхідні матеріали: Додаток 2.1.3.1.1, мультимедійне обладнання.

Хід проведення:

Тренер/тренерка виводить на екран цитату: *«Завдання глобального суспільства полягає, з одного боку, у розробленні й побудові досвіду для підлітків, який допомагає їм скористатися можливостями інтернету, з іншого – у пом'якшенні проблем у житті, які частково опосередковані цифровими технологіями»* та запитує в учасників, як вони розуміють її зміст, враховуючи тему заняття. Після висловлення учасниками своїх думок тренер/тренерка наголошує на тому, що профілактичні заходи для захисту дітей від насильства і експлуатації в кіберпросторі мають бути комплексними та передбачати висвітлення питань цифрової грамотності загалом, після чого презентує інформацію із Додатка 2.1.3.1.1.

До уваги тренера/тренерки!

Під час підготовки до заняття доцільно підготувати презентацію, використовуючи матеріал з Додатка 2.1.3.1.1.

Слід наголосити, що **профілактичні заходи захисту дітей** від насильства та експлуатації в кіберпросторі **мають бути комплексними і містити різні компоненти**:

1. знання і навички безпечного користування інтернетом, зокрема соціальними мережами (наприклад вміння розпізнати ситуацію ризику, розуміти наслідки публікації особистої інформації тощо);
2. навички критичного мислення, необхідні для визначення й розуміння позитивних та негативних сторін власної поведінки в цифровому просторі, а також для прийняття обдуманих безпечних рішень;
3. список номерів телефонів організацій, до яких діти можуть звернутися в разі потреби;
4. спільні навчальні заходи для дітей, батьків та освітян, спрямовані на розуміння ситуацій онлайн-насильства та набуття навичок для ефективного реагування на них.

Запитання для обговорення:

- *Чи мали ви досвід проведення профілактичних заходів серед дітей взагалі та з питань кібербезпеки зокрема?*
- *Які, на вашу думку, можна виокремити причини та умови потрапляння дітей в ситуацію насильства і експлуатації в кіберпросторі?*
- *Враховуючи названі вами причини та умови, які питання, на вашу думку, мають охоплювати профілактичні заходи для захисту дітей від насильства і експлуатації в кіберпросторі?*
- *До виконання яких рекомендацій із аналітичного звіту «Сексуальне насильство над дітьми та сексуальна експлуатація дітей в інтернеті в Україні», на вашу думку, можуть долучатись поліцейські? Яких підрозділів поліції?*

До уваги тренера/тренерки!

Якщо є час, можна приділити увагу обговоренню психоемоційного стану дитини, яка зазнає насильства в кіберпросторі за допомогою проведення інтерактивної вправи:

тренер тримає чистий аркуш паперу, просить уявити, що це дитина. Завдання учасників/учасниць – «ображати» дитину, надаючи негативні коментарі в умовному чаті. З кожною образою аркуш паперу слід зминати. На наступному етапі тренер/тренерка просить групу вибачитись перед «дитиною», розпрямляючи аркуш паперу. Слід звернути увагу, що аркуш все одно вже не такий як був, має очевидні ушкодження, та наголосити, що своєчасна профілактика насильства в кіберпросторі важлива, оскільки такі дії дуже впливають на стан дитини, її поведінку та потребують своєчасного виявлення та реагування.

2. Обговорення «Сучасні форми та ресурси для планування профілактичних заходів з питань захисту дітей від насильства і експлуатації в кіберпросторі»

Мета: сприяти обміну досвідом щодо наявних практик та ресурсів, спрямованих на захист дітей від насильства і експлуатації в кіберпросторі.

Час: 20 хв.

Необхідні матеріали: Додаток 2.1.3.1.2, мультимедійне обладнання, фліпчарт, аркуші для фліпчарту, маркери.

Хід проведення:

Тренер/тренерка звертається до учасників із запитанням: *«Які форми профілактичних заходів можуть використовуватись для захисту дітей від насильства і експлуатації в кіберпросторі?»* та занотовує відповіді учасників на аркуші для фліпчарту. Після чого, використовуючи інформацію із Додатка 2.1.3.1.2, надає додаткову інформації щодо сучасних ініціатив, спрямованих на профілактику насильства і експлуатації дітей в кіберпросторі та ресурсів, які можна використовувати під час планування тематичних профілактичних заходів.

Запитання для обговорення:

- *Які форми профілактичної роботи ви переважно використовуєте в своїй практичній роботі? Чому саме їх?*
- *Коли ви обираєте форму профілактичної роботи, які фактори ви враховуєте?*
- *Які партнерські організації можуть долучитися до виконання профілактичної діяльності поліцейських?*

До уваги тренера/тренерки!

Додаткову інформацію про поняття, види та рівні профілактики можна знайти у Додатку 2.1.2.1.1.

Якщо є час та необхідна кількість учасників, а також наявна карткова гра «Коло безпеки», можна продемонструвати цю гру та пропрацювати коло В «Дитина і насильство в інтернет-мережі».

Крім того, доцільно продемонструвати сайт проєкту #stop_sextинг, зокрема наявні на ньому методичні розробки для проведення занять з дітьми різного віку, а також з дітьми з особливими освітніми потребами. Також на сайті проєкту містяться інструкції щодо налаштувань безпеки у соціальних мережах, встановленні програм батьківського контролю, тощо.

3. Відеолекторій «Online сексуальне насильство над дітьми (онлайн-грумінг)»

Мета: продемонструвати особливості застосування відеоматеріалів в профілактичній роботі та обговорити тактики маніпулювання, які використовують особи, які вчиняють сексуальне насильство та експлуатацію дітей в кіберпросторі.

Час: 20 хв.

Необхідні матеріали: відео «Online сексуальне насильство над дітьми (кібергрумінг)» https://www.youtube.com/watch?v=b-gaa9ZI2JE&ab_channel=StopSextingUkraine, мультимедійне обладнання, Додаток 2.1.3.1.3.

Хід проведення:

Тренер/тренерка пропонує переглянути відео та зазначає: *«Це відео є адаптацією інформаційної кампанії Європолу «Скажи «Ні» сексуальному примушенню дітей та вимаганню в*

інтернеті», після чого звертається до учасників з питанням: «*Які питання варто обговорити з дітьми після перегляду цього відео?*»

До уваги тренера/тренерки!

Слід акцентувати увагу учасників, що використання відео під час проведення профілактичної роботи має супроводжуватись його обговоренням. Серед питань, які доцільно обговорити після перегляду цього відео, можна зазначити такі:

1. У чому переваги й недоліки знайомства через інтернет?
2. Скільки тобі потрібно часу для того, щоб людина, з якою ти спілкуєшся в мережі, отримала твою повну довіру? Як ти визначаєш, коли людині можна довіряти?
3. Чи повіриш ти в щирість людини, якій для побудови романтичних стосунків важлива не твоя особистість (думки, хобі, досягнення, характер), а зображення вашого оголеного тіла?
4. Як би ти відреагував на пропозицію зробити оголене фото? Сформулюй кілька фраз-відмов.
5. Що робити, якщо потрапив в таку ситуацію?
6. Як допомогти другу, що потрапив у таку ситуацію?

Також можна обговорити тактики маніпуляцій, які використовують особи, що вчиняють сексуальне насильство та експлуатацію дітей в кіберпросторі, використовуючи Додаток 2.1.3.1.3.

Запитання для обговорення:

- *Чи використовуєте ви відео під час профілактичної роботи з дітьми?*
- *З яких ресурсів ви підбираєте відео для профілактичної роботи?*

4. Робота в парах «Які принципи слід враховувати під час планування та проведення профілактичних заходів з питань безпеки в інтернеті?»

Мета: надати інформацію про принципи діяльності під час планування та проведення профілактичних заходів, спрямованих на захист дітей від насильства і експлуатації в кіберпросторі та сприяти розумінню важливості їх дотримання.

Час: 30 хв.

Необхідні матеріали: Додаток 2.1.3.1.4, аркуші А4, маркери.

Хід проведення:

Тренер/тренерка об'єднує учасників у пари та надає кожній парі роз'яснення одного із принципів із Додатка 2.1.3.1.4, аркуш паперу А4 та маркери. Учасники протягом десяти хвилин мають ознайомитись із принципом та схематично або ребусом мають зобразити його на аркуші паперу. Після закінчення часу роботи в парах учасники по черзі презентують свої напрацювання. Інші учасники спочатку мають здогадатись по зображенню, про який принцип йдеться. Після цього пара учасників, яка з ним працювала, розкриває його зміст.

Запитання для обговорення:

- *Чому важливо дотримуватись принципів під час профілактичної діяльності, спрямованої на захист дітей від насильства і експлуатації в кіберпросторі?*
- *Як ви відреагуєте, якщо помітите під час проведення профілактичного заходу в школі з питань безпеки в інтернеті та зокрема після наведення вами прикладу кібербулінгу з історії життя Аманди Тодд, що одна із учениць плаче?*

Тестові питання до заняття:

1. Яку тематику мають охоплювати профілактичні заходи для захисту дітей від насильства та експлуатації в кіберпросторі?

А) цифрова грамотність дітей;

Б) приклад шкоди, якої можна зазнати в цифровому середовищі;

В) правила безпеки в інтернеті та контакти звернення по допомогу;

Г) усі відповіді правильні.

2. Формою проведення заходу загальної профілактики для захисту дітей від насильства та експлуатації в кіберпросторі може бути:

А) соціальна реклама;

Б) спеціалізований чат-бот;

В) тематичний квест;

Г) усі відповіді правильні.

3. З якого віку рекомендовано інформувати в школі дітей про особливості безпечної поведінки в інтернеті та соцмережах?

А) 1-2 класи;

Б) 3-4 класи;

В) 5-8 класи;

Г) 9-11 класи.

4. День безпечного інтернету відзначається:

А) 18 листопада;

Б) 01 червня;

В) у вівторок другого тижня лютого;

Г) у суботу першого тижня жовтня.

5. Який принцип наголошує на важливості врахування індивідуальних характеристик цільових груп під час планування та проведення профілактичних заходів з питань безпеки в інтернеті?

А) позитивної атмосфери;

Б) наукової обґрунтованості;

В) участі;

Г) доступності інформації.

Ключі-відповіді:

1. Г; 2. Г; 3. А; 4. В; 5. Г.

Додаток 2.1.3.1.1

Поліція, згідно з покладеними на неї завданнями, відповідно до п. 1 ч. 1 ст. 23 Закону України «Про Національну поліцію», здійснює превентивну та профілактичну діяльність, спрямовану на запобігання вчиненню правопорушень.

Відповідно до національного законодавства, уповноважені підрозділи органів Національної поліції зобов'язані виявляти причини та умови, що сприяють вчиненню правопорушень дітьми, вживати в межах своєї компетенції заходів з їх усунення; брати участь у правовому вихованні дітей (ст. 5 Закону України «Про органи і служби у справах дітей та спеціальні установи для дітей»).

В Інструкції з організації роботи підрозділів ювенальної превенції Національної поліції України, зокрема у п. 2 Розділу II, йдеться про профілактичну роботу ювенальних поліцейських та їх основні повноваження:

- планування і реалізація профілактичних заходів у дитячому середовищі щодо запобігання негативним явищам серед дітей;
- вжиття заходів для запобігання і припинення стосовно дитини будь-яких протиправних діянь;
- участь у профілактичних заходах щодо запобігання дитячій бездоглядності та правопорушенням серед дітей.

Поліцейські підрозділи ювенальної превенції відповідно до їх компетенції:

- надають рекомендації батькам або їхнім законним представникам щодо запобігання правопорушень, вчинених дітьми та стосовно них, поширення негативних явищ у дитячому середовищі;
- організовують профілактичні заходи для дітей спільно з іншими уповноваженими органами та підрозділами Національної поліції України, а також із заінтересованими органами державної влади, місцевого самоврядування, об'єднаними територіальними громадами, громадськими організаціями.

Додатково до повноважень представників відділів/секторів ювенальної превенції належать:

1. складання та виконання плану заходів з індивідуальної профілактики в роботі з дітьми, схильними до правопорушень, які перебувають на обліку у підрозділах ювенальної превенції;
2. проведення ознайомлювальних, попереджувальних і виховних бесід з ними та їхніми батьками, законними представниками, членами сім'ї з метою усунення причин та умов, які сприяли вчиненню дитиною адміністративного чи кримінального правопорушення;
3. залучення дітей, які перебувають на обліку в ювенальній превенції, до участі в просвітницько-профілактичних чи корекційних програмах.

Варто звернути увагу на те, що профілактика не обмежується лише впливом на поведінку дитини, а й передбачає виявлення й усунення причин/факторів та умов, що сприяють протиправній поведінці.

Поняття захисту дітей в цифровому середовищі не має універсального закріпленого визначення, проте передбачає цілісний підхід до нього та комплекс заходів, спрямованих на забезпечення безпеки дітей в кіберпросторі з урахуванням їхнього віку.

Основні аспекти захисту дітей в цифровому середовищі передбачають:

- навчання дітей безпечної поведінки в мережі, розвиток цифрової грамотності, критичного мислення;
- використання технічних засобів для обмеження доступу до небезпечних сайтів, контактів, блокування небажаного контенту;
- залучення батьків, освітян та інших дорослих з метою надання необхідної інформації та створення безпечного простору для дітей;
- розроблення та впровадження відповідного законодавства та політик, спрямованих на убезпечення дітей в цифровому середовищі та забезпечення їхнього правового захисту.

Загальна мета полягає у створенні безпечного й позитивного онлайн-середовища, яке діти можуть використовувати для навчання та розвитку, не наражаючись на ризики потрапити під вплив негативного вмісту або в небезпечні ситуації.

Відповідно до аналітичного звіту «Сексуальне насильство над дітьми та сексуальна експлуатація дітей в інтернеті в Україні» за результатами дослідження, проведеного у 2020 році МБО «Служба порятунку дітей» у партнерстві із Уповноваженим Президента України з прав дитини, сформовані **рекомендації для організації роботи з дітьми:**

- інформувати дітей про особливості безпечної поведінки в інтернеті та соцмережах, зокрема з молодшої школи – 1-2 класи;
- додати до навчання дітей інформацію про безпечне та гігієнічне користування соціальними мережами (навички блокування акаунтів, подання скарги у службу підтримки, налаштування власного акаунту, як приватного, тощо), також розпочати з молодшої школи;
- додати до навчання дітей інформацію про технічну безпеку перебування в інтернеті – захист власних даних, важливість запам'ятовування паролів, видалення власних сторінок тощо, використання захисних функцій соцмереж, можливо у форматі тренінгів з відпрацюванням навичок;
- інформувати дітей про наявність сексуального контенту з молодшого шкільного віку з метою зменшення випадків непідготовленого знайомства та зниження ризику ранньої травматизації;
- інформувати про можливі варіанти ситуацій сексуального насильства та експлуатації, знижуючи стигматизованість теми та готуючи ґрунт для подальшої готовності діяти активно у ситуаціях зустрічі з сексуальним насильством/експлуатацією;
- збільшити роботу з хлопцями – акцент на важливості розповідати, що з ними сталось;
- збільшити роботу із дітьми середнього віку (10-13 років), як з більш уразливою категорією, їхні дії на ситуації сексуального насильства ближчі до дітей старшого віку, тоді як емоційні реакції – ще ближчі до дітей молодшого віку;
- підготувати алгоритми для реагування на ситуації сексуального насильства/експлуатації, а особливо у випадках, коли акт насильства коїть знайома у реальному житті доросла людина;
- розробити алгоритм активного захисту від ситуацій сексуального насильства, включивши мотивацію захисту інших дітей;
- розробити алгоритм реагування для ситуацій, коли дитина знає про ситуації насильства свого друга/подруги, але та дитина не може звернутись до близьких дорослих (так як діти переважно діляться тим, що з ними трапилось з друзями, варто залучити дітей як важливих учасників процесу захисту дітей від насильства).

Додаток 2.1.3.1.2

Профілактична робота з дітьми може бути проведена в різноманітних формах та методах – ігрових, освітніх, інформаційних та соціально-психологічних.

Рекомендовані для дітей заходи:

- **відеолекторії/уроки-презентації** з переглядом навчальних відео та інших фрагментів про ризики в онлайн, обговорення їх особливостей та способів запобігання;
- **квести,** коли, наприклад, діти шукають «скарби» – зашифровані повідомлення з порадами про безпечне користування інтернетом, або стають «кібердетективами», котрі мають розкрити кіберзлочин, визначити, що є правдою, а що – міфом, інші види квестів, зміст яких залежить від ідей організаторів;
- **уроки-зустрічі** з представниками поліції чи іншими запрошеними експертами, які можуть поділитися професійним досвідом виявлення та запобігання онлайн-загрозам;
- **тренінгові та інтерактивні заняття** з ігровими вправами, практичними завданнями, розглядом ситуацій, що обов'язково передбачають обговорення й допомагають засвоєнню та застосуванню знань;
- **дискусійні групи/дебати**, під час яких учні обговорюють актуальність кібербезпеки, діляться досвідом, шукають відповіді на суперечливі запитання, наприклад, чи може бути світ без насильства, або чи можна убезпечити дітей від загроз, заборонивши їм користуватися інтернетом, тощо;
- **рольові ігри**, під час яких діти моделюють уявні ситуації та напрацьовують безпечні стратегії інтернет-спілкування, граючи роль доброго друга/подруги, який/яка підтримує нас в разі онлайн-загроз, або негативних персонажів, які нам шкодять або маніпулюють нами;
- **індивідуальні зустрічі та консультації**, під час яких обговорюється конкретна ситуація, що сталася з дитиною, визначаються потенційні загрози, способи їх уникнення і реагування на них.

Також можна запропонувати дітям розробити проєкт чат-боту або застосунку, який надає поради та інструменти для безпечного користування інтернетом, має функції блокування небажаних вебсайтів, перевірки паролів тощо, або зняти відеоролик, підготувати брошуру, комікс, інші інформаційні матеріали з питань кібербезпеки.

Усі заходи мають відповідати віковим особливостям учнів та зацікавлювати їх, сприяти ефективному засвоєнню ними навчального матеріалу.

Під час планування та проведення заходів загальної профілактики серед дітей рекомендовано впроваджувати матеріали, рекомендовані Міністерством освіти і науки України. Зокрема, на сайті Міністерства освіти і науки України міститься низка посилань на ресурси, які рекомендовано використовувати під час здійснення запобігання правопорушенням серед дітей, зокрема булінгу, безпеки дітей в інтернеті тощо. Міністерство освіти і науки України також рекомендує навчальний посібник із безпеки дітей в інтернеті, розроблений компанією Google у співпраці з організаціями The Net Safety Collaborative та Internet Keep Safe Coalition.

Міністерство освіти і науки України приділяє увагу проведенню профілактичних заходів в закладах освіти, зокрема в пам'ятні дні:

День безпечного інтернету (SID/ДБІ) (англ. Safer Internet Day), який з 2004 року відзначається *у вівторок другого тижня лютого*, запровадили мережі Insafe та INHOPE за підтримки

Європейської комісії для просування безпечного та позитивного використання цифрових технологій, особливо дітьми й молоддю. Зараз він відзначається у близько 170 країнах та на шести континентах у світі. Національний комітет Дня безпечного інтернету в Україні представляє Центр кращого інтернету.

> ***До уваги!*** *Слід наголосити, що Центр кращого інтернету занепокоєний тією кількістю фотографій та відео дітей, яка розповсюджуються онлайн, зокрема і протягом Дня безпечного інтернету в Україні, поважає право людини та приватність і не заохочує публікацію фотографій та відео дітей, на яких їх можна ідентифікувати, і які поширені у будь-який спосіб без попередньої письмової згоди їхніх батьків або осіб, які їх замінюють.*

Європейський день захисту дітей від сексуальної експлуатації та сексуального насильства (18 листопада). Завданнями проведення заходів до Європейського дня захисту дітей від сексуальної експлуатації та сексуального насильства є:

- підвищення обізнаності громадськості щодо проблеми сексуального насильства над дітьми, виявлення випадків насильства, їх запобігання та допомоги дітям, які постраждали від сексуального насильства;
- сприяння відкритій дискусії про захист дітей від сексуальної експлуатації та сексуального насильства;
- недопущення стигматизації постраждалих осіб і надання їм допомоги.

Більшість матеріалів громадської організації «Ла Страда-Україна» мають схвалення до використання в закладах освіти від Міністерства освіти і науки України, тому можуть використовуватись поліцейськими під час організації заходів загальної профілактики: https://la-strada.org.ua/biblioteka. Крім того, саме при даній громадській організації працює **Національна «гаряча лінія» для дітей та молоді – 116 111**, про яку варто нагадувати дітям під час проведення заходів загальної профілактики. Доцільно інформувати дітей про можливість отримати консультацію від фахівців цієї «гарячої лінії» також в Інстаграм (childhotline_ua) та Телеграм (CHL116111).

Так само схвалено Міністерством освіти і науки України до використання у закладах освіти **профілактичні програми «Будуємо майбутнє разом» та «Школа і поліція».**

«Будуємо майбутнє разом» – програма профілактики конфліктів та правопорушень серед учнівської молоді від 14 до 18 років. Чотири тренінгові модулі Програми спрямовані на формування належного рівня усвідомленості підлітками, молодими людьми власної ціннісної сфери, розуміння та прийняття цінностей іншої людини, почуття відповідальності за власне життя, а також на оптимізацію процесу постановки життєвих цілей та пошуку способів їх досягнення, підвищення рівня вмотивованості до позитивних змін, розвиток активної життєвої позиції.

Програма **«Школа і поліція»** розроблена для роботи з учнями 1–11 класів та спрямована на формування у них правослухняної поведінки, запобігання конфліктам та правопорушенням. Зокрема програма охоплює і такі заняття, як «Протидія булінгу в дитячому середовищі», «Безпечний інтернет», «Запобігання насильству над дітьми».

До просвітницько-профілактичної діяльності важливо залучати партнерів. Доцільно **сформувати базу даних організацій, які працюють у громаді**, з якими можна взаємодіяти під час планування та проведення профілактичної роботи, а також направляти до них осіб для отримання необхідної допомоги.

До уваги! *Зазвичай громадські, міжнародні та неурядові організації мають фінансові, людські та експертні ресурси для проведення якісних інформаційно-просвітницьких кампаній, тому їх доцільно залучати до планування заходів, які посилять поліцейську діяльність у сфері профілактики.*

Формуючи банк даних громадських та неурядових організацій, важливо враховувати:

- зміст роботи / послуги (консультування, групові заняття, тренінги, підготовка/поширення інформаційно-просвітницьких матеріалів тощо);
- цільові групи (діти, дорослі, групи ризику, інші), з якими працюють організації.

Рекомендовані ресурси громадських організацій

Громадська організація «Всеукраїнський громадський центр «Волонтер» розробила настільну гру «Коло безпеки», яка активно використовується багатьма фахівцями, зокрема і поліцейськими, для інформаційно-просвітницьких заходів в закладах освіти, спрямованих на формування системи уявлень та знань щодо феномену насильства, форм та методів його попередження та подолання, а також звернення за допомогою у разі ризику ситуації насильства або безпосереднього випадку. Ознайомитися з цією грою можна за посиланням: https://volunteer.kyiv.ua/publikaciyi#gallery-8.

Поліцейські під час здійснення загальної профілактики можуть використовувати також інші ресурси даної громадської організації за посиланням: https://volunteer.kyiv.ua/publikaciyi.

Національна інформаційна кампанія ТЯМ, що була проведена у 2021 р. Українським фондом «Благополуччя дітей» за фінансування Ради Європи, спрямована на привернення уваги батьків і освітян до проблеми сексуального насильства над дітьми онлайн та офлайн і підвищення рівня обізнаності підлітків 13–17 років, освітян і батьків про культуру безпеки, яка захищає від насильства. Сторінка «Школи безпеки ТЯМ» доповнена оригінальними матеріалами для підлітків (картки з правилами безпечної поведінки офлайн та онлайн), відеокурсом для освітян, які працюють в темі профілактики насильства, та порадником для батьків з побудови довірливих взаємин із підлітками.

Також можна скористатись іншими практичними напрацюваннями фахівців **Українського фонду «Благополуччя дітей»**, зокрема: методичний посібник «Формування навичок безпечної поведінки дітей»; матеріали кампанії «Уважні батьки»; інформаційно-методичний посібник «Сексуальне насильство над дітьми: причини, наслідки, профілактика»; відеолекція «Сексуальне насильство над дітьми: форми та ознаки»; методичний посібник «Навчіть дитину захищатися»; листівка для батьків «Навчіть дитину правила «Тут мене не торкайся»; брошура для батьків «Навчіть дитину правила «Тут мене не торкайся»; брошура для батьків та дітей «Я можу себе захистити»; відеокурс для батьків «Навчіть дитину захищатися»; мультфільм «Розкажи дорослому, якому довіряєш»; відео (щодо проблеми секстингу) «Історія Юльки» та «Історія Матеуша»; відео (щодо проблеми грумінгу) «Уважні батьки».

Stop_sextинг – проєкт для підлітків, батьків та вчителів щодо захисту дітей в інтернеті від сексуального насильства та експлуатації. Має офіційний сайт та сторінки у соціальних мережах, а також освітню платформу, на якій можна знайти корисний контент для батьків та освітян: матеріали для проведення уроків, методичні посібники, тематичні книги та фільми, VR-квест, онлайн-виставку та останні новини. Крім того, на платформі працює запис на консультацію з психологом та портал повідомлень про матеріали, що зображують сексуальне насильство над дітьми. Портал працює як лінія звітування: ці повідомлення

допомагають захистити дітей та не допустити їх подальшої сексуальної експлуатації. Також в межах цього проєкту було розроблено методичні рекомендації для проведення уроку на тему: «Інтимне селфі в інтернеті – жарт чи небезпечний ризик?», які також можуть використовувати поліцейські під час проведення профілактичних заходів з дітьми. Також розроблений посібник з рекомендаціями для слідчих, прокурорів та суддів щодо імплементації національного законодавства та міжнародних рекомендацій. Крім того, ця організація підтримує діяльність чат-боту з питань безпечного користування інтернетом.

Сайти інших організацій та проєктів, дотичних до теми безпеки в інтернеті:

- сайт Ради Європи: https://www.coe.int/en/web/portal.
- сайт офісу Ради Європи в Україні: https://www.coe.int/uk/web/kyiv.
- координатор проєктів ОБСЄ в Україні: https://www.osce.org/uk/project-coordinator-in-ukraine, за сприяння якого зокрема було розроблено навчально-методичний посібник «Онлайк», який містить теоретичний матеріал про безпечну поведінку в інтернеті, опис занять і тренінгових вправ з розвитку компетентностей безпечної поведінки в інтернеті.
- сайт Уповноваженого Верховної Ради України з прав людини: http://www.ombudsman.gov.ua.
- сайт Управління Верховного комісара ООН з прав людини: http://www.ohchr.org.
- сайт Департаменту кіберполіції Національної поліції України: https://cyberpolice.gov.ua/.
- сайт Центру кращого інтернету: https://betterinternetcentre.org/.
- офіційна сторінка Дня безпечного інтернету в Україні у Фейсбуці: https://betterinternetcentre.org/?page_id=30.
- сервіс з порадами з цифрової безпеки для кожного гаджета та операційної системи: https://yak.dslua.org.
- сервіс для звернень з питань онлайн-безпеки в режимі реального часу: https://nadiyno.org/.

Додаток 2.1.3.1.3

Тактики маніпулювання, які можуть використовувати особи, які вчиняють насильство та експлуатацію дітей в кіберпросторі

- реципрокація: «Я покажу тобі, якщо ти мені покажеш»;
- встановлення дружби або романтичних стосунків в онлайн-середовищі;
- використання кількох онлайн-ідентифікацій проти певної дитини: як особа, яка примушує або вимагає контент сексуального характеру, а також як друг/подруга, який підтримує постраждалу;
- прикидатися молодшим;
- прикидатися жінкою, коли насправді є чоловіком;
- доступ до онлайн-облікового запису дитини (наприклад соціальні мережі) без авторизації та крадіжка сексуального контенту;
- запис дитини без відома під час відеочату;
- спочатку щось пропонувати дитині, наприклад гроші або наркотики в обмін на матеріали сексуального характеру;
- вдавати, що працює в модельному агентстві або є авторитетною особою.

У випадку фінансово вмотивованих злочинців матеріал сексуального характеру зазвичай створюється на основі згоди, як відповідь на привабливе онлайн-повідомлення та маніпулятивні техніки. Це може включати використання попередньо записаного матеріалу, що часто створюється за допомогою спеціального програмного забезпеченням або отримується з порнографічних вебсайтів.

Поширеною тактикою отримання первинного сексуального матеріалу є погрози опубліковати раніше отриманий контент сексуального характеру в інтернеті, розмістивши його в місці, де його можуть побачити родина та друзі.

Інші тактики включають:

- фізичні погрози завдати шкоди або вчинити сексуальне насильство над дитиною або її членам сім'ї;
- погрози покінчити життя самогубством;
- погрози створити контент сексуального характеру за участю дитини за допомогою засобів цифрового редагування;
- створення фальшивого профілю дитини та погрози розміщувати контент сексуального характеру за її участю;
- збереження відверто сексуальних розмов з дитиною та погрози опублікувати їх в інтернеті.

Додаток 2.1.3.1.4

Готуючи профілактичні заходи та програми, важливо пам'ятати про такі **принципи:**

Інтернет є значущою складовою частиною життя сучасних дітей і важливим чинником їхньої соціалізації.

Саме тому слід пояснювати дітям, на які віртуальні та реальні загрози вони наражаються та як їм запобігати. Під час проведення заходів варто враховувати позитивний вплив певних видів інтернет-діяльності на розвиток творчих здібностей, пошук навчальних матеріалів, підтримку зв'язку з рідними, друзями, інше.

Використовуючи інтернет, дитина навмисно або випадково може стати або постраждалою особою, або спостерігачем, або навіть кривдником, а отже – джерелом небезпеки для інших.

Тому зміст освітніх заходів та програм має орієнтувати учнів на визначення цінностей, навчати їх самоаналізу, зокрема власної поведінки в інтернеті. Досвід профілактичної діяльності показує, що недостатньо уваги приділяється тим, хто стає свідком (спостерігачем), адже їхня роль може бути вирішальною у випадках насильства в інтернеті. До прикладу, припинити потенційно небезпечну ситуацію може навіть висловлення осуду чиєїсь агресивної поведінки або повідомлення про неї модераторові/адміністраторові платформи, а також підтримка постраждалої особи, надання їй контактної інформації організацій чи фахівців, які можуть допомогти. Важливо наголошувати, що діти-свідки жодним чином не повинні виправляти ситуацію та брати на себе відповідальність за скоєне іншими.

Доцільно до окремих заходів (програм) залучати дітей-кривдників, які, вчиняючи насильство в інтернеті, були помічені чи перебувають на обліку внаслідок вчинення булінгу, кібербулінгу.

Взаємодія освітнього закладу та поліції має бути чітко скоординованою та реалізовуватися із залученням батьків.

Це передбачає підвищення обізнаності освітян та батьків/осіб, які їх замінюють, з питань загроз та механізмів захисту дітей від них. Освітяни й батьки мають бути долучені до процесу профілактики, використовувати однакові підходи й інструменти, взаємодіяти між собою та з поліцейськими на базі закладу освіти.

Учні мають брати участь у розробленні та втіленні програм і заходів.

Участь дітей у заходах, які для них і з ними проводяться, є одним із основних прав, закріплених Конвенцією ООН про права дитини, тому є актуальною діяльність поліцейських в організації обговорень, під час яких діти й молодь можуть вільно висловити власні думки про зміст заходів з формування безпечної поведінки в інтернеті та залучатися до їх реалізації. Доцільним є залучення поліцейськими представників шкільного самоврядування до планування таких заходів та спільного їх проведення, наприклад, для учнів молодших класів.

Профілактична робота має бути поєднана з реальним життям дітей.

Під час заходів пропонуйте дітям вільно обговорювати теми, спираючись на їхній особистий щоденний досвід користування мережею, планувати її безпечне використання незалежно від виду діяльності – чи це спілкування, чи замовлення товарів онлайн, чи пошук інформації, тощо.

Заняття 2.1.3.2. Запобігання потраплянню дітей в небезпечні ситуації

Мета: надати знання щодо ведення комунікації з дітьми різних вікових категорій щодо дотримання правил безпеки в інтернеті, а також інструменти для проведення різних форм профілактичних заходів для різних учасників.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Вік дитини та онлайн-ризики	Інформаційне повідомлення	15 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 2.1.3.2.1
2.	Історія, яку ми пишемо	Рольова гра	40 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери
3.	Формати роботи	Робота в групах	35 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 2.1.3.2.2

ХІД ЗАНЯТТЯ

1. Інформаційне повідомлення «Вік дитини та онлайн-ризики»

Мета: ознайомити учасників з важливістю врахування віку дитини під час профілактики онлайн-ризиків.

Час: 15 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 2.1.3.2.1.

Хід проведення:

Тренер/тренерка, попередньо ознайомившись із Додатком 2.1.3.2.1, наголошує, що під час профілактики онлайн-ризиків серед дітей важливо враховувати особливості їхнього розвитку залежно від віку.

До уваги тренера/тренерки!

Важливо фіксувати на фліпчарті ключові аспекти своєї доповіді. Який саме матеріал фіксувати визначає тренер/тренерка самостійно.

Запитання для обговорення:

- *Як діти різних вікових категорії по-різному сприймають онлайн-світ?*
- *Враховуючи вікові особливості дітей, щодо яких онлайн-ризиків більш уразливі діти молодшого, середнього та старшого шкільного віку?*

2. Рольова гра «Історія, яку ми пишемо»

Мета: покращити навички комунікації з дітьми та дорослими щодо потенційних онлайн-ризиків, які можуть трапитися з дітьми, виробити правила безпечного поводження у мережі.

Час: 40 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери.

Хід проведення:

Тренер/тренерка об'єднує учасників у групи по 3-4 особи. Далі потрібно підготувати та розіграти у ролях ситуації, які можуть виникнути з дітьми в онлайн-просторі.

До уваги тренера/тренерки!

Важливо, щоб перед початком роботи над ситуацією учасники визначилися із віковою категорією дитини (молодшого, середнього, старшого віку).

Приклад 1: це може бути ситуація, коли дитина отримує запрошення про зустріч офлайн від незнайомця у соціальній мережі. У цьому випадку ролі будуть розподілятися так: один учасник грає роль дорослого, який починає комунікацію. Другий учасник виконує роль дитини. Третій учасник грає поліцейського, який аналізує ситуацію, спілкується з «дитиною» та дає поради. Четвертий учасник може грати роль тата/мами дитини та відіграє реакцію батьків на цю ситуацію.

Приклад 2: дитина отримує повідомлення від незнайомця з проханням надіслати свої оголені фото. Один із учасників грає роль незнайомця, який пропонує свій варіант розвитку подій. Другий учасник грає роль дитини, яка має реагувати на цю ситуацію. Третій учасник грає роль поліцейського, який спілкується з дитиною та пропонує їй правила поведінки в інтернеті.

Час на підготовку ситуацій та розподіл ролей – 15 хвилин. Решта часу – це представлення своїх історій та відігравання ролей відповідно до ситуацій.

Після закінчення презентації кожна група має представити два правила безпеки в інтернеті для відповідної вікової категорії дітей, які тренер/тренерка запишуть на фліпчарті.

Запитання для обговорення:

- *Які складнощі можуть виникнути у процесі комунікації з дитиною?*
- *Як можна змінити цю вправу для проведення профілактичного заходу з дітьми?*

До уваги тренера/тренерки!

Доцільно обговорити з учасниками можливість модифікації цієї вправи і проведення її з дітьми у форматі форум-театру.

3. Робота у групах «Формати роботи»

Мета: обговорити формати превентивної роботи з дітьми, батьками, вчителями та адміністрацією закладів освіти.

Час: 35 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 2.1.3.2.2.

Хід проведення:

Тренер/тренерка об'єднує учасників у групи, відповідно до кількості, та повідомляє їм тему для підготовки матеріалів, наприклад:

група 1 – форми профілактичної роботи з дітьми молодшого шкільного віку;

група 2 – форми профілактичної роботи з дітьми середнього шкільного віку;

група 3 – форми профілактичної роботи з дітьми старшого шкільного віку;

група 4 – форми профілактичної роботи з вчителями та адміністрацією закладу освіти;

група 5 – форми профілактичної роботи з батьками дітей.

Кожній групі пропонується створити список можливих форм профілактичної роботи з їхньою цільовою аудиторією. Список має бути представлений для інших учасників у вигляді постера або малюнка.

Час на роботу в групах – 15 хвилин, решта часу – на представлення перед іншими групами своїх результатів роботи та загального обговорення.

До уваги тренера/тренерки!

За потреби можна додати фактор змагання: оцінювання робіт команд іншими командами.

Під час загального обговорення доцільно використовувати інформацію із Додатка 2.1.3.2.2.

Тестові питання до заняття:

1. Для якої вікової групи дітей характерно те, що вони намагаються знайти відповіді на свої питання щодо сексуальних стосунків, найчастіше шукають інформацію в інтернеті, питають у «старших друзів» в мережі чи дивляться порнографію?

А) старший шкільний вік;

Б) середній шкільний вік;

В) молодший шкільний вік.

2. Це період від сформованої статевої ідентичності до початку статевого дозрівання, що характеризується виникненням інтересу до протилежної статі і виявляється у своєрідному залицянні.

А) старший шкільний вік;

Б) середній шкільний вік;

В) молодший шкільний вік.

3. Про те, що дитина досягла цієї стадії, свідчить поява інтересу до своєї зовнішності, одягу, косметики і прикрас, прагнення виділитися з-поміж однолітків.

А) старший шкільний вік;

Б) середній шкільний вік;

В) молодший шкільний вік.

4. Як ви можете дізнаватися нову інформацію про онлайн-безпеку дітей в інтернеті?

А) підписка на тематичні електронні ресурси, сторінки у соціальних мережах, акаунти експертів;

Б) ознайомлення з результатами новітніх досліджень, відвідування тематичних семінарів;

В) всі відповіді правильні.

5. Чим небезпечне переоцінення дітьми своєї власної компетентності щодо викликів, які можуть трапитися з ними у мережі?

А) діти будуть діяти у мережі більш осмислено та правильно уникатимуть небезпек;

Б) це призведе до того, що профілактичні дії не матимуть ніякого сенсу для дітей;

В) діти думатимуть, що вчиняють у мережі правильно, але насправді не усвідомлюватимуть наслідки своїх дій.

Ключі-відповіді:

1. А; 2. В; 3. Б; 4. В; 5. В.

Додаток 2.1.3.2.1

Вік дитини та онлайн-ризики

Важливо враховувати, що рівень знань та навичок безпечного поводження дітей в онлайн залежить від їхнього віку та досвіду користування мережею. Нижче подано інформацію про необхідні знання й навички, а також про те, що слід брати до уваги, готуючись до зустрічі з дітьми.

Діти початкової школи (1–4 класи) повинні мати базове розуміння безпеки онлайн, що допоможе їм уникнути потенційних ризиків та захистити себе. В цьому віці важливо навчити:

- розуміти основи своєї безпеки в інтернеті, зокрема стосовно персональної інформації, збереження в таємниці паролів, неприпустимості зустрічей з незнайомцями, з якими познайомилися в онлайн-середовищі також, тощо;
- відрізняти безпечні та небезпечні сайти й застосунки, не відкривати невідомих або підозрілих посилань, використовувати безпечні пошукові системи;
- звертатися по допомогу до дорослих, якщо щось стривожило або налякало, виникла неприємна ситуація чи натрапили на шкідливий контент, є потреба спитати або порадитися;
- бути ввічливими, уважними й обережними як у реальному житті, так і онлайн.

Діти, які навчаються у 5-7 класах, вже мають володіти достатньою інформацією про безпеку в інтернеті, оскільки в них більше досвіду користування онлайн-середовищем та, імовірно, були випадки складних ситуацій.

У цьому віці важливо навчити:

- розпізнавати онлайн-небезпеки та способи реагування на них;
- використовувати в соціальних мережах налаштування приватності для захисту персональної та іншої інформації;
- створювати складні паролі для своїх облікових записів, регулярно їх змінювати, користуватися двоетапною перевіркою;
- цінувати свій час, обмежуючи перебування в інтернеті;
- критичному мисленню для розпізнавання неправдивої інформації;
- оцінювати потребу розміщення повідомлень, користуючись «правилом білборда», тож, перш ніж натиснути на кнопку «надіслати»/«опублікувати», подумай, чи хотів (-ла) би ти, щоби це фото/відео/текст/аудіо було на білборді біля твоєї школи (якщо твоя відповідь несхвальна – не поширюй інформації);
- розпізнавати потенційні загрози у відеоіграх з онлайн-гравцями;
- враховувати феномен «ілюзія спальні», коли, перебуваючи вдома у безпечному середовищі, діти й батьки думають, що дітям нічого не загрожує, хоча це не завжди так;
- говорити дорослим про відчуття дискомфорту, якщо щось налякало, була неприємна ситуація в інтернеті, або натрапили на шкідливий контент; запитувати, якщо потрібно;
- застосовувати правила ввічливості, поваги та безпеки в реальному житті та онлайн.

Діти, які навчаються у 8-11 класах, мають більше досвіду в онлайн-просторі, тому можуть більше знати про складні аспекти кібербезпеки.

У цьому віці важливо:

- сформувати уявлення про цифрові сліди та цифрову ідентичність (те, що потрапило в мережу, неможливо видалити, і ми не знаємо, хто й як цим захоче скористатися);

- вміти визначати, що таке онлайн-насильство, які його ознаки та прояви;
- розуміти свої дії в разі онлайн-небезпек – кібербулінгу, секстингу, онлайн-грумінгу;
- знати про «ілюзію спальні» – оманливий феномен, коли, перебуваючи з рідними у фізичній безпеці, діти і батьки думають, що загроз немає. Потрібно пам'ятати, що дії, зроблені онлайн, – можуть мати наслідки в офлайн-світі;
- застосовувати налаштування приватності в соціальних мережах для захисту особистих даних;
- критично оцінювати та перевіряти достовірність інформації;
- обдумувати зміст імовірного контенту перед поширенням і користуватися «правилом білборда», тож спочатку уявити, що фото/відео/текст/аудіо буде розміщено на ньому біля школи, де навчаєшся (якщо твоя відповідь несхвальна – не поширюй інформації);
- володіти інформацією про способи захисту від шахрайства, користуючись онлайн-платежами та іншими фінансовими послугами в інтернеті;
- про ситуації ризиків чи небезпек одразу повідомляти дорослим, яким дитина довіряє, та/або представникам правоохоронних органів;
- обговорювати з підлітками етичні питання, пов'язані з використанням технологій, – цифрову етику, повагу до інших осіб у мережі, відповідальне використання медіа тощо;
- наголошувати на потребі балансу між реальним та онлайн-життям, розпізнавати ознаки цифрової втоми та стресу.

Наведений вище розподіл є умовним. У профілактичній роботі з дітьми важливо розуміти їхні вікові особливості, запити та потреби.

Додаток 2.1.3.2.2

Форми профілактичної роботи

Покращенню власного розуміння основ онлайн-безпеки дітей в інтернеті та сучасних тенденцій стосовно запобіганню насильству щодо них у цифровому просторі допоможе ознайомлення з результатами новітніх досліджень, організація та участь у профільних заходах – семінарах, обговореннях, мозкових штурмів, ініціатив Національної поліції України з цієї тематики.

Доцільно підписатися на електронні ресурси, розсилки на електронну пошту, сторінки у соціальних мережах або на акаунти експертів, щоби ділитися цими знаннями з дітьми, батьками й педагогами на заходах закладів освіти.

Пам'ятайте! Діти сприймають поліцейських (і загалом людей у формі) з особливими почуттями, що викликають захоплення, повагу та відчуття захищеності. Від вас як особистостей та від вашої роботи в закладі освіти залежатиме ставлення дітей до правоохоронних органів загалом. Отож, будьте щирими, відповідально готуйтеся до зустрічей з дітьми, батьками та освітянами, плекайте в собі вмотивованість до такої роботи. Це – вкрай важлива частина вашої професійної діяльності, спрямованої на захист дітей.

Головним методом організації профілактичної роботи є регулярна робота із дітьми всіх вікових груп, а також робота із вчителями, адміністрацією закладу освіти та батьками. Водночас заходи для дітей проводяться відповідно до їхнього віку.

Розглянемо, як представники правоохоронних органів можуть працювати із дітьми, вчителями, адміністрацією закладу освіти та батьками.

Робота з дітьми

- *Проведення заходів у межах навчального закладу.* Наприклад, проведення інтерактивних уроків, де буде демонстрація навчальних відео/аудіо, або показ відео-/фото-/аудіофрагментів, які стосуються конкретних ситуацій в онлайн-світі і пов'язані із реальними випадками із життя та інших форм інтерактивних уроків; проведення квесту для дітей; прослуховування аудіокниги або перегляд відео «Хаппі та її суперсила» та подальше обговорення її з дітьми тощо.

Можлива добірка матеріалів для проведення тематичних уроків та квестів (https://stop-sexting.in.ua/adult/uroky):

- «Моя суперсила – безпека в інтернеті» (1-2 клас)
- Я знаю, як спілкуватись в інтернеті #не_ведусь (5-6 клас)
- #Не_ведусь: ми – герої безпеки в інтернеті (3-4 клас)
- Квест (7-8 клас)
- Квест (9-11 клас)
- Урок онлайн-загрози в час війни: як захистити себе? (1-4 клас)
- Урок онлайн-загрози в час війни: як захистити себе? (9-11 клас)
- #Не_ведись – прояви свою стійкість в інтернеті (5-9 клас)
- Відеоматеріали можете знайти на Ютуб каналі: https://www.youtube.com/@StopSextingUkraine.

Детальніше про рекомендовані для дітей заходи ви можете знайти у Додатку 2.1.3.1.2.

Робота з батьками та особами, які їх замінюють

У проведенні профілактичної роботи з батьками/особами, які їх замінюють, є важливим:

- **своєчасне інформування** про потенційні ризики, на які можуть наразитися діти в мережі, вчасне й ефективне реагування на них;
- **регулярне оновлення знань** батьків, зокрема у межах профілактичної роботи з ними, для більш ефективного впливу на безпеку дітей в цифровому середовищі, що постійно змінюється;
- **створення безпечного середовища,** яке допоможе мінімізувати ризики для дітей у мережі, забезпечити конфіденційність їхніх даних, сприятиме взаєморозумінню між батьками та дітьми для відкритого обговорення цифрових проблеми і спільного пошуку рішень.

Рекомендовані профілактичні заходи з батьками/особами, які їх замінюють:

- **зустрічі з батьками конкретного класу за запитом** для інформування про онлайн-ризики та загрози в мережі, надання практичних порад з безпечного користування інтернетом (наприклад під час батьківських зборів, на вебінарах, виступах);
- **дискусійні групи/дебати**, де батьки можуть поділитися побоюваннями стосовно перебування дітей в кіберпросторі, обговорити суперечливі питання, наприклад, чи доцільна заборона користування інтернетом як найбільш ефективний спосіб убезпечення дітей від загроз, а також поділитися досвідом і стратегіями захисту;
- **тематичні зустрічі з батьками окремо або разом із дітьми,** наприклад, спільні робочі групи, де обговорюються способи подолання проблем, пов'язаних із кібербезпекою, опрацьовуються практичні вправи, які вчать розпізнавати потенційні загрози і вчасно реагувати на них;
- **індивідуальні консультації** для обговорення з поліцейськими конкретних питань, які непокоять батьків;
- **підготовка та розповсюдження брошур** з кібербезпеки, зокрема, як захистити приватність дитини в інтернеті, як діяти, якщо вона постраждала від онлайн-загрози, тощо.

Для забезпечення особистої комунікації доцільно залишити контактні дані працівників поліції, до яких батьки можуть звернутися у разі потреби.

Профілактичні заходи з батьками можуть відбуватися не лише в закладах освіти, а й, зокрема, у бібліотеках, приміщеннях центрів життєстійкості, якщо такі є в громаді, будинках культури та у хабах.

Рекомендації до комунікації поліцейських з батьками/особами, які їх замінюють, з питань безпечної поведінки дітей в кіберпросторі

1. **Будьте відкритими до розмови.** Проявляйте готовність слухати та відповідати на запитання батьків.
2. **Говоріть зрозумілою для них мовою.** Уникайте технічної та іншої термінології, пояснюйте значення складних або малопоширених слів.
3. **Надавайте конкретних порад** для зменшення ризиків у кіберпросторі, наприклад налаштування приватності облікових записів, створення унікальних паролів та їх періодичне оновлення, використання двоетапної перевірки, налаштування фільтрів для блокування небажаного контенту.
4. **Наголошуйте на важливості довірливих стосунків з дітьми**, потребі спілкуватися з ними без критики та агресії, цікавитися тим, що дитина робить в інтернеті, який тип контенту переглядає, створює, надсилає тощо, якими платформами користується, які ігри їй до вподоби, з ким спілкується.

5. **Рекомендуйте корисні ресурси**, де можна більше дізнатися про кібербезпеку, отримати поради, дізнатися про навчальні та розважальні сайти, якими можна користуватися спільно з дітьми (детальніше про це – у темі 4).

6. **Будьте емпатійними.** Батьківство – завжди відповідальне, а особливо – тоді, коли йдеться про захист дітей у цифровому просторі. Підтримуйте зусилля батьків та підкреслюйте їхню значущість у цьому процесі.

Робота з педагогічним колективом

За результатами дослідження ключових компетентностей безпечної поведінки підлітків в інтернеті від 2016 року 50% опитаних зазначили, що отримують інформацію про загрози від викладачів. Це означає, що освітяни є основними партнерами у цьому напрямі, так як саме вони впливають на формування звичок у дітей на щоденному рівні.

Як спрямувати роботу педагогічного колективу на підвищення безпеки дітей в інтернеті

1. Проводити для освітян зустрічі/бесіди/семінари з практичними заняттями.

Це може бути:

- інформування про види і сутність онлайн-загроз (кібербулінг, шахрайство тощо) з поясненням, як ці загрози розпізнати, й надання практичних порад;
- ознайомлення зі способами/засобами забезпечення безпеки дітей в інтернеті (встановлення контент-фільтрів, обмеження часу користування мережею, навчання правил безпечного користування, сприяння відкритому спілкуванню про досвід в онлайн тощо);
- інформування про важливість особистої безпеки (складні паролі, завантаження/оновлення програм з офіційних джерел, встановлення антивірусного програмного забезпечення, блокування екрану для обмеження доступу інших осіб до гаджету);
- обговорення основних тенденцій кіберпростору (збільшення чисельності кіберзлочинів та способи захисту від них; стрімке поширення технологій штучного інтелекту та способів їх застосування; важливість розвитку цифрової грамотності).

Під час проведення таких заходів важливо застосовувати інтерактивні методи навчання, спонукаючи учасників до виконання вправ, участі в дискусіях та обговореннях, що сприятиме засвоєнню та використанню матеріалу у роботі з дітьми.

2. Забезпечити зворотний зв'язок з учителями після проведеного навчання та планування додаткових зустрічей/навчальних заходів.

3. Разом з педагогічним колективом розробити план реагування на онлайн-ризики для швидкої координації дій та визначити осіб, які відповідатимуть за його виконання. Аналізувати потенційні ризики відповідно до віку учнів з урахуванням їхніх освітніх потреб та особливостей користування інтернетом. Визначити способи комунікації з батьками, надати їм інформацію про політику безпеки та план спільних заходів з реагування на ризики.

4. Підтримувати з адміністрацією навчального закладу та педагогічними працівниками постійну комунікацію з питань захисту дітей та їхньої безпеки в кіберпросторі. Обговорювати та погоджувати ініційовані закладом освіти заходи, зокрема превентивні.

5. Запропонувати в навчальному закладі спільну з адміністрацією перевірку усіх елементів онлайн-безпеки, за можливості – із залученням відповідних експертів.

Загальний підхід до організації роботи з освітянами полягає у формуванні освіченої свідомої спільноти, яка має можливості створити безпечне середовище для дітей, ефективно реагуючи на онлайн-загрози.

ТЕМА 2.1.4. Організація роботи з батьками в громаді щодо безпеки в інтернеті

Заняття 2.1.4.1. Профілактична робота поліцейських з батьками щодо безпеки дітей в інтернеті

Мета: сформувати розуміння важливості залучення батьків до забезпечення безпеки дітей в інтернеті та особливості організації та реалізації профілактичної роботи з батьками в громаді.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Актуальність залучення батьків до забезпечення безпеки дітей в інтернеті	Перегляд відео Обговорення	20 хв	Мультимедійне обладнання, відео «Максим вдома?» (https://youtu.be/xzGorKfTzpY), «Злочинці шукають дітей в інтернеті» (https://www.youtube.com/watch?v=e-vsl2Xr5Cw&t=25s&ab_channel=StopSextingUkraine)
2.	Обізнані батьки – захищені діти	Робота в групах	40 хв	Додаток 2.1.4.1.1, фліпчарт, аркуші для фліпчарту, маркери
3.	Планування профілактичних заходів з батьками щодо безпеки в інтернеті	Робота в групах	30 хв	Додатки 2.1.4.1.2, 2.1.4.1.3, фліпчарт, аркуші для фліпчарту, маркери

ХІД ЗАНЯТТЯ

1. Перегляд відео «Актуальність залучення батьків до забезпечення безпеки дітей в інтернеті»

Мета: сприяти усвідомленню учасниками важливої ролі батьків у забезпеченні безпеки дітей в інтернеті, а також надати інформацію про відео як інструмент роботи з батьками щодо безпеки в інтернеті.

Час: 20 хв.

Необхідні матеріали: мультимедійне обладнання, відео «Максим вдома?» (https://youtu.be/xzGorKfTzpY) та «Злочинці шукають дітей в інтернеті» (https://www.youtube.com/watch?v=e-vsl2Xr5Cw&t=25s&ab_channel=StopSextingUkraine.

Хід проведення:

Тренер/тренерка зазначає: «*У межах профілактичних заходів важливим елементом є робота з батьками та особами, які їх замінюють, оскільки вони не завжди усвідомлюють загрози і небезпеки для дітей в кіберпросторі*», та пропонує переглянути відео, після чого звертається до учасників з питанням: «*Які питання варто обговорити з батьками після перегляду цих відео?*»

До уваги тренера/тренерки!

Серед питань, які доцільно обговорити після перегляду відео, можна зазначити такі:

1. Які загрози для дітей в інтернеті існують навіть за умови присутності поряд батьків?
2. До яких наслідків може призвести неуважне ставлення батьків до питань безпеки дітей в інтернеті?
3. Чи приділяють батьки стільки ж уваги питанням безпеки дітей онлайн, як і офлайн? Якщо ні, то чому?
4. Як поліцейські можуть сприяти підвищенню обізнаності батьків з питань безпеки в інтернеті?

Запитання для обговорення:

- *Чи здійснюєте ви профілактичну роботу з батьками щодо безпеки в інтернеті?*
- *Які форми профілактичної роботи ви переважно використовуєте у своїй практичній роботі з батьками? Чому саме їх?*

До уваги тренера/тренерки!

Слід підкреслити важливість взаємодії поліції з батьками у питаннях забезпечення безпеки дітей в інтернеті. Саме батьки можуть допомогти своїм дітям розвинути стійкість, допомагаючи їм підвищити самосвідомість і самооцінку; показуючи їм, що їх приймають і люблять такими, якими вони є; навчаючи їх долати складні ситуації; викликаючи позитивні емоції, знаходити задоволення і гумор в житті; через розвиток навичок вирішення проблем; навчання бути гнучким у своїх відповідях; і показуючи їм важливість співпереживання.

Слід наголосити на доцільності використання відео в роботі з батьками. Проєктом Stop Секстинг створена добірка фільмів про безпеку онлайн, які можна використовувати в формі відеолекторію з батьками.

2. Робота в групах «Обізнані батьки – захищені діти»

Мета: сприяти усвідомленню учасниками важливості обізнаності батьків про основні правила безпеки в інтернеті для дітей та продемонструвати один із можливих інструментів роботи з батьками з цих питань.

Час: 40 хв.

Необхідні матеріали: Додаток 2.1.4.1.1, фліпчарт, аркуші для фліпчарту, маркери.

Хід проведення:

Тренер/тренерка зазначає: «*У межах профілактичної роботи з батьками важливо інформувати їх про правила безпечної поведінки дітей в кіберпросторі. Водночас важливо, щоб батьки усвідомлювали, в яких ситуаціях яке правило має застосовуватись і від яких загроз захищати. Можна проводити відповідну роботу з батьками з використанням ситуаційних завдань*».

Тренер/тренерка об'єднує учасників у п'ять груп та надає кожній із них роздруківку із Додатка 2.1.4.1.1. Учасники в групах протягом десяти хвилин мають ознайомитись із запропонованим діалогом між дітьми та сформулювати правила інтернет-безпеки для дітей, дотримання яких убезпечить їх від подібних загроз. Час на презентацію напрацювань – до трьох хвилин.

Тренер/тренерка під час презентації напрацювань груп фіксує запропоновані правила на аркуші фліпчарту.

Запитання для обговорення:

- *Як ви думаєте, чи обізнані батьки про правила інтернет-безпеки для дітей?*
- *Для чого батькам знати про конкретні правила інтернет-безпеки для дітей?*
- *Про які ще правила інтернет-безпеки доцільно знати батькам?*

3. Робота в групах «Планування профілактичних заходів з батьками щодо безпеки в інтернеті»

Мета: відпрацювати вміння планування профілактичних заходів з батьками щодо захисту дітей від насильства та експлуатації в кіберпросторі, зокрема їх змістовного наповнення.

Час: 30 хв.

Необхідні матеріали: Додатки 2.1.4.1.2, 2.1.4.1.3, фліпчарт, аркуші для фліпчарту, маркери.

Хід проведення:

Тренер/тренерка зазначає: «*Профілактика будь-якої соціальної проблеми чи негативного явища повинна спрямовуватись на особистість людини, яка стикається з певною проблемою, і на соціальне середовище, в якому вона виникає. Тому взаємодія поліції з батьками або особами, які їх замінюють, є вкрай важливою, зокрема для розвитку в них навичок цифрової грамотності, що необхідна для якісної комунікації між батьками та дітьми, взаєморозуміння в питаннях інтернет-безпеки, усвідомлення онлайн-загроз та взаємодії*».

Тренер/тренерка об'єднує учасників у чотири групи та надає завдання спланувати проведення профілактичного заходу для батьків, спрямованого на безпеку в інтернеті, заповнивши таблицю за зразком, який міститься в Додатку 2.1.4.1.2.

Групи 1-2 розробляють профілактичний захід, спрямований на навчання самих батьків цифровій безпеці.

Групи 3-4 розробляють профілактичний захід, спрямований на навчання батьків щодо безпеки дітей в інтернеті.

Час на роботу в групах – 15 хвилин, час на презентацію напрацювань кожної групи – 3 хвилини.

До уваги тренера/тренерки!

Слід наголосити, що проведення профілактичних заходів потребує ретельного планування. Планування є запорукою забезпечення їх ефективності та дієвості. Окрему вагу слід звернути на те, що профілактичні заходи з батьками в громаді не обов'язково проводити в школах. Місцями проведення таких заходів можуть виступати інші публічні простори, зокрема бібліотеки, відкриті простори. Проводити такі заходи доцільно в тематичні дати, наприклад в День безпечного інтернету, однак не обмежуючись ними.

В фокусі уваги під час проведенні профілактичних заходів з інтернет-безпеки мають бути також питання загальної цифрової безпеки, наприклад убезпечення від зараження шкідливим програмним забезпеченням. Деякі поради та правила безпеки щодо цього зазначені в Додатку 2.1.4.1.3. Можна перед або після виконання цієї вправи вивести інформацію з Додатка на екран та запитати в учасників, яким із цих правил та порад важливо навчати батьків, а яким – дітей.

Запитання для обговорення:

- *Які виникали складнощі під час виконання вправи?*
- *Які фактори ви враховували під час обрання змістовного наповнення заходу?*
- *Як часто, на вашу думку, слід проводити профілактичні заходи з батьками щодо безпеки в інтернеті?*

Тестові питання до заняття:

1. Профілактична робота з батьками з питань безпеки дітей в інтернеті передбачає:

А) розвиток навичок цифрової грамотності самих батьків;

Б) навчання батьків щодо методів та способів убезпечення дітей від онлайн ризиків ;

В) усі відповіді правильні.

2. Де можна проводити профілактичні заходи з батьками?

А) лише в закладі освіти під час батьківських зборів;

Б) лише в шкільному кабінеті інформатики;

В) як в закладі освіти, так і в будь-якому іншому публічному просторі.

3. Які форми проведення профілактичних заходів можна використовувати під час профілактичної роботи з батьками щодо безпеки дітей в інтернеті? (можна обрати декілька варіантів відповідей)

А) перегляд та обговорення тематичних відео;

Б) робота з практичними ситуаціями (кейсами);

В) практичне заняття з налаштування параметрів безпеки на мобільних пристроях .

4. Коли доцільно проводити профілактичні заходи з батьками з питань безпеки дітей в інтернеті?

А) на початку кожного навчального року;

Б) виключно в тематичні дати, наприклад до Дня безпечного інтернету;

В) в тематичні дати, але не обмежуючись ними.

5. Що має викликати підозру під час знайомства та спілкування в інтернеті? (можна обрати декілька відповідей)

А) небажання інтернет-знайомого спілкуватися через інтернет-відеозв'язок;

Б) прохання тримати у секреті сам факт спілкування;

В) наполегливе прохання перейти до секретного чату для подальшого спілкування.

Ключі-відповіді:

1. В; 2. В; 3. А,Б,В; 4. В; 5. А,Б,В.

Додаток 2.1.4.1.1

Група 1

Персонаж 1: Ок, я буду у тебе о 17.

Персонаж 2: Ок, я живу на вулиці...

Персонаж 1: (перебиває) Знаю, знаю... Та ж на твоїй інтернет-сторінці зазначено все: і адреса, і список друзів, і навіть ті кав'ярні, де любиш бувати. Адже ти ж завжди використовуєш геолокацією.

Персонаж 2: І що з того?

Персонаж 1: Це необачно й навіть небезпечно: будь-хто зможе не тільки мати всю інформацію про тебе, а й використати її не на твою користь.

Персонаж 2: Не вигадуй... Кому це потрібно?

Персонаж 1: Так думав і мій друг, поки квартиру, де він мешкає з родиною, не обікрали... А все через те, що на інтернет-сторінці він вказав свою домашню адресу та виклав світлину про родинний відпочинок за кордоном.

Правило №1. Не надавай в інтернеті інформацію про місце свого проживання, телефон, номери банківських карток, логіни та паролі. Не зловживай геолокацією.

Правило №2. Закрий сторінку та список друзів від сторонніх осіб.

Група 2

Персонаж 1: Привіт. Підемо сьогодні в кіно?

Персонаж 2: Вибач. Сьогодні ніяк. Зустрічаюсь з моїм інтернет-другом.

Персонаж 1: І давні ви знайомі?

Персонаж 2: Декілька днів, але мені здається, що знаю його все життя. Він такий суперовий... І розуміє мене, як ніхто інший. Мабуть, я закохалась.

Персонаж 1: Ти ж його навіть не бачила. А раптом фото фейкове? Ви спілкувались через відеозв'язок?

Персонаж 2: Ні... Я намагалась йому зателефонувати, але він не відповів через відео... Написав, що не працює камера.

Персонаж 1: Тебе це не здивувало?

Персонаж 2: Всяке буває. З нетерпінням чекаю на нашу зустріч. Він на фото, особливо на наших, секретних, такий мужній...

Персонаж 1: Секретних фото?

Персонаж 2: Так, ми спілкуємось в секретному чаті, обмінюємося різними фотками. Я, правда, іноді ніяковію від його відвертих зображень, та й свої спочатку соромилася надсилати. Але він образився, адже ми ж вже досить дорослі... Ой, я проговорилася тобі, а він просив нікому не говорити!

Персонаж 1: Не хвилюйся, я нікому не розкажу. А ти не боїшся, що він викладе ці фото в інтернеті?

Персонаж 2: Ні, навіщо йому це? У нас все чудово.

Персонаж 1: Знаєш, минулого тижня до нашого класу приходив поліцейський та пояснив, що фото, які потрапили до інтернету, залишаються там назавжди, а отже, будь-хто може ними скористатися: наприклад, розмістити на сайті для дорослих, а потім вимагати грошей за їх видалення, погрожувати тим, що в разі відмови заплатити, надішле фото знайомим… На жаль, такі випадки непоодинокі й у нашому місті.

Правило №1. З обережністю зустрічайтеся та спілкуйтеся з інтернет-знайомими, з якими ніколи не бачились офлайн.

Правило №2. «Правило білборда»: надсилайте до інтернету тільки ті матеріали, які готові побачити на білборді біля школи.

Зауважте! Підозру має викликати таке:

- небажання інтернет-знайомого спілкуватися через інтернет-відеозв'язок;
- прохання тримати у секреті сам факт спілкування;
- обурення у разі відмови надіслати інтимні фото;
- наполегливе прохання перейти до секретного чату для подальшого спілкування;
- перехід до розмов про секс після нетривалого знайомства.

Група 3

Персонаж 1: Привіт. Ти можеш мені позичити 1000 грн?

Персонаж 2: Отакої! Навіщо тобі?

Персонаж 1: Та… потрапив в одну халепу… Я вчора отримав повідомлення, що виграв Iphone 14. Дуже зрадів, хоча і не брав нібито ж участь в розіграшах. Але мені було цікаво – і я перейшов за посиланням. Одразу ж з'явилося повідомлення, що комп'ютер буде заблоковано доти, доки я не перерахую 1000 грн на вказаний рахунок.

Персонаж 2: А ти батькам говорив?

Персонаж 1: Звісно, ні. Та й навіщо? Нічим не допоможуть, тільки насварять.

Правило №1. Не відкривати листи від незнайомих адресатів, не переходити за посиланнями в них. Не встановлювати невідомі програми й застосунки.

Правило №2. Не замовчувати, не приховувати проблему. Звернутися по допомогу до батьків або осіб, яким ти довіряєш. Вони завжди знайдуть вихід із скрутної ситуації.

Група 4

Персонаж 1: Привіт! Чого ти така засмучена?

Персонаж 2: А ти ще не знаєш? Уже всі бачили…

Персонаж 1: ??? (здивований)

Персонаж 2: Пам'ятаєш, на вечірці Максим розлив на мене напій – мій одяг став просвічуватись… Таня саме в цей час зробила фото, яке виклала в Instagram, та ще й позначила мене. Там таке почалось в коментарях… І як тепер до школи йти? Усі будуть глузувати з мене. Хоча й так всі глузують: щодня пишуть мені образливі повідомлення, навіть погрожують вивісити це фото в школі.

Персонаж 1: Не переймайся так, адже не буває безвихідних ситуацій. Нам у таких випадках радили телефонувати на «гарячу дитячу лінію»: 116 111. Там підкажуть, що робити далі.

Правило №1. Не замовчуй про ситуації, які тебе засмучують. По допомогу щодо видалення фото, які тебе компрометують, можеш звернутися до:

- батьків або дорослих, яким довіряєш;
- національної «гарячої дитячої лінії»: 116 111;
- чат-бот проєкту stop_sexting;
- батьків дитини, яка виклала компрометуючий матеріал;
- служби підтримки соціальних мереж або сайтів, на яких розміщені фото.

Правило №2. Не видаляй образливі повідомлення. Зроби з них скріншоти. Це може потім бути використано як доказ.

Група 5

Персонаж 1: (сидить пише в телефоні повідомлення)

Персонаж 2: Привіт! З ким листуєшся?

Персонаж 1: Один інтернет-знайомий все намагається зустрітись, а я не хочу. От і не знаю, як йому про це сказати.

Персонаж 2: Просто заблокуй його. Ти не повинна нічого нікому пояснювати, якщо спілкування тобі неприємне.

Правило №1. У випадку неприємного спілкування в інтернеті, краще заблокувати контакт, ніж пояснювати причини відмови в спілкуванні.

Додаток 2.1.4.1.2

Назва заходу/ активації	Мета та зміст	Цільова аудиторія	Місце проведення	Час проведення	Необхідні ресурси (людські, матеріальні тощо) та їх джерела	Очікувані результати	Аналіз оцінки результатів

Додаток 2.1.4.1.3

Фокуси уваги щодо цифрової грамотності та безпеки

Шкідливе програмне забезпечення. Як захиститися: поради й рекомендації від Europol

- **Обирайте застосунок лише з офіційних джерел**. Перед завантаженням дізнайтесь якомога більше про нього та його видавця. Поцікавтесь рейтингами та відгуками користувачів. Прочитайте про дозволи застосунку. Перевірте, до яких з них він має доступ, і чи може передавати інформацію назовні, а також, чи потрібні йому такі дозволи, і тоді приймайте рішення. Намагайтеся користуватися останніми версіями програмного забезпечення та регулярно оновлюйте операційну систему та застосунки. Завантажуйте оновлення одразу, щойно воно буде запропоновано. Це гарантуватиме підвищення безпеки та продуктивності вашого пристрою.
- **Не відправляйте своїх персональних даних** у відповідь на отримані повідомлення або електронні листи, що нібито відправлені вашим банком чи іншою компанією. Для підтвердження запиту зв'язуйтеся з такими відправниками в інший спосіб. Регулярно переглядайте банківські виписки задля виявлення підозрілих нарахувань. Якщо ви помітили витрати, яких ви не здійснювали, негайно зверніться до постачальника послуг.
- **Не знімайте обмежень безпеки,** визначених розробником операційної системи, для отриманням повного доступу до неї та її функцій.
- **Не входьте за посиланням чи вкладенням в електронні листи чи текстові повідомлення**, надходження яких ви не очікували, та видаляйте їх негайно. Ретельно перевіряйте скорочені інтернет-адреси та QR-коди, що можуть або скерувати вас до небезпечних вебсайтів, або завантажити на ваш пристрій шкідливе програмне забезпечення. Перш ніж натиснути на вебадресу, скористайтесь інструментами, що дають змогу попередньо переглянути сайт.
- **Робіть резервні копії файлів** та зберігайте їх в різних місцях, тим більше що є багато смартфонів та планшетів, здатних до бездротового резервного копіювання. За наявності резервних копій, ви легко відновите свої персональні дані, навіть якщо пристрій загублений, викрадений або пошкоджений.
- **Вимикайте Wi-Fi, служби визначення розташування та Bluetooth**, коли вони не потрібні, адже кіберзлочинці можуть отримати доступ до інформації, якщо з'єднання не захищене. Якщо є змога, замість точок доступу використовуйте передачу даних через підключення 3G або 4G, а також обирайте режим віртуальної приватної мережі (VPN) для шифрування ваших даних під час передачі.
- В разі блокування пристрою вірусом-вимагачем, **не сплачуйте викуп**, не підтримуйте у такий спосіб фінансове шахрайство, не заохочуйте злочинців до подальших незаконних дій.
- Здійснивши платіж, **виходьте з облікового запису**, а вже потім закривайте браузер. Не зберігайте в ньому або в застосунках імена користувачів та паролі. Якщо ваш ґаджет буде загублений або вкрадений, до облікових записів зможе увійти будь-хто. Не користуйтеся банківськими послугами та не купуйте товарів з використанням загальнодоступних мереж Wi-Fi.
- **Використовуйте носії інформації** (USB-флешки, зовнішні жорсткі диски, інші) **лише від офіційних та перевірених виробників або продавців**. Перед підключенням носія до свого комп'ютера чи іншого пристрою перевіряйте наявність підозрілих дефектів чи нестандартних властивостей. Нові носії інформації спочатку перевірте на відсутність вірусів, а

вже потім користуйтеся ними, зберігаючи в безпечному місці без доступу до них випадкових осіб.

- **Завжди критично ставтеся до інтернет-відомостей**. Порівнюйте інформацію з різних джерел та навчіться відрізняти правдиву серед усіх.
- **Майте мінімум персональних даних, доступних у мережі.** Не викладайте фотознімків та відеозаписів, що можуть зашкодити вашій репутації. Якщо це сталося – повідомляйте уповноваженим особам. Вживайте заходів убезпечення вцілілих відомостей.
- **Постійно оновлюйте свої знання у сфері кібергігієни.**

Загальна мета цих рекомендацій – захист особистих даних та мінімізація ризиків їх злочинного використання. Дотримання цих порад підвищить вашу безпеку в інтернеті, збереже ваш особистий простір та захистить особисту інформацію від стороннього втручання.

Заняття 2.1.4.2. Роль батьків у захисті дітей від загроз в інтернеті

Мета: надати учасникам знання щодо ролі батьків у захисті дітей від різних загроз в інтернеті, підвищити їхню обізнаність про можливі інструменти батьківського контролю, а також про інструменти організації роботи з батьками з питань безпеки в інтернеті.

Загальна тривалість: 2 академічні години (90 астрономічних хвилин)

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Угода про правила користування інтернетом як інструмент батьків для захисту дітей від ризиків в інтернеті	Робота в парах	20 хв	Роздруковані примірники угод з Додатка 2.1.4.2.1 за кількістю пар учасників, кулькові ручки, аркуші А4.
2.	Батьківство – це виклик. Будьте пильними, аби чогось не проґавити!	Перегляд відео Обговорення	30 хв	Додаток 2.1.4.2.2, мультимедійне обладнання, відео «Батьківство – це виклик. Будьте пильними, аби чогось не проґавити!»
3.	Причини та шляхи залучення дітей до протиправної діяльності через інтернет, батьківські заходи з протидії	Робота в групах Карусель	40 хв	Додаток 2.1.4.2.3, фліпчарт, аркуші для фліпчарту, маркери

ХІД ЗАНЯТТЯ

1. Робота в парах «Угода про правила користування інтернетом як інструмент батьків для захисту дітей від ризиків в інтернеті».

Мета: надати учасникам інформацію про один із інструментів взаємодії батьків та дітей з питань безпеки в інтернеті, відпрацювати навички його застосування.

Час: 20 хв.

Необхідні матеріали: роздруковані примірники угод з Додатка 2.1.4.2.1 за кількістю пар учасників, кулькові ручки, аркуші А4.

Хід проведення:

Тренер/тренерка зазначає: *«Ризики заподіяння шкоди дітям, пов'язані з використанням цифрового середовища, були поділені мережею «EU Kids Online» на 4С (Content, Contact, Conduct, Contract), серед яких:*

- Ризики контенту: дитина отримує попередньо виготовлений медіаконтент, який може негативно вплинути на неї – наприклад порнографія, зображення з мотивами насильства, контент расистського характеру.
- Ризики контакту: діти можуть брати участь у взаємодіях (зазвичай), ініційованих дорослими, які загрожують їм – наприклад онлайн-грумінг, домагання, експлуатація.
- Ризики поведінки: діти беруть участь (як посередники, постраждалі, або ті й ті, бо ці групи можуть збігатися) у (зазвичай) взаємодіях між однолітками, які можуть виявитися згубними, – наприклад кібербулінг, напади на репутацію в інтернеті, підбурювання до заподіяння собі шкоди, фішинг, гакінг та шахрайство.

- *Ризики угод: діти можуть погодитися на угоди, яких вони не розуміють (бо вони не відповідають вікові або через дизайн вебсайту чи контенту), які є надмірно переконливі, або діти можуть отримати доступ в інтернеті до різних товарів чи послуг (наприклад ножів, наркотиків, азартних ігор тощо).*
- *Зважаючи на значну кількість різноманітних ризиків в інтернеті та неможливість постійно перебувати поруч з дітьми для захисту дітей в кіберпросторі, батькам доцільно використовувати певні інструменти контролю та домовленостей з дітьми. Одним із таких інструментів, крім програм батьківського контролю, може бути підписана Угода про правила користування інтернетом».*

Тренер/тренерка об'єднує учасників у пари, в кожній із яких один із учасників відіграватиме роль дитини, інший – батька/матері.

До уваги тренера/тренерки!

Під час об'єднання учасників в пари доцільно врахувати вік їхніх дітей (у разі наявності). Для цього можна розмістити на стіні роздруковані 4 аркуші з написами: 0-5 років, 6-10 років, 11-14 років, 15-18 років та запросити учасників підійти до того аркушу, напис на якому відповідає віку їхніх дітей. У разі відсутності власних дітей, учасники можуть врахувати вік молодших братів-сестер або підійти до аркушу з написом «0-5 років» (на вибір). Після цього учасники в мінігрупах повинні об'єднатись у пари.

Після об'єднання учасників у пари тренер/тренерка надає кожній парі відповідний примірник угоди із Додатка 2.1.4.2.1 та пропонує протягом десяти хвилин заповнити його з врахуванням завчасно визначеної ролі.

До уваги тренера/тренерки!

Для виконання вправи можна також використати варіанти угод, запропонованих в межах проєкту «Дія.Цифрова освіта», які містяться за посиланнями:

https://osvita.diia.gov.ua/uploads/0/530-ugoda_1.pdf – сімейна угода для контрою часу онлайн.

https://osvita.diia.gov.ua/uploads/0/531-ugoda_2.pdf – сімейна угода щодо безпеки в соціальних мережах.

https://osvita.diia.gov.ua/uploads/0/532-ugoda_3.pdf – сімейна угода щодо безпеки в інтернеті.

Після закінчення часу роботи в парах тренер залучає учасників до обговорення.

Запитання для обговорення:

- *Чи вважаєте ви угоду можливим інструментом батьків для захисту дітей від ризиків в інтернеті? Чому?*
- *З якого та до якого віку слід укладати таку угоду?*
- *Чи варто переглядати таку угоду та як часто?*

2. Перегляд відео. Обговорення. «Батьківство – це виклик. Будьте пильними, аби чогось не проґавити!»

Мета: сприяти усвідомленню учасниками ролі батьків у питаннях захисту дітей від сексуального насильства і експлуатації онлайн, а також надати інформацію щодо ознак, за якими батьки можуть розпізнати, що дитина стикнулася з насильством чи експлуатацією в інтернеті.

Час: 30 хв.

Необхідні матеріали: відео «Батьківство – це виклик. Будьте пильними, аби чогось не проґавити!» https://bit.ly/41ycXEE, мультимедійне обладнання, Додаток 2.1.4.2.2.

Хід проведення:

Тренер/тренерка пропонує переглянути відео та зазначає: *«Це відео було розроблено Українським фондом «Благополуччя дітей» в межах кампанії «Уважні батьки»»*, після чого звертається до учасників з питанням: *«Які питання варто обговорити з батьками після перегляду цього відео?»*.

До уваги тренера/тренерки!

Під час обговорення слід спиратись на матеріал, що міститься в Додатку 2.1.4.2.2.

Запитання для обговорення:

- *Що означає, на вашу думку, «уважне» батьківство?*
- *Чи доцільно батькам перевіряти месенджери дітей без їхнього дозволу?*
- *Чи можуть батьки самі створити загрози для безпеки дитини онлайн?*

До уваги тренера/тренерки!

Під час обговорення сутності уважного батьківства слід звернути увагу на такі ознаки:

- побудова стосунків з дитиною;
- розмови з дитиною, вислуховування дитини;
- інтерес до дитини (її почуттів, мрій, ідей тощо);
- спостереження за дитиною, спроба зрозуміти її поведінку;
- реагування на потреби дитини;
- реагування в ситуації загрози без звинувачень дитини.

Саме розмови та хороші стосунки з дитиною – це ключ до захисту її від багатьох загроз. Розмови на так звані складні теми повинні бути природним, пристосованим до віку елементом повсякденного життя, а не одноразовою подією. Також важливо, щоб вони мали форму діалогу, а не лекції. Важливо пояснити дітям, що справжні довірливі стосунки – це не про інтимні фото чи про особисті таємниці, а про спільні інтереси та цінності, про підтримку та взаєморозуміння. Людина, яка справді дружить з іншою людиною чи має до неї романтичні почуття, не буде вимагати робити те, що іншій людині не хочеться. Ми завжди можемо сказати іншій людині про те, що її прохання ми не будемо виконувати, бо маємо певний острах, чи це не збігається з нашими цінностями, і це нормально, через такі обмеження дійсно довірливі стосунки не мають закінчуватися. Батькам доцільно навчити дитину використовувати **тест «білборда»** у ситуаціях, коли ми не можемо одразу визначити правильну дію в мережі: вчити дитину уявляти те, що вона хоче опублікувати чи надіслати, на білборді поруч зі школою чи домом. Якщо це викликає негативні емоції, то значить цей матеріал не підходить для надсилання чи публікації.

Доцільно поінформувати учасників про сторінку кампанії «Уважні батьки» Українського фонду «Благополуччя дітей»: https://childfund.org.ua/diialnist/kampaniia-uvazhni-batky та спонукати їх поширювати інформацію про навички уважного батьківства.

Батьків слід застерігати від того, щоб вони зламували акаунти дітей чи перевіряли месенджери без дозволу. Натомість варто навчити дитину тому, як розпізнати особу, з якою вона познайомилась онлайн. Можна перевірити таку інформацію щодо особи, з якою познайомилися онлайн: акаунти в інших соціальних мережах; частоту й історію публікацій онлайн, інформацію про школу та знайомих нового онлайн-друга, а також групи, до яких він чи вона належить; взаємодію з іншими знайомими; готовність побачитися за допомогою вебкамери чи іншого застосунку, який забезпечує відеозв'язок. У контексті небезпечних контактів варто також говорити з дитиною на теми, пов'язані із захистом

приватності онлайн – звернути увагу на те, що інформація (зокрема дані, фото, відео), яку вона про себе публікує в мережі, впливають на її безпеку.

Батьки не лише відіграють вирішальну роль у захисті особистого життя їхніх дітей в інтернеті, але й можуть загрожувати їхній конфіденційності. **«Шерентинг»** (англ. – «*Sharenting*») – це слово, утворене від слів «ділитися» (*share*) та «батьківство» (*parenting*). Воно означає явище, коли батьки діляться інформацією про своїх дітей, фотографіями, наприклад у блогах чи соціальних мережах, таких як Фейсбук, Інстаграм чи Ютуб. Звісно, переважно батьки роблять це з хорошими намірами, тому що пишаються своїми дітьми або хочуть поділитися досвідом з іншими батьками щодо чудових, але іноді й складних аспектів батьківства. Деякі батьки діляться лише зрідка, інші – діляться майже всім, що відбувається в їхньому повсякденному житті. Діти, особливо коли дорослішають, не завжди почуваються комфортно через інформацію, яку поширюють їхні батьки. Іноді виникають конфлікти між правом дитини на особисте життя та правом на свободу вираження поглядів батьків. Незалежно від обставин батьки повинні пам'ятати про найкращі інтереси дитини та обговорювати з дитиною те, чим вони діляться і чому.

4. Робота в групах. Карусель. «Причини та шляхи залучення дітей до протиправної діяльності через інтернет, батьківські заходи з протидії»

Мета: актуалізувати знання учасників про причини, шляхи залучення дітей до протиправної діяльності через інтернет, заходи батьків щодо протидії, а також надати практичні інструменти для організації профілактичної роботи з батьками з питання безпеки дітей в інтернеті.

Час: 40 хв.

Необхідні матеріали: Додаток 2.1.4.2.3, фліпчарт, аркуші для фліпчарту, маркери.

Хід проведення:

Тренер/тренерка зазначає: «*Одним із сучасних ризиків, з якими можуть зіткнутися діти в інтернеті, є втягнення їх у протиправну діяльність. Це питання особливо актуальне в умовах війни. Кіберпростір стає ще одним фронтом ведення війни, а найбільш уразливими є діти та підлітки, оскільки вони проводять багато часу в мережі, що збільшує ризик зустрічі з небезпекою. Батькам важливо усвідомлювати, чому діти погоджуються на участь у ризикованих ситуаціях, які шляхи втягнення використовують правопорушники, а також, що вони можуть зробити для захисту своїх дітей від цієї загрози*».

Тренер/тренерка об'єднує учасників у три групи та надає кожній із груп аркуш фліпчарту з написом:

група 1 – причини, або чому діти погоджуються;

група 2– шляхи комунікації правопорушників з дітьми, або як знаходять потенційних постраждалих;

група 3 – що можуть зробити батьки для захисту дітей.

Учасники в групах протягом п'яти хвилин обговорюють поставлене питання та зазначають відповіді на аркуші фліпчарту. Через п'ять хвилин групи передають аркуші фліпчарту за годинниковою стрілкою та протягом п'яти хвилин зазначають доповнення до напрацювань іншої групи. Кожна група учасників має попрацювати з кожним аркушем. Після того, як групи знову отримають аркуші, з якими вони починали виконувати цю вправу, тренер пропонує їм презентувати напрацювання. Час на презентацію – до трьох хвилин. Тренер/тренерка доповнює відповіді учасників/учасниць, використовуючи Додаток 2.1.4.2.3.

Запитання для обговорення:

- *Чи можна використовувати цю вправу під час проведення профілактичних заходів з батьками?*

Тестові питання до заняття:

1. У ситуаціях, коли дитина сумнівається, чи доцільно публікувати щось в мережі, доцільно:

А) не публікувати в жодному разі, якщо є сумніви;

Б) застосувати феномен «ілюзії спальні»;

В) застосувати тест «білборда»;

Г) підкинути монетку.

2. Переконання, що нічого не може трапитись онлайн, якщо ми фізично у безпеці, має назву:

А) феномен «ілюзії спальні»;

Б) тест «білборда»;

В) «шерентинг»;

Г) немає правильної відповіді.

3. Якщо батькам стало відомо про те, що дитина зазнає будь-яких проявів насильства чи експлуатації в інтернеті, вони повинні:

А) заборонити дитині користуватись інтернетом;

Б) написати кривднику дитини, що їм відомо про його дії;

В) не звертати уваги, нічого серйозного в інтернеті статися не може;

Г) звернутись із заявою до поліції.

4. Чи правильно, якщо батьки без дозволу переглядають месенджери дитини?

А) звісно, так;

Б) звісно, ні;

В) так, якщо у них є будь-які підозри;

Г) залежить від поведінки дитини.

5. Які зміни в поведінці дитини можуть бути попереджувальними ознаками про небезпечне спілкування в інтернеті?

А) зміни настрою;

Б) страх залишити телефон чи планшет хоч на секунду;

В) стрес та надмірні емоційні реакції в ситуації відсутності доступу до інтернету;

Г) усі відповіді правильні.

Ключі-відповіді:

1. В; 2. А; 3. Г; 4. Б; 5. Г.

Додаток 2.1.4.2.1

за підтримки КИЇВСТАР

реалізатор проєкту STOP sexтинг

Сімейна угода
щодо безпеки в Інтернеті

Ця угода укладена _____ (дата) між:

_____ (ПІБ дитини) _____ (ПІБ батька/матері)

Я можу публікувати/писати на своїй сторінці в соціальних мережах, на форумах, у чатах та переписках .....

(наприклад, інформацію про улюблені музичні гурти)

Я НЕ буду публікувати/писати на своїй сторінці в соціальних мережах, на форумах, у чатах та переписках....

(наприклад, особисту інформацію щодо місця проживання)

Ми домовляємось....

(наприклад, раз на тиждень обговорювати програми, якими найчастіше користуємось і чому саме цими)

Що буде, якщо хтось порушить угоду?

Ми переглянемо та оновимо угоду: _____ (дата)

Наголошуємо, що обом сторонам важливо мати зобов'язання і дотримуватись їх в рамках цієї угоди.

Міністерство цифрової трансформації України

Уповноважений Президента України з прав дитини

Додаток 2.1.4.2.2

Питання, які доцільно обговорити після перегляду відео «Батьківство – це виклик. Будьте пильними, аби чогось не проґавити!»:

1. Що у фільмі привернуло вашу увагу?
2. Чому дівчина піддалася спокушанню?
3. У чому полягає маніпуляція з боку кривдника?
4. Як дівчина почувалася у стосунках із кривдником?
5. Як поводилися батьки дитини?
6. Що могли зробити батьки, щоб уникнути цієї ситуації?
7. Які є попереджувальні ознаки у контексті стосунків онлайн?
8. Що робити батькам, якщо дитина зіткнулась з насильством онлайн?

Важливо, щоб прозвучали такі тези:

- *Дівчина почувалась самотньою.* У потоці щоденних справ та обов'язків часом легко проґавити сигнали, які свідчать про те, що в житті дитини відбувається щось тривожне чи складне, або що вона почувається самотньою. Буває, що дорослі легковажно ставляться до проблеми дитини тоді, як вона її глибоко переживає. У фільмі батьки присутні – відвозять дітей до школи, разом їдять, ходять на прогулянки. Але не помічають, що у дівчини є проблеми з однолітками, сумніви щодо зовнішнього вигляду, її не підтримують.
- *Кривдник використав потреби дитини для маніпуляції.* Кривдник виявив потреби дитини (під час побудови стосунків, а можливо, проглядаючи інформацію про дитину, доступну в мережі) та використав її в маніпуляції, граючи роль друга, людини, яка розуміє проблеми, знаходить час на розмову про них та пропонує підтримку. Відео представляє найбільш типовий, але не єдиний можливий сценарій спокушання. Воно часто супроводжується брехнею кривдника щодо свого віку та намірів, вдаваною увагою до потреб і проблем дитини, розмовами на тему сексу, проханням зберігати стосунки в таємниці, показом еротичних матеріалів, видурюванням фотографій або шантажем чи погрозами задля отримання зображень чи зустрічі.
- *Дівчина повірила кривднику.* Типовий початок маніпуляції дитиною в мережі – здобуття її довіри, а потім ізолювання від найближчого оточення (батьків, друзів). Довіра до кривдника та потреба контакту з кривдником призвела до того, що дівчина наважилася відправити йому свої інтимні фотографії – це чергова типова фаза спокушання.
- *Дівчина відчувала страх і не знала, що робити з шантажем.* Часто після отримання від дитини еротичних матеріалів кривдник вимагає наступних матеріалів або зустрічі з метою сексуального використання. У дітей це викликає страх і почуття безвиході. Багато з них не можуть відповідно відреагувати, а через почуття сорому та страху бояться повідомити про це батькам.
- *У контексті стосунків онлайн можливими попереджувальними сигналами є:*
  - швидке прагнення до зміцнення стосунків;
  - спроба ізоляції від сім'ї та знайомих;
  - контроль щоденного життя;
  - постійний контакт та очікування постійної доступності;
  - емоційний шантаж та провокування почуття провини;

- злість та агресія у разі невиконання чи недостатньо ретельного виконання очікувань кривдника;
- схиляння до приховування стосунків і того, що в них відбувається, а також до зберігання спільної таємниці;
- прохання, спонукання або змушування до відсилання інтимних фотографій чи відео;
- очікування різних доказів кохання та важливості стосунків.

Батьки найкраще знають, як зазвичай поводиться їхня дитина – її типові реакції, що приносить їй задоволення, тощо. Коли ж у поведінці щось змінюється, і вони не знають причини – це може бути тривожним сигналом. *Слід звертати особливу увагу на:*

- відсторонення, сум, поганий настрій;
- зміни настрою;
- агресивну поведінку;
- надмірну таємничість, особливо щодо активності онлайн (дитина приховує екран телефона чи планшета, виходить з кімнати, коли отримує повідомлення тощо);
- зустрічі або бажання зустрічей з незнайомцями, що супроводжуються відмовою говорити на цю тему;
- страх залишити телефон чи планшет хоч на секунду, стрес та надмірні емоційні реакції в ситуації відсутності доступу до інтернету;
- аутоагресію, думки про самогубство.

Перераховані прояви можуть бути викликані статевим дозріванням підлітка. Але слід придивитися до них в контексті небезпечних стосунків дитини, особливо якщо вони з'явилися несподівано та є інтенсивними.

- *Коли батьки знають чи підозрюють про те, що дитина зіткнулась з насильством онлайн, вони мають звернутись до поліції із заявою, яка повинна містити якомога більше інформації про ситуацію, в якій опинилася дитина*. До заяви треба додати всі доступні докази – записи (скріншоти екрану) розмов, фотографії чи лінки на сайти, якими користувалася дитина. Також слід пам'ятати про існування Національної дитячої «гарячої лінії» 116 111 (з мобільного) або 0 800 500 225 (зі стаціонарного телефону), яка надає безоплатну анонімну допомогу дітям, молоді, а також батькам і вчителям, які потребують підтримки або інформації, зокрема й щодо насильства онлайн.

Додаток 2.1.4.2.3

Шляхи комунікації: як знаходять потенційних постраждалих?

Злочинці можуть використовувати різні способи для знаходження потенційних постраждалих дітей онлайн.

- **Соціальні мережі, форуми та інші онлайн-платформи**

Злочинці можуть намагатися встановити контакт з дитиною через приватні повідомлення або її коментарі в публічних дописах. Якщо профіль дитини не закритий, це дає змогу зібрати багато персональної інформації про неї (ім'я, вік, місце навчання, місця відвідування, уподобання тощо).

- **Онлайн-ігри та чати**

Злочинці можуть намагатися вступити в діалог з дитиною, використовуючи псевдоніми та фальшивий профіль, який виглядає як справжній, бо має фото, дописи, коментарі.

- **Платформи відеострімінгу та спільноти контенту**

На таких платформах діти активно взаємодіють та діляться своїми враженнями, тому злочинці можуть досить легко розпочати спілкування з кимось із них.

- **Залучення дитини до закритої групи в Телеграм чи Вайбер**

Контакт дитини без погодження з нею додають до закритої групи в соціальній мережі/месенджері. Діти часто не знають, хто їх доєднав до чату, тому не можуть ідентифікувати особу, яка це зробила. Також зловмисники можуть пропонувати дитині за певну винагороду додати її до групи їхніх друзів.

- **Загальне рандомне повідомлення у певному чаті**

Злочинці застосовують таку схему контакту зазвичай у відкритому чаті, наприклад, в якому обговорюється волонтерська допомога, і відправляють найпростіше повідомлення, наприклад «Привіт», а потім спілкуються з тими, хто відреагував на їхнє повідомлення.

Чому діти спілкуються зі злочинцями?

Феномен «ілюзії спальні».

Коли ми фізично у безпеці, то виникає ілюзія, ніби з нами нічого не може трапитись в інтернеті в цей час. Але, на жаль, це є хибною думкою.

Цікавість.

Доволі часто діти та підлітки досліджують щось нове в інтернеті саме через цікавість. Так відбувається і зі спілкуванням з незнайомцями, оскільки це викликає багато передчуття та невідомості – а що людина хоче від мене, а що буде, якщо я відповім певним чином.

Пропозиції, які викликають інтерес.

Злочинці можуть пропонувати зробити щось за винагороду: гроші, дорогі подарунки, таємний секрет, який дасть змогу дитині стати популярною, додаткові можливості в онлайн-іграх тощо. А також надають відчуття особливості та секретності таким завданням: що це є таємним та надважливим й ніхто, окрім цієї дитини, не може допомогти в цьому.

Гра.

Часом діти та підлітки сприймають те, що відбувається з ними, особливо в інтернеті, як певну гру, де можна обрати, як поводитися з тою чи іншою людиною, де можна використовувати неправдиву інформацію про себе, щоб здаватись дорослішим чи кращим у чомусь.

Особливість віку.

Часом діти та підлітки впевнені, що через їхній вік їм нічого не страшно, і ніхто не може їх скривдити, бо вони є дітьми. Але злочинці в інтернеті саме за ними і полюють, а також запевняють дітей, що ті не будуть нести відповідальність за злочинні дії, оскільки є дітьми. Діти відчувають себе цінними та особливими, коли дорослі просять їх виконати якісь завдання, які є важливими і навіть секретними для інших.

Як дорослі можуть протидіяти залученню дітей до протиправної діяльності через інтернет?

Важливо говорити з дітьми про їхній стан, переживання та побоювання, які в них є зараз. Наприклад, втрата особистих соціальних зв'язків може спонукати дитину шукати нових друзів в інтернеті, а втрата роботи батьками – способів заробітку.

Обговорювати правила онлайн-безпеки, які є універсальними на всі часи. Для цього можна використовувати вправи згідно з віком дитини: https://stop-sexting.in.ua/category/materials/, також брошуру щодо онлайн-злочинів під час війни: https://stop-sexting.in.ua/wp-content/uploads/2022/05/broshura-nasylstvo-v-interneti.pdf.

Спільно налаштувати приватність акаунтів дитини. Підказки, як це зробити, можете знайти за посиланням: https://stop-sexting.in.ua/nalashtuvannya-pryvatnosti-v-instagram-ta-facebook-instrukcziya-vid-stop_sextyng/.

Використовувати навички критичного мислення та дискутувати з дитиною, як вона б вчинила в тій чи іншій ситуації, чому саме так, а як можна по-іншому підійти до розв'язання проблемної ситуації. За таким алгоритмом ви можете обговорити з дитиною ситуації, коли їй пишуть незнайомі користувачі та просять виконати якесь завдання.

Бути прикладом відповідального користування інтернетом – мати спільні години відпочинку від девайсів та онлайн середовища, вдома започаткувати прийоми їжі без телефонів, спільні традиції.

Слід також пам'ятати про базові рекомендації батькам, як убезпечити своїх дітей від злочинів у віртуальному просторі:

- *навчіть дитину ставитися скептично до нових знайомств у соціальних мережах. Особливо в умовах війни, коли ворог може використовувати чужі фото та представлятися будь-ким, переслідуючи власні інтереси;*
- *пояснюйте про важливість збереження особистих даних у секреті. Насамперед це стосується адреси, місця перебування, номера мобільного телефона, банківських даних батьків. Якщо хтось запитує дітей таку інформацію – навчіть повідомляти про це вам;*
- *вчіть дітей не переходити за сумнівними посиланнями, це стосується не лише посилань у соцмережах чи пошті, за рекламою у різних іграх та додатках також може ховатися «вірус» або фішинг;*
- *навчіть дитину розумно ставитися до повідомлень про надання допомоги та отримувати інформацію лише з офіційних джерел;*
- *поширена небезпека – створення інтимних фотографій. Зловмисники часто маніпулюють та зловживають довірою дітей, вимагаючи відверті світлини. Найчастіше погрожують оприлюднити інтимні матеріали та в подальшому шантажують неповнолітніх для реалізації інших злочинних намірів. Дорослі мають пояснювати дітям про можливі наслідки такого «спілкування»;*
- *можливість легко підзаробити або виконати певне завдання у форматі гри, як-от зробити фото різних об'єктів чи нанести «малюнок» на асфальті, – окупанти використовують різні засоби для ведення війни. Розкажіть дитині про небезпеку таких пропозицій.*

2.2. ОСОБЛИВОСТІ ДІЯЛЬНОСТІ ПОЛІЦЕЙСЬКИХ ПІДРОЗДІЛІВ СЛІДСТВА ТА ДІЗНАННЯ

ТЕМА 2.2.1. Тактичні особливості проведення окремих слідчих (розшукових) дій під час розслідування злочинів проти дітей, вчинених в кіберпросторі. Особливості складання процесуальних документів

Мета: навчитися особливостям здійснення тимчасового доступу до окремих електронних документів та проведення їх огляду.

Загальна тривалість: 4 академічні години (180 астрономічних хвилин).

План:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Робота з електронними доказами	Інформаційне повідомлення	40 хв	Мультимедійне обладнання, Додаток 2.2.1.1
2.	Огляд електронних документів	Індивідуальна робота	130 хв	Комп'ютери для учасників з доступом до інтернету
3.	Висновки	Запитання – відповіді	10 хв	

ХІД ЗАНЯТТЯ

1. Інформаційне повідомлення «Робота з електронними доказами»

Мета: вивчити загальні підходи до закріплення цифрових слідів, вимоги до форми і змісту електронних доказів.

Час: 40 хв.

Необхідні матеріали: мультимедійне обладнання, Додаток 2.2.1.1.

Хід проведення:

Тренер/тренерка звертається до учасників: «*Маючи справу з документуванням кримінальних правопорушень проти дітей, вчинених з використанням кіберпростору, правоохоронцям часто доводиться працювати з цифровими слідами. В Україні ситуація з роботою з електронними (цифровими) доказами є особливо складною через недостатнє оснащення територіальних підрозділів сучасною технікою і програмним забезпеченням, а також суттєвий брак технічно обізнаних правоохоронців. Крім того, відчувається відсутність доступу до значної частини державних баз даних, не кажучи вже про приватні. Велика кількість проваджень, які розслідуються або перебувають під процесуальним керівництвом однієї особи, лише ускладнює проблему, зокрема в арифметичній, а іноді і геометричній прогресії*», після чого презентує інформацію із Додатка 2.2.1.1.

2. Індивідуальна робота «Огляд електронних документів»

Мета: навчитися автоматизації аналізу електронних даних для складання протоколів слідчих (розшукових) дій.

Час: 130 хв.

Необхідні матеріали: комп'ютери для учасників з доступом до інтернету.

Хід проведення:

Тренер надає учасникам/учасницям фабулу завдання для розкриття кримінального правопорушення:

До правоохоронного органу надійшла низка заяв про те, що невстановлена особа регулярно вступає в переписку з неповнолітніми під вигаданими даними. Шляхом зловживання довірою правопорушник виманює у неповнолітніх фото та відео інтимного характеру за їхньою участю. Після шантажує неповнолітніх, примушуючи їх переводити йому кошти, надсилати нові матеріали інтимного характеру, залучати інших неповнолітніх до створення порнографічного контенту. Відомо, що розшукуваний суб'єкт одержує кошти на картку.

та файли-відповіді установ (підприємств, організацій) (приклад наведено за посиланням: http://surl.li/ssvpx) для їх аналізу та складання протоколу огляду електронного документу.

Складені протоколи огляду учасники повертають тренеру/тренерці, який/яка вказує учасникам на можливі способи їх покращення.

До уваги тренера/тренерки!

Можна використати запропоновану фабулу завдання та файли-відповіді установ (підприємств, організацій) або завчасно підготувати іншу фабулу завдання для розкриття кримінального правопорушення та розмістити її разом з файлами-відповідями в сервісі Google Classroom або використати інші освітні платформи.

3. Висновки

Мета: підбити підсумки заняття та поділитись враженнями.

Час: 10 хв.

Хід проведення:

Тренер пропонує учасникам відповісти на такі запитання:

- *Що важливого ви сьогодні зрозуміли для себе?*
- *Чому новому навчились?*
- *Як будете використовувати набуті знання?*

Тестові питання до теми:

1. Який з наведених сервісів можна використати для накладання електронного підпису?

А) hootsuite.com;

Б) brand24.com;

В) sign.diia.gov.ua;

Г) police.gov.ua.

2. Кого з наведених осіб потрібно залучити для того, щоб виготовлені слідчим, прокурором копії інформації визнавалися судом як оригінал документа?

А) оперативного працівника;

Б) спеціаліста;

В) понятого;

Г) статиста.

3. У якому розділі КПК описується порядок зняття інформації з електронних інформаційних систем?

А) 12;

Б) 17;

В) 21;

Г) 8.

4. Який з наведених документів не є процесуальним?

А) запит;

Б) протокол слідчої (розшукової) дії;

В) протокол негласної слідчої (розшукової) дії;

Г) результати експертизи.

5. У якій формі краще одержувати інформацію від банківських установ?

А) електронної таблиці;

Б) малюнка;

В) pdf;

Г) виключно паперовій.

Ключі-відповіді:

1. В; 2. Б; 3. В; 4. А; 5. А.

Додаток 2.2.1.1

Робота з електронними доказами

Важливим аспектом роботи з електронними доказами є те, що наявний кадровий склад правоохоронних органів не завжди має достатні знання і навички для обробки та аналізу даних. Тому під час виконання цієї роботи слідчими та оперативними працівниками важливо використовувати якомога простіші програмні рішення.

Відповідно до ч. 1 ст. 7 Закону України «Про електронні документи та електронний документообіг», оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, зокрема з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронні довірчі послуги». Продемонструвати, як підписувати та перевіряти електронний підпис, можна за допомогою онлайн-сервісів sign.diia.gov.ua та sign.diia.gov.ua/verify.

Відповідно до ч. 4 ст. 99 КПК України, дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також **копії інформації**, зокрема комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням **спеціаліста, визнаються судом як оригінал документа**. Водночас інформацію в електронному вигляді, розміщену на віддалених серверах, не завжди можливо скопіювати структурно повною мірою, навіть із залученням спеціаліста. Так, наприклад, вебсторінка, яка написана з використанням різних мов програмування (PHP, Python, Java, PERL, Ruby, JavaScript тощо), на боці сервера буде виглядати по-іншому, ніж на боці клієнта, де вона відображена у форматі HTML. Отже, правоохоронні органи можуть зафіксувати лише проєкцію оригінальної вебсторінки, яку аж ніяк не можна вважати оригіналом.

Законодавець передбачив ще один спосіб фіксації електронних доказів в межах негласної слідчої (розшукової) дії зі зняття інформації з електронних інформаційних систем за ч. 2 ст. 264 КПК. І хоча окремі науковці досить скептично ставляться до можливості фіксації електронних доказів за описаною процедурою, проте існують прецеденти саме такого процесуального оформлення електронної інформації. В принципі, з логічного погляду такий порядок фіксації є більш правильним, аніж у межах сучасної процедури роботи з електронними доказами як з документами. Але справа в тому, що згідно з положеннями чинного законодавства, відомості про факт або методи проведення негласної слідчої (розшукової) дії мають гриф обмеження доступу «таємно», отже, фактично нетаємна процедура штучно перетворюватиметься на таємну. Це так само може породжувати інші проблеми, пов'язані з розсекречуванням відповідних відомостей та представленням результатів негласних слідчих (розшукових) дій в суді. Зокрема, лише восени 2019 року було вирішене питання доказової сили процесуальних документів, які стали підставою для проведення негласних слідчих розшукових дій та які на стадії досудового розслідування не було відкрито стороні захисту в порядку, передбаченому ст. 290 Кримінального процесуального кодексу.

Одним з різновидів даних, з якими доводиться мати справу правоохоронцям, є **відповіді установ, підприємств, організацій**. Найчастіше, правоохоронні органи мають справу з банківськими транзакціями, файлами протоколів провайдерів та операторів комунікацій, відповідями фінансових установ. Їх аналіз є достатньо нетривіальним завданням, але потрібним, оскільки описані документи можуть містити відомості про справжні IP-адреси фігурантів, їхні номери телефонів, інформацію про рахунки для сплати комунальних послуг тощо.

Перша проблема, з якою стикаються правоохоронці, пов'язана з тим, що інформацію часто отримують на підставі запиту, який не є процесуальним документом. Це зумовлює необхідність паралельного проведення слідчої (розшукової) дії «тимчасовий доступ до речей і документів». Якщо цієї дії не вжити, строк зберігання відомостей може спливти. Тому важливо підтримувати постійний контакт з виконавцем запиту.

Другим проблемним моментом є те, що не завжди просто знайти контактні дані адресата запитуваних відомостей — відповідного підприємства, установи або організації. Крім того, існують певні вимоги до змісту та форми наданих відомостей. Під час складання запитової частини документа важливо формулювати запит так, щоб отримати якомога повнішу інформацію та уникнути необхідності надсилання додаткових запитів. Наприклад, у разі запиту інформації про інтернет-гаманці, слід одразу вказати на потребу надання повних номерів банківських платіжних карток, які використовувалися для поповнення/виведення коштів з гаманців. Також важливо запитати дані щодо гаманців, на які виводилися кошти, а також про інші гаманці, з яких здійснювалися перекази на такі самі банківські платіжні картки, що й із зазначених у запиті гаманців.

Що стосується форми наданих відомостей, то оптимальним є їх одержання у форматі, придатному для аналізу **в табличному процесорі**. Проте нерідко трапляються випадки, коли відомості надаються у pdf форматі, та навіть у вигляді зображень. Якщо відомості від організації, підприємства, установи надійшли в pdf форматі, то найбільш якісне переведення до форми таблиці можна здійснити за допомогою функції експорту в програмі Adobe Acrobat Reader Pro. Очевидно, це пов'язано з тим, що компанія Adobe Systems є розробником стандарту pdf.

Під час опрацювання даних, наданих підприємствами, установами, організаціями, слід звернути увагу на:

- *засоби фільтрації табличних процесорів (простий та водночас потужний інструмент, доступний для розуміння пересічному правоохоронцю);*
- *засоби візуалізації текстової інформації (корисно використовувати для графічного представлення текстових даних та відображення відповідних зв'язків);*
- *методи логічного опрацювання;*
- *засоби автоматизації перевірки та вилучення даних.*

В останньому пункті йдеться про програми, спеціально розроблені для вирішення нескладних завдань, спрямованих на автоматизацію обробки даних:

- *перевірка великої кількості IP-адрес щодо їх належності до українського сегменту кіберпростору;*
- *вилучення номерів карток з файлів, наданих банками;*
- *побудова хмари ключових слів з файлу великих даних;*
- *проведення ретроспективного аналізу за авторством.*

Так, наприклад, завантаження усього змісту даних з сайту оголошень протиправного характеру дає матеріал для подальшого аналізу. Цілком ймовірною ситуацією є те, що спочатку особа була пересічним користувачем на форумі, ставила питання, повідомляла якусь інформацію про себе, а згодом її діяльність стала більш злочинно-орієнтованою. Надалі це могло сприяти виникненню злочинного угруповання та навіть злочинної організації. Здійснюючи ретроспективний аналіз відповідних повідомлень, інколи можна встановити справжні особисті дані особи фігуранта.

Тема 2.2.2. Особливості кримінально-правового захисту дітей від сексуальної експлуатації та сексуального насильства, вчиненого із використанням електронних засобів комунікації

Мета: надати учасникам інформацію щодо характеристики кримінальних правопорушень, пов'язаних із сексуальною експлуатацією та сексуальним насильством щодо дітей, які вчиняються із використанням електронних засобів комунікації, розвинути практичні навички щодо кваліфікації вказаних кримінальних правопорушень.

Загальна тривалість: 4 академічні години (180 астрономічних хвилин).

План проведення:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Вступ до тематики	Інформаційне повідомлення	15 хв	Мультимедійне обладнання, Додаток 2.2.2.1
2.	Віддзеркалення	Робота в групах Обговорення	40 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 2.2.2.2, ККУ (друкований або електронний примірник)
3.	Загальні питання кваліфікації кримінальних правопорушень, пов'язаних із сексуальною експлуатацією та сексуальним насильством щодо дітей, які вчиняються із використанням електронних засобів комунікації	Інформаційне повідомлення	35 хв	Мультимедійне обладнання, Додаток 2.2.2.3
4.	Кримінально-правова характеристика кримінальних правопорушень, пов'язаних із сексуальною експлуатацією та сексуальним насильством щодо дітей, які вчиняються із використанням електронних засобів комунікації	Інформаційне повідомлення	45 хв	Мультимедійне обладнання, Додаток 2.2.2.4
5.	Кваліфікація кримінальних правопорушень, пов'язаних із сексуальною експлуатацією та сексуальним насильством щодо дітей, які вчиняються із використанням електронних засобів комунікації	Робота в групах Обговорення	45 хв	Фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 2.2.2.5, ККУ (друкований або електронний примірник)

ХІД ЗАНЯТТЯ

1. Інформаційне повідомлення «Вступ до тематики»

Мета: надати учасникам інформацію щодо нормативно-правових актів, які забезпечують кримінально-правовий захист дітей від сексуальної експлуатації та сексуального насильства, вчиненого із використанням електронних засобів комунікації.

Час: 15 хв.

Необхідні матеріали: мультимедійне обладнання, Додаток 2.2.2.1.

Хід проведення:

Тренер/тренерка надає учасникам інформацію про основні питання, які будуть розглядатися під час проведення заняття та його мету, після чого презентує інформацію відповідно до Додатка 2.2.2.1 з використанням мультимедійного обладнання.

2. Робота в групах. Обговорення «Віддзеркалення»

Мета: надати учасникам змогу самим безпосередньо визначити, як міжнародні зобов'язання України щодо кримінально-правового захисту дітей від сексуальної експлуатації та сексуального насильства, вчиненого із використанням електронних засобів комунікації, реалізовані в законодавстві України про кримінальну відповідальність.

Час: 40 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 2.2.2.2, ККУ (друкований або електронний примірник).

Хід проведення:

Тренер/тренерка об'єднує учасників у три групи та зазначає завдання: «*Проаналізуйте витяги з міжнародної угоди та визначте положення, які стосуються кримінально-правової заборони сексуальної експлуатації та сексуального насильства щодо дітей, які можуть бути вчинено із використанням електронних засобів комунікації. За допомогою запропонованої схеми побудови відповіді зазначте, як відповідні положення міжнародних угод реалізовані в ККУ*».

Група 1 – аналіз положень Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротська конвенція).

Група 2 – аналіз положень Конвенції Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу із цими явищами (Стамбульська конвенція).

Група 3 – аналіз положень Факультативного протоколу до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії.

Кожна група отримує витяги з відповідних угод та картку з рекомендованою схемою побудови відповіді. На підготовку групи отримують 15 хвилин і по 5 хвилин для презентації роботи групи.

До уваги тренера/тренерки!

У разі проведення занять зі слухачами з високим рівнем підготовки, замість витягів можна надати повний текст міжнародних угод.

Варто звернути увагу, що переважна більшість міжнародно-правових угод кримінально-правого характеру поряд з матеріальними нормами, які визначають обов'язок сторін криміналізувати певні діяння, містять процесуальні положення, які визначають порядок і особливості співпраці сторін з метою протидії кримінальним правопорушенням.

Під час оцінки результатів роботи груп доцільно скористатися переліком статей ККУ, визначеному в Додатку 2.2.2.4.

Запитання для обговорення:

- *Чи всі види сексуальної експлуатації та сексуального насильства щодо дітей можуть бути вчинені із використанням електронних засобів комунікації? Визначте, які саме.*
- *Чи всі положення міжнародних угод, що стосуються злочинів, пов'язаних з сексуальною експлуатацією та сексуальним насильством щодо дітей, вчинених з використанням електронних засобів комунікації, знайшли відображення в ККУ?*
- *Чи у всіх статтях ККУ, які криміналізують сексуальну експлуатацію та сексуальне насильство щодо дітей, які вчиняються із використанням електронних засобів комунікації, безпосередньо передбачено зазначений спосіб вчинення кримінального правопорушення?*
- *Чи виявили ви випадки, коли час ратифікації міжнародних угод не відповідає часу внесення змін до законодавства України про кримінальну відповідальність? Чи впливають зазначені факти на кваліфікацію відповідних діянь?*
- *Чи помітили ви у текстах угод терміни, які вам важко зрозуміти/розтлумачити?*
- *Чи стикалися ви в своїй практичній діяльності з випадками сексуальної експлуатації та сексуального насильства дітей, вчиненими з використанням електронних засобів комунікації? Які складності ви можете зазначити щодо їх кваліфікації/розслідування?*

До уваги тренера/тренерки!

Деякі положення міжнародних угод, які криміналізують сексуальну експлуатацію та сексуальне насильство щодо дітей, які вчиняються з використанням електронних засобів комунікації, внесено до ККУ завчасно (положення Стамбульської конвенції), а деякі – із запізненням (положення Ланцаротської конвенції).

Під час обговорення важливо звернути увагу, що законодавець, на жаль, не завжди своєчасно вносить відповідні зміни до ККУ. ККУ є єдиним нормативно-правовим актом, який встановлює кримінальну протиправність діянь та їх караність (ч. 3 ст. 3 ККУ). Норми міжнародних угод, які передбачають криміналізацію відповідних діянь, не мають прямої дії, хоча можуть бути використані для тлумачення деяких термінів і понять у правозастосуванні. Крім того, закон про кримінальну відповідальність, що встановлює кримінальну протиправність діяння, посилює кримінальну відповідальність або іншим чином погіршує становище особи, не має зворотної дії в часі (ч. 2 ст. 5 ККУ), тому зміни, внесені до ККУ щодо криміналізації відповідних діянь, розповсюджуються лише на діяння, вчинені після вступу відповідного закону в силу.

3. Інформаційне повідомлення «Загальні питання кваліфікації кримінальних правопорушень, пов'язаних із сексуальною експлуатацією та сексуальним насильством щодо дітей, які вчиняються із використанням електронних засобів комунікації»

Мета: надати учасникам інформацію щодо загальних питань кваліфікації кримінальних правопорушень, пов'язаних із сексуальною експлуатацією та сексуальним насильством щодо дітей, які вчиняються із використанням електронних засобів комунікації, та визначити ключові правові терміни, що використовуються під час кваліфікації вказаних кримінальних правопорушень.

Час: 35 хв.

Необхідні матеріали: мультимедійне обладнання, Додаток 2.2.2.3.

Хід проведення:

Тренер/тренерка презентує інформацію відповідно до Додатка 2.2.2.3 з використанням мультимедійного обладнання, відповідає на запитання учасників. Під час презентації навчального матеріалу тренеру/тренерці варто приділити особливу увагу термінам та поняттям, які викликали в учасників особливу складність щодо їх тлумачення або розуміння під час проведення вправи 2.

До уваги тренера/тренерки!

Під час розгляду питання про потерпілого від кримінальних правопорушень, пов'язаних з сексуальною експлуатацією та сексуальним насильством щодо дітей, слід обов'язково звернути увагу учасників, що до досягнення особою шістнадцятирічного віку встановлена абсолютна заборона стосовно дорослих осіб займатися з нею будь-якою формою діяльності сексуального характеру. З досягненням шістнадцятирічного віку неповнолітній набуває статевої свободи, під якою розуміють його право самостійно обирати собі партнера для сексуального спілкування і форму такого спілкування, не допускаючи водночас будь-якого примусу. Також слід звернути увагу, що у контексті ККУ дорослою може вважатися особа, якій виповнилось шістнадцять років, а не особа, яка досягла повноліття або визначеного Сімейним Кодексом України шлюбного віку (18 років).

Аналізуючи зміст поняття сексуального насильства щодо дітей, слід звернути увагу, що цей термін використовується в широкому розумінні, охоплюючи різні форми сексуального насильства щодо дітей (відповідно до тлумачення, наданого Ланцаротською конвенцією), і не обмежується складом кримінального правопорушення, закріпленим у ст. 153 ККУ «Сексуальне насильство».

4. Інформаційне повідомлення «Кримінально-правова характеристика кримінальних правопорушень, пов'язаних із сексуальною експлуатацією та сексуальним насильством щодо дітей, які вчиняються із використанням електронних засобів комунікації».

Мета: надати учасникам інформацію про склади кримінальних правопорушень, передбачені ККУ, які пов'язані із сексуальною експлуатацією та сексуальним насильством щодо дітей та які вчиняються із використанням електронних засобів комунікації.

Час: 45 хв.

Необхідні матеріали: мультимедійне обладнання, Додаток 2.2.2.4.

Хід проведення:

Тренер/тренерка презентує інформацію відповідно до Додатка 2.2.2.4 з використанням мультимедійного обладнання, відповідає на запитання учасників.

До уваги тренера/тренерки!

Варто врахувати особливості обчислення строків давності притягнення до кримінальної відповідальності за кримінальні правопорушення, пов'язані із сексуальною експлуатацією та сексуальним насильством щодо дітей (доповнення внесені до ККУ 18.02.2021 р.): у разі вчинення кримінального правопорушення, передбаченого статтями 151-2 – 156-1, 301-1 – 303 КК України, стосовно малолітньої чи неповнолітньої особи обчислення строку давності притягнення до кримінальної відповідальності розпочинається з дня, коли така потерпіла особа досягла повноліття або, у разі її смерті, мала б досягти повноліття (ч. 6 ст. 49 КК України).

Доцільно звернути увагу учасників, що персональні дані засуджених, які будь-яким способом зазіхнули на недоторканість дітей віком до 14 років, вносяться до Єдиного реє-

стру осіб, засуджених за злочини проти статевої свободи та статевої недоторканості малолітньої особи (так званий «реєстр педофілів»). Відповідно до ст.6-1 Кримінально-виконавчого кодексу України *Єдиний реєстр осіб, засуджених за злочини проти статевої свободи та статевої недоторканості малолітньої особи* – це автоматизована електронна база даних, створена для забезпечення збирання, зберігання, захисту, обліку, пошуку, узагальнення даних про осіб, які вчинили злочини проти статевої свободи та статевої недоторканості малолітньої особи, у тому числі осіб, судимість яких за такі злочини знята або погашена в установленому законом порядку. Інформація про особу вноситься до реєстру на підставі обвинувального вироку суду, який набрав законної сили. У разі, якщо особа вчинила кримінальне правопорушення проти статевої свободи та статевої недоторканості малолітньої особи до створення реєстру, інформація про таку особу вноситься до реєстру на підставі ухвали суду за місцем проживання такої особи або місцем відбування нею покарання за клопотанням прокурора. Інформація про особу виключається з реєстру у разі скасування обвинувального вироку або ухвали суду. Користувачами реєстру є керівники прокуратур та органів досудового розслідування, прокурори, слідчі та інші уповноважені особи Національної поліції України та Державного бюро розслідувань. Особам, інформацію про яких внесено до Єдиного реєстру осіб, засуджених за злочини проти статевої свободи та статевої недоторканості малолітньої особи, забороняється працювати у контакті з дітьми (ч. 11 ст. 10 Закону України «Про охорону дитинства»).

В Україні встановлена кримінально-правова заборона щодо ввезення в Україну творів, зображень або інших предметів порнографічного характеру з метою збуту чи розповсюдження або їх виготовлення, зберігання, перевезення чи інше переміщення з тією самою метою, або їх збут чи розповсюдження. Продукція відноситься до такої, що має порнографічний характер, за умови, якщо вона відповідає таким критеріям: 1) основний зміст продукції або її значну частину становить демонстрація великим планом статевих органів у збудженому стані або деталізований опис чи демонстрація статевого акту; 2) продукція містить натуралістичне зображення, максимально наближене до реальної анатомії і фізіології людини та її статевого акту; 3) продукція створена виключно з метою статевого збудження її споживачів (Критерії віднесення продукції до такої, що має порнографічний характер, затверджені Наказом Міністерства культури України від 16.03.2018 р. № 212). На відміну від дитячої порнографії, щодо обігу і володіння якою з 18.02.2021 р. в Україні встановлена повна заборона, володіння порнографією, що зображує дорослих осіб (одержання доступу до порнографії з використанням інформаційно-телекомунікаційних систем чи технологій, її придбання та зберігання для власного користування), без мети її збуту не є кримінально протиправним в Україні.

Доцільно звернути увагу учасників, що в Україні передбачено застосування заходів кримінально-правового характеру до юридичних осіб за вчинення її уповноваженою особою від імені та в інтересах юридичної особи кримінальних правопорушень, пов'язаних із сексуальною експлуатацією та сексуальним насильством щодо дітей, передбачених ст. 152 – 156-1, 301-1 – 303 ККУ (п. 6 ч. 1 ст. 96-1 ККУ). Відповідною наявність цих фактів має бути встановлено під час досудового розслідування. Уповноваженими особами юридичної особи слід розуміти службових осіб юридичної особи, а також інших осіб, які відповідно до закону, установчих документів юридичної особи чи договору мають право діяти від імені юридичної особи. Кримінальні правопорушення, пов'язані із сексуальною експлуатацією та сексуальним насильством щодо дітей, визнаються вчиненими в інтересах юридичної особи, якщо вони призвели до отримання нею неправомірної вигоди або створили умови для отримання такої вигоди, або були спрямовані на ухилення від передбаченої законом відповідальності (Примітка до ст. 96-1 ККУ).

5. Робота в групах. Обговорення. «Кваліфікація кримінальних правопорушень, пов'язаних із сексуальною експлуатацією та сексуальним насильством щодо дітей, які вчиняються із використанням електронних засобів комунікації»

Мета: за допомогою практичної вправи закріпити отримані знання щодо кваліфікації кримінальних правопорушень, пов'язаних із сексуальною експлуатацією та сексуальним насильством щодо дітей, які вчиняються із використанням електронних засобів комунікації.

Час: 45 хв.

Необхідні матеріали: фліпчарт, аркуші паперу для фліпчарту, маркери, Додаток 2.2.2.5, ККУ (друкований або електронний примірник).

Хід проведення:

Тренер/тренерка об'єднує учасників у три групи та зазначає завдання: «*Надати кримінально-правову кваліфікацію відповідно до наданих фабул*» (роздатковий матеріал Додатка 2.2.2.5).

Групам надається 15 хвилин на виконання завдання і по 5-7 хвилин для презентації напрацювань групи.

Під час презентації один або декілька учасників групи мають зачитати фабулу, представити записану на фліпчарті формулу кваліфікації та обґрунтувати свою відповідь.

Після презентації кожної з груп тренер/тренерка надає змогу учасникам з інших груп висловити свою думку щодо повноти й правильності здійсненої кваліфікації. Після презентації та висловлення позицій учасників з інших груп тренер/тренерка оцінює правильність та повноту відповідей учасників груп.

До уваги тренера/тренерки!

Для зручності виконання завдання та заощадження часу доцільно заздалегідь підготувати для груп картки із завданнями (роздатковий матеріал Додатка 2.2.2.5).

Для побудови повної та обґрунтованої відповіді доцільно порекомендувати учасникам груп визначити та записати на фліпчарті склад (-и) кримінального правопорушення/кримінальних правопорушень, за якими вони здійснюють кваліфікацію (об'єкт, об'єктивна сторона, суб'єкт, суб'єктивна сторона, за необхідністю, інші ознаки кримінального правопорушення).

Тестові питання до теми:

1. Відповідно до законодавства, вік сексуальної згоди в України становить:

А) 14 років;

Б) 16 років;

В) 18 років;

Г) вік сексуально згоди не встановлено в законодавстві України.

2. У якому з наведених нижче випадків є дитяча порнографія?

А) публічний показ сценічних дій сексуального характеру, в яких задіяна дитина;

Б) зображення у будь-який спосіб дитини чи особи, яка виглядає як дитина, у реальному чи змодельованому відверто сексуальному образі;

В) зображення особи у відверто сексуальному образі з використанням інформаційно-телекомунікаційних систем або технологій;

Г) зображення статевих органів дитини.

3. Яке з наведених нижче кримінальний правопорушень, пов'язаних із сексуальною експлуатацією та сексуальним насильством щодо дітей, не може бути вчинено способом «використання інформаційно-телекомунікаційних систем або технологій»?

А) сексуальне насильство (ст. 153 КК України);

Б) розбещення неповнолітніх (ст. 156 КК України);

В) домагання дитини для сексуальних цілей (ст. 156-1 КК України);

Г) одержання доступу до дитячої порнографії (ст. 301-1 КК України);

Д) проведення видовищного заходу сексуального характеру за участю неповнолітньої особи (ст. 301-2 КК України).

4. Кримінальне правопорушення, передбачене ст. 156-1 КК України «Домагання дитини для сексуальних цілей», є закінченим з моменту:

А) коли суб'єкт кримінального правопорушення вийшов на зв'язок з потерпілою особою з використанням інформаційно-телекомунікаційних систем або технологій;

Б) коли суб'єкт кримінального правопорушення запропонував зустріч потерпілій особі і вчинив хоча б одну дію, спрямовану на те, щоб така зустріч відбулася, незалежно від того, чи вона відбулася в подальшому;

В) здійснення зустрічі суб'єкту кримінального правопорушення з потерпілою особою з метою її розбещення;

Г) вчинення дій, спрямованих на інтелектуальне або фізичне розбещення неповнолітньої особи.

5. Під кібергрумінгом розуміють:

А) одержання доступу або створення зображень дитини у реальному чи змодельованому відверто сексуальному образі або задіяної у реальній чи змодельованій відверто сексуальній поведінці із використанням інформаційно-телекомунікаційних систем або технологій;

Б) діяння учасників освітнього процесу, які полягають у психологічному, фізичному, економічному, сексуальному насильстві, що вчиняються стосовно дитини із застосуванням засобів електронних комунікацій;

В) здійснення публічного показу у будь-якій формі продукції сексуального характеру або сценічних дій, метою яких є втілення сексуальних дій, зокрема з використанням інформаційно-телекомунікаційних систем або технологій;

Г) налагодження довірливих стосунків з неповнолітньої особою з метою сексуального насильства над нею із використанням інформаційно-телекомунікаційних систем або технологій.

Ключі-відповіді:

1. Б; 2. Б; 3. А; 4. Б; 5. Г.

Додаток 2.2.2.1

Сексуальна експлуатація та сексуальне насильство вважаються одними із найгірших форм насильства стосовно дітей. Згідно зі статистичними даними Ради Європи, приблизно кожна п'ята дитина в Європі стає постраждалою від тієї чи іншої форми сексуального насильства, і 80% випадків – це знайомі, рідні, близькі дитини.

Легкий доступ до мобільних пристроїв із виходом в інтернет значно розширили можливості злочинців у вчиненні сексуальної експлуатації та сексуального насильства щодо дітей:

- кримінальні правопорушення можуть вчинятися щодо дітей, які знаходяться на значній відстані від правопорушника;
- полегшується доступ до дітей з метою вербування та примушування до різних форм сексуального насильства і сексуальної експлуатації;
- збільшується вразливість і потенційна кількість дітей, які зазнають сексуальної експлуатації, сексуального насильства та розбещення;
- новітні технології надають змогу вчинення і демонстрації сексуального насильства або видовищних заходів сексуального характеру з використанням дітей, зокрема в режимі реального часу;
- новітні технології та відкритий доступ до всесвітньої мережі інтернет розширюють можливості щодо створення та розповсюдження фотовізуальних матеріалів, які зображують сексуальне насильство та експлуатацію дітей, спрощують отримання за це фінансового прибутку;
- збільшується попит на продукцію, що містить фотовізуальні матеріали сексуальної експлуатації дітей;
- діяльність, пов'язана з сексуальною експлуатацією і сексуальним насильством щодо дітей, приймає форму організованої злочинності.

Наразі у базі Європолу зберігається понад 46 млн зображень сексуального насильства щодо дітей. Кожні 5 хвилин в інтернеті фіксується нова сторінка, що зображує сексуальне насильство щодо дитини, водночас кожне третє з подібних зображень зроблене дитиною власноруч унаслідок шантажу та погроз. Нерідкими є випадки створення і використання контенту сексуального характеру за участю дітей їхніми власними батьками, законними представниками або близькими родичами з метою отримання фінансового прибутку.

Нормативно-правова база, що забезпечує кримінально-правовий захист дітей від сексуальної експлуатації та сексуального насильства, вчиненого із використанням електронних засобів комунікації, становить міжнародні договори України у відповідні сфери, ратифіковані Верховною Радою України, КК України та інші закони України.

Україна, обравши шлях євроінтеграції, є учасницею всіх основних міжнародних угод, які встановлюють міжнародно-правову заборону сексуальної експлуатації та сексуального насильства щодо дітей. Серед них слід зазначити:

- ✔ Конвенцію про права дитини;
- ✔ Факультативний протокол до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії;
- ✔ Конвенцію Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротська конвенція);
- ✔ Конвенцію Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу із цими явищами (Стамбульська конвенція);

- Конвенцію про кіберзлочинність;
- Конвенцію Ради Європи про заходи щодо протидії торгівлі людьми.

Так, зокрема, у ст. 34 Конвенції про права дитини 1989 р. (ратифікована Постановою Верховної Ради УРСР 27.02.91 р., Україна є правонаступницею щодо цієї угоди) зазначено, що держави-учасниці зобов'язані захищати дитину від усіх форм сексуальної експлуатації та сексуальних розбещень. З цією метою держави-учасниці, зокрема, вживають на національному, двосторонньому та багатосторонньому рівнях всіх необхідних заходів щодо запобігання:

a) схилянню або примушуванню дитини до будь-якої незаконної сексуальної діяльності;

b) використанню дітей з метою експлуатації у проституції або в іншій незаконній сексуальній практиці;

c) використанню дітей з метою експлуатації у порнографії та порнографічних матеріалах.

ККУ є єдиним в Україні нормативно правовим актом, що встановлює кримінальну протиправність діяння, його караність та інші кримінально-правові наслідки діяння (ч. 3 ст. 3 КК України). Норми законодавства України про кримінальну відповідальність повинні відповідати положенням, що містяться в чинних міжнародних договорах, згоду на обов'язковість яких надано Верховною Радою України (ч. 5 ст. 3 ККУ).

До інших законів України, що забезпечують кримінально-правовий захист дітей від сексуальної експлуатації та сексуального насильства, слід віднести:

- Закон України «Про охорону дитинства»;
- Закон України «Про медіа».

Додаток 2.2.2.2

Схема побудови відповіді

1. Назва міжнародно-правової угоди.
2. Дата укладення.
3. Дата ратифікації Верховною Радою України.

Положення міжнародно-правової угоди	Кореспондуюча норма КК України	Дата внесення відповідних змін до КК України (якщо внесення змін було необхідним)

Роздатковий матеріал для Групи 1

Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротська конвенція)

(витяг)

Дата укладання: 25.10.2007.

Дата ратифікації Україною: 20.06.2012.

Глава VI
Матеріальне кримінальне право

Стаття 18
Сексуальне насильство

1. Кожна Сторона вживає необхідних законодавчих або інших заходів для забезпечення криміналізації такої умисної поведінки:

a) заняття діяльністю сексуального характеру з дитиною, яка не досягла передбаченого законодавством віку для заняття діяльністю сексуального характеру;

b) заняття діяльністю сексуального характеру з дитиною, коли:

- використовується примус, сила чи погрози або
- насильство здійснюється зі свідомим використанням довіри, авторитету чи впливу на дитину, зокрема в сім'ї, або
- насильство здійснюється в особливо вразливій для дитини ситуації, зокрема з причини розумової чи фізичної неспроможності або залежного становища.

2. Для цілей пункту 1 цієї статті кожна Сторона визначає вік, до досягнення якого забороняється займатися діяльністю сексуального характеру з дитиною.

3. Дія положень підпункту «a» пункту 1 цієї статті не поширюється на врегулювання статевих стосунків між неповнолітніми, що здійснюються за взаємною згодою.

Стаття 19
Правопорушення, що стосуються дитячої проституції

1. Кожна Сторона вживає необхідних законодавчих або інших заходів для забезпечення криміналізації такої умисної поведінки:

a) вербування дітей для заняття проституцією або спонукання дитини до участі в проституції;

b) примушування дитини до проституції або отримання прибутку від цього або іншого використання дитини із цією метою;

c) звернення до дитячої проституції.

2. Для цілей цієї статті термін «дитяча проституція» означає факт використання дитини для діяльності сексуального характеру, коли грошова чи інша форма винагороди або відшкодування надаються чи обіцяються як оплата, незалежно від того, чи здійснюється ця оплата, ця обіцянка або це відшкодування дитині чи третій особі.

Стаття 20
Правопорушення, що стосуються дитячої порнографії

1. Кожна Сторона вживає необхідних законодавчих або інших заходів для забезпечення криміналізації такої умисної поведінки, учиненої без правових підстав:

a) виготовлення дитячої порнографії;

b) пропонування або надання доступу до дитячої порнографії;

c) розповсюдження або передавання дитячої порнографії;

d) придбання дитячої порнографії для себе або іншої особи;

e) володіння дитячою порнографією;

f) свідоме одержання доступу до дитячої порнографії за допомогою інформаційно-комунікаційних технологій.

2. Для цілей цієї статті термін «дитяча порнографія» означає будь-які матеріали, які візуально зображують дитину, залучену до реальної або модельованої явно сексуальної поведінки, чи будь-яке зображення дитячих статевих органів, здебільшого із сексуальною метою.

3. Кожна Сторона може залишити за собою право не застосовувати цілком або частково підпунктів «a» та «e» пункту 1 цієї статті до виготовлення порнографічної продукції та володіння нею:

- яка складається лише з модельованих образів або реалістичних зображень неіснуючої дитини;
- до якої залучено дітей, які досягли віку, визначеного під час застосування пункту 2 статті 18 цієї Конвенції, якщо за їхньою згодою й тільки для їхнього приватного використання вони виготовили ці зображення або володіють ними.

4. Кожна Сторона може залишити за собою право не застосовувати цілком або частково підпункту «f» пункту 1 цієї статті.

Стаття 21
Правопорушення, що стосуються участі дитини в порнографічних виставах

1. Кожна Сторона вживає необхідних законодавчих або інших заходів для забезпечення криміналізації такої умисної поведінки:

a) вербування дітей для участі в порнографічних виставах або спонукання дитини до участі в таких виставах;

b) примушування дитини до участі в порнографічних виставах або отримання користі від цього чи іншого використання дитини із цією метою;

c) свідоме відвідування порнографічних вистав, у яких залучено дітей.

2. Кожна Сторона може залишити за собою право обмежити застосування підпункту «c» пункту 1 цієї статті до випадків, коли дітей вербували або примушували відповідно до підпунктів «a» чи «b» пункту 1 цієї статті.

Стаття 22
Розбещення дітей

Кожна Сторона вживає необхідних законодавчих або інших заходів для забезпечення криміналізації умисного спонукання дитини, яка не досягла віку, передбаченого пунктом 2 статті 18 цієї Конвенції, спостерігати за сексуальним насильством або діяльністю сексуального характеру, навіть якщо вона не бере в цьому участі.

Стаття 23
Домагання дитини для сексуальних цілей

Кожна Сторона вживає необхідних законодавчих або інших заходів для забезпечення криміналізації умисної пропозиції, зробленої дорослою людиною за допомогою інформаційно-комунікаційних технологій, зустрітися з дитиною, яка не досягла віку, передбаченого пунктом 2 статті 18 цієї Конвенції, для скоєння проти неї одного з правопорушень, передбачених підпунктом «a» пункту 1 статті 18 або підпунктом «a» пункту 1 статті 20 цієї Конвенції, якщо після цієї пропозиції відбулись істотні дії, що призвели до такої зустрічі.

Стаття 24
Пособництво, спонукання та замах

1. Кожна Сторона вживає необхідних законодавчих або інших заходів для визнання кримінальними правопорушеннями умисно скоєного пособництва та підбурення у вчиненні будь-якого з правопорушень, установлених відповідно до цієї Конвенції.

2. Кожна Сторона вживає необхідних законодавчих або інших заходів для визнання кримінальними правопорушеннями умисно вчинених замахів на скоєння правопорушень, установлених відповідно до цієї Конвенції.

3. Кожна Сторона може залишити за собою право не застосовувати цілком або частково пункту 2 цієї статті до правопорушень, установлених відповідно до підпунктів «b», «d», «e» та «f» пункту 1 статті 20, підпункту «c» пункту 1 статті 21, статті 22 й статті 23 цієї Конвенції.

Роздатковий матеріал для Групи 2

Конвенція Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу із цими явищами (Стамбульська конвенція)

(витяг)

Дата укладання: 11.05.2011.

Дата ратифікації Україною: 20.06.2022.

ГЛАВА V
Матеріальне право

Стаття 36
Сексуальне насильство, у тому числі зґвалтування

1. Сторони вживають необхідних законодавчих або інших заходів для забезпечення того, щоб було криміналізовано такі форми умисної поведінки:

a) здійснення, без згоди, вагінального, анального або орального проникнення сексуального характеру в тіло іншої особи з використанням будь-якої частини тіла або предмета;

b) здійснення, без згоди, інших актів сексуального характеру з особою;

c) примушування іншої особи до здійснення, без згоди, актів сексуального характеру з третьою особою.

2. Згоду повинно бути надано добровільно як результат вільного волевиявлення особи, отриманого в контексті супутніх обставин.

3. Сторони вживають необхідних законодавчих або інших заходів для забезпечення того, щоб положення пункту 1 також застосовувалися до актів, учинених проти колишніх чи теперішніх подружжів або партнерів, як це визнається національним законодавством.

Стаття 37
Примусовий шлюб

1. Сторони вживають необхідних законодавчих або інших заходів для забезпечення того, щоб умисну поведінку, яка полягає в примушуванні дорослого або дитини до вступу в шлюб, було криміналізовано.

2. Сторони вживають необхідних законодавчих або інших заходів для забезпечення того, щоб умисну поведінку, яка полягає в заманюванні дорослого або дитини на територію Сторони або держави іншої, ніж та, у якій він чи вона проживає, для примушування цього дорослого або дитини до вступу в шлюб, було криміналізовано.

Стаття 38
Каліцтво жіночих геніталій

Сторони вживають необхідних законодавчих або інших заходів для забезпечення того, щоб було криміналізовано такі форми умисної поведінки:

a) видалення, інфібуляція або здійснення будь-якого іншого каліцтва в цілому або частково великих статевих губ, малих статевих губ або клітора;

b) примушування жінки до того, щоб вона зазнала актів, перелічених у підпункті «a», або схилення її до цього;

c) підбурювання, примушування дівчини до того, щоб вона зазнала актів, перелічених у підпункті «a», або схилення її до цього.

Стаття 39
Примусовий аборт та примусова стерилізація

Сторони вживають необхідних законодавчих або інших заходів для забезпечення того, щоб було криміналізовано такі форми умисної поведінки:

a) проведення аборту жінці без її попередньої та інформованої згоди;

b) проведення хірургічного втручання, метою або наслідком якого є припинення здатності жінки до природної репродукції без її попередньої та інформованої згоди або розуміння процедури.

Стаття 40
Сексуальне домагання

Сторони вживають необхідних законодавчих або інших заходів для забезпечення того, щоб будь-яка форма небажаної вербальної, невербальної або фізичної поведінки сексуального характеру, метою або наслідком якої є порушення гідності особи, зокрема шляхом створення залякувального, ворожого, принизливого або образливого середовища, підлягала кримінальній або іншій юридичній санкції.

Стаття 41
Пособництво або підбурювання та замах

1. Сторони вживають необхідних законодавчих або інших заходів для визнання правопорушенням умисно вчиненого пособництва або підбурювання у вчиненні будь-якого з правопорушень, установлених відповідно до статей 33, 34, 35, 36, 37, пункту «a» статті 38 та статті 39 цієї Конвенції.

2. Сторони вживають необхідних законодавчих або інших заходів для встановлення правопорушеннями умисно вчинених замахів на вчинення правопорушень, установлених відповідно до статей 35, 36, 37, пункту «a» статті 38 та статті 39 цієї Конвенції.

Стаття 42
Неприйнятні виправдання злочинів, у тому числі злочини, учинені в ім'я так званої «честі»

1. Сторони вживають необхідних законодавчих або інших заходів для забезпечення того, щоб у кримінальному провадженні, розпочатому після вчинення будь-якого з актів насильства, які підпадають під сферу застосування цієї Конвенції, культура, звичаї, релігія, традиція або так звана «честь» не розглядалися як виправдання таких актів. Це охоплює, зокрема, заяви про те, що постраждала особа порушила культурні, релігійні, соціальні чи традиційні норми або звичаї належної поведінки.

2. Сторони вживають необхідних законодавчих заходів для забезпечення того, щоб підбурювання будь-якою особою стосовно дитини вчинити будь-який з актів, зазначений у пункті 1, не зменшувало кримінальної відповідальності такої особи за вчинені акти.

Стаття 43
Настання відповідальності за кримінальні правопорушення

Відповідальність за правопорушення, установлені відповідно до цієї Конвенції, настає незалежно від характеру відносин між постраждалою особою та правопорушником.

Роздатковий матеріал для Групи 3

Дата укладання: 01.01.2000.

Дата ратифікації Україною: 03.04.2003.

Стаття 1

Держави-учасниці забороняють торгівлю дітьми, дитячу проституцію і дитячу порнографію, як це передбачено цим Протоколом.

Стаття 2

Для цілей цього Протоколу:

a) торгівля дітьми означає будь-який акт або угоду, внаслідок яких дитина передається будь-якою особою або будь-якою групою осіб іншій особі або групі осіб за винагороду або інше відшкодування;

b) дитяча проституція означає використання дитини у діяльності сексуального характеру за винагороду або будь-яку іншу форму відшкодування;

c) дитяча порнографія означає будь-яке зображення будь-якими засобами дитини, яка здійснює реальні або змодельовані відверто сексуальні дії, або будь-яке зображення статевих органів дитини, головним чином в сексуальних цілях.

Стаття 3

1. Кожна держава-учасниця забезпечує, щоб, як мінімум, наступні діяння і види діяльності були повною мірою охоплені її кримінальним або карним правом, незалежно від того, чи були ці злочини вчинені на національному або транснаціональному рівні, або в індивідуальному чи організованому порядку:

a) у контексті торгівлі дітьми, визначеній у статті 2:

I) пропозиція, передача чи отримання будь-якими засобами дитини з метою:

a. сексуальної експлуатації дитини;

b. передачі органів дитини за винагороду;

c. використання дитини на примусових роботах;

II) неправомірне схиляння в якості посередництва до згоди на усиновлення дитини з порушенням застосовних міжнародно-правових актів щодо усиновлення;

b) пропозиція, отримання, передача чи надання дитини для цілей дитячої проституції, визначеній у статті 2;

c) виробництво, розподіл, розповсюдження, імпорт, експорт, пропозиція, продаж або зберігання у вищезазначених цілях дитячої порнографії, визначеної у статті 2.

2. Враховуючи положення національного законодавства держави-учасниці, аналогічні положення застосовуються до спроби вчинення будь-якого з цих діянь, а також до пособництва та співучасті у вчиненні будь-якого з цих діянь.

3. Кожна держава-учасниця передбачає належні міри покарання за ці злочини, виходячи зі ступеня їхньої тяжкості.

4. З урахуванням положень свого національного законодавства кожна держава-учасниця у відповідних випадках вживає заходів щодо визначення відповідальності юридичних осіб за злочини, передбачені у пункті 1 цієї статті. З урахуванням правових принципів держави-учасниці ця відповідальність юридичних осіб може бути кримінальною, цивільною або адміністративною.

5. Держави-учасниці вживають всіх відповідних правових та адміністративних заходів з метою забезпечення того, щоб всі особи, які мають відношення до всиновлення дитини, діяли відповідно до положень застосовних міжнародно-правових актів.

Додаток 2.2.2.3

Загальні питання кваліфікації кримінальних правопорушень, пов'язаних із сексуальною експлуатацією та сексуальним насильством щодо дітей, які вчиняються з використанням електронних засобів комунікації.

Кваліфікація кримінального правопорушення – це встановлення відповідності між вчиненим особою суспільно небезпечного діянням і складом кримінального правопорушення, описаним в законі. Склад кримінального правопорушення є законодавчою моделлю його кваліфікації і відповідно до закону є єдиною необхідною законною підставою кримінальної відповідальності (ч. 1 ст. 2 КК України). Склад кримінального правопорушення дає змогу відмежувати кримінально протиправні діяння від інших видів правопорушень та діянь, щодо яких не існує кримінально правової заборони.

Будь-який склад кримінального правопорушення складається з чотирьох обов'язкових елементів: 1) об'єкта; 2) об'єктивної сторони; 3) суб'єкта; 4) суб'єктивної сторони. Тільки в сукупності перераховані елементи можуть утворювати юридичний зміст підстави кримінальної відповідальності.

Об'єкт складу кримінального правопорушення – це те, на що спрямовано кримінальне правопорушення й чому воно заподіює певної шкоди або створює реальну загрозу заподіяння такої шкоди.

Склади кримінальних правопорушень, пов'язані з сексуальною експлуатацією та сексуальним насильством щодо дітей, які вчиняються з використанням електронних засобів комунікації, розміщені в різних розділах Особливої частини КК України та стосуються таких об'єктів, як суспільна мораль, воля, статева недоторканість неповнолітніх тощо. Важливість зазначених суспільних відносин обумовлює високі стандарти їх кримінально-правового захисту:

- відповідно до українського законодавства, за вчинення будь-яких дій сексуального характеру щодо дитини встановлена кримінальна відповідальність;
- за вчинення вказаний діянь передбачені суворі покарання. У всіх санкціях відповідних статей покаранням передбачено позбавлення волі. Отже, усі кримінальні правопорушення, пов'язані з сексуальною експлуатацією та сексуальним насильством щодо дітей, є злочинами.

Переважна більшість кримінальних правопорушень, пов'язаних з сексуальною експлуатацією та сексуальним насильством щодо дітей, які вчиняються з використанням електронних засобів комунікації, спрямовані на спричинення шкоди конкретній дитині. Склад зазначених кримінальних правопорушень містить таку обов'язкову ознаку як **потерпілий**, яку традиційно розглядають разом з об'єктом кримінального правопорушення та яка є обов'язковою для встановлення. Водночас деякі кримінальні правопорушення, пов'язані з сексуальною експлуатацією та сексуальним насильством щодо дітей, спрямовані на охорону дитинства та статевої недоторканості неповнолітніх загалом, як важливої моральної засади українського суспільства. Наприклад, дитячою порнографією визнається не лише зображення дитини у будь-який спосіб у реальному чи змодельованому відверто сексуальному образі, а також й особи, яка виглядає як дитина (п. 2 Примітки до ст. 156-1 КК України). Подібні види кримінальних правопорушень хоча й безпосередньо не заподіюють шкоду конкретній дитині, але створюють у суспільстві попит на сексуальне насильство та експлуатацію дітей. Тому ці кримінальні правопорушення є не менш суспільно небезпечними.

Для кваліфікації кримінальних правопорушень, пов'язаних з сексуальною експлуатацією та сексуальним насильством щодо дітей, надзвичайно важливим є встановлення віку потерпілої особи. У цьому зв'язку розглянемо декілька ключових понять.

Дитина – будь-яка особа віком до вісімнадцяти років.

Неповнолітній – особа віком до вісімнадцяти років (фактично є синонімом терміну «дитина»).

Малолітній – особа, віком до чотирнадцяти років.

У деяких кримінальних правопорушеннях (наприклад ст. 156 КК України «Розбещення неповнолітніх») потерпілим (-ою) є особа, яка не досягла шістнадцятирічного віку.

Саме з цим віком українське законодавство пов'язує вік, до досягнення якого встановлена абсолютна заборона займатися діяльністю сексуального характеру з дитиною. Отже, в Україні **вік сексуальної згоди** становить 16 років.

Об'єктивна сторона кримінального правопорушення – це сукупність передбачених в КК України ознак, які характеризують зовнішню сторону (зовнішнє вираження) кримінального правопорушення.

Ознаки об'єктивної сторони визначаються в диспозиції через встановлення основних, загальних рис, притаманних конкретному кримінальному правопорушенню. Для встановлення змісту деяких ознак об'єктивної сторони кримінальних правопорушень, пов'язаних з сексуальною експлуатацією та сексуальним насильством щодо дітей, які вчиняються з використанням електронних засобів комунікації, слід звертатися до інших частин цієї або іншої статті, приміток до статей КК України, інших національних або міжнародно-правових актів.

Відповідно до положень Лансаротської конвенції, під **сексуальним насильством щодо дітей** розуміється умисна поведінка дорослої особи, яка полягає в:

a) заняттi дiяльнiстю сексуального характеру з дитиною, яка не досягла передбаченого законодавством віку для заняття діяльністю сексуального характеру;

b) заняттi дiяльнiстю сексуального характеру з дитиною, коли:

- використовується примус, сила чи погрози або
- насильство здійснюється зі свідомим використанням довіри, авторитету чи впливу на дитину, зокрема в сім'ї, або
- насильство здійснюється в особливо вразливій для дитини ситуації, зокрема з причини розумової чи фізичної неспроможності або залежного становища.

Під **сексуальною експлуатацією дітей** розуміють використання дитини для проституції, створення дитячої порнографії, участі в порнографічних виставах тощо.

Важливою ознакою об'єктивної сторони аналізованих кримінальний правопорушень є **спосіб** їх вчинення – «з використанням інформаційно-телекомунікаційних систем або технологій». Під **інформаційно-телекомунікаційними системами** розуміють сукупність інформаційних та електронних комунікаційних систем, які використовують технологію обробки інформації з використанням технічних і програмних засобів. Зазначені системи працюють на основі інформаційно-телекомунікаційних технологій, які є системою методів, процесів та способів використання обчислювальної техніки і систем зв'язку для створення, збору, передачі, пошуку, оброблення та поширення інформації. Вчинення кримінального правопорушення з використанням інформаційно-телекомунікаційних систем або технологій охоплює використання всіх видів сучасних електронних мереж зв'язку, враховуючи всесвітню мережу інтернет, та обробку даних в автоматизованих системах, які є основою функціонування сучасної електронної техніки. Зазначений спосіб вчинення кримінальних правопорушень не завжди безпосередньо зазначений в диспозиції відповідних статей (як, зокрема, в статтях 156-1, 301-1, 301-2 КК України), проте це не виключає можливості вчинення інших кримінальних правопорушень, пов'язаних з сексуальною експлуатацією та сексуальним насильством щодо дітей, з

використанням інформаційно-телекомунікаційних систем або технологій. Так, зокрема, вербування дитини з метою експлуатації (частини 2 і 3 ст. 149 КК України), спонукання неповнолітнього до переміщення на територію іншої держави з метою вступу в шлюб (ст. 151-2 КК України), розбещення неповнолітнього (ст. 156 КК України), втягнення неповнолітнього в заняття проституцією (ч. 3 ст. 303 КК України) можуть бути вчинені з використанням інформаційно-телекомунікаційних систем або технологій. Відсутність безпосереднього закріплення вказано способу в диспозиції статті КК України на кваліфікацію не впливає, проте може бути враховано судом під час призначення покарання.

Суб'єктом кримінального правопорушення є фізична осудна особа, яка вчинила кримінальне правопорушення у віці, з якого відповідно до КК України може наставати кримінальна відповідальність (ч. 1 ст. 18 КК України). В Україні загальний вік кримінальної відповідальності становить шістнадцять років. Знижений вік кримінальної відповідальності – чотирнадцять років – встановлено лише щодо двох найбільш тяжких злочинів, пов'язаних із сексуальним насильством, – зґвалтування (ст. 152 КК України) і сексуального насильства (ст. 153 КК України). Ці злочини зазвичай вчиняються без використанням інформаційно-телекомунікаційних систем або технологій, проте вони можуть поєднуватися з іншими кримінальним правопорушеннями, які вчиняються з їх використанням. Наприклад, створення порнографічних матеріалів може бути поєднано з сексуальним насильством над неповнолітнім; проведення видовищного заходу сексуального характеру також може бути поєднано зі зґвалтуванням неповнолітнього. У таких випадках вчинене має бути кваліфіковано за сукупністю кримінальних правопорушень. Водночас слід врахувати:

- зґвалтування та сексуальне насильство (статті 152, 153 КК України) вчиняються без добровільної згоди потерпілої особи. Згода вважається добровільною, якщо вона є результатом вільного волевиявлення особи, з урахуванням супутніх обставин;
- вік сексуально згоди становить 16 років, тому вчинення з повнолітньою особою дій сексуального характеру, пов'язаних із вагінальним, анальним або оральним проникненням в тіло особи, яка не досягла шістнадцятирічного віку, з використанням геніталій, іншого органу чи частини тіла або будь-якого предмета, навіть за наявності згоди неповнолітньої особи є злочином, передбаченим ст. 155 КК України «Вчинення дій сексуального характеру з особою, яка не досягла шістнадцятирічного віку»; здійснення дій сексуального характеру без проникнення в тіло потерпілої особи – злочином, передбаченим ст. 156 КК України «Розбещення неповнолітніх»;
- зґвалтування та сексуальне насильство щодо особи, яка не досягла чотирнадцяти років, є злочином незалежно від її добровільної згоди, тобто у всіх випадках;
- відповідно до положень Лансаротської конвенції та їх закріплення в КК України, норми про кримінальну відповідальність за сексуальні злочини не поширюються на врегулювання статевих стосунків між неповнолітніми, що здійснюються за взаємною згодою (тобто за відсутності насильства, погрози його застосування або наявності фізичної або психічної безпорадності неповнолітнього).

Слід звернути увагу, що у значній кількості складів кримінальних правопорушень, які пов'язані із сексуальною експлуатацією та сексуальним насильством щодо дітей, у статтях КК України встановлено підвищений вік кримінальної відповідальності – 18 років (наприклад статті 155, 156-1 КК України) або цей факт випливає зі змісту відповідної норми (частини 2 і 3 ст. 149, ч. 3 ст. 301-2 або ч. 3 ст. 303 КК України – діяльність, пов'язана з втягненням неповнолітніх у сексуальну експлуатацію).

Суб'єктивна сторона кримінального правопорушення – це його внутрішня сторона, тобто психічна діяльність особи, що відображає ставлення її свідомості і волі до вчинюваного суспільно небезпечного діяння та до його наслідків.

Обов'язковою ознакою суб'єктивної сторони будь-якого складу кримінального правопорушення є вина особи. Кримінальні правопорушення, пов'язані з сексуальною експлуатацією та сексуальним насильством щодо дітей, які вчиняються з використанням електронних засобів комунікації, характеризуються лише з прямим умислом, тобто особа усвідомлювала суспільно небезпечний характер свого діяння і бажала його вчинити. Водночас необхідним є доведення, що, вчиняючи відповідне діяння, особа **усвідомлювала (достовірно знала чи припускала), що вчиняє такі дії щодо неповнолітньої або малолітньої особи або повинна була і могла це усвідомлювати**. Згідно з роз'ясненням Пленуму Верховного Суду України, суд повинен враховувати не тільки показання підсудного, а й потерпілої особи, ретельно перевіряти їх відповідність усім конкретним обставинам справи. Під час вирішення цього питання враховується вся сукупність обставин справи, зокрема зовнішні фізичні дані потерпілої особи, її поведінка, знайомство винної особи з нею, володіння винною особою відповідною інформацією (п. 10 Постанови Пленуму Верховного Суду України «Про судову практику у справах про злочини проти статевої свободи та статевої недоторканості особи» від 30.05.2008 р. № 5). У переважній більшості випадків злочинці, що вчиняють сексуальну експлуатацію та сексуальне насильство з використанням електронних засобів комунікації, навмисно спрямовують свою злочинну діяльність на неповнолітніх і малолітніх осіб.

Останнє, на що хотілося б звернути увагу, – це особливості застосування кримінальної юрисдикції щодо кримінальних правопорушень, пов'язаних з сексуальною експлуатацією та сексуальним насильством щодо дітей, які вчиняються з використанням електронних засобів комунікації. Встановлення кримінальної юрисдикції України щодо певного діяння є передумовою застосування до нього закону України про кримінальну відповідальність. Значна кількість аналізованих правопорушень вчиняється з використанням всесвітньої мережі інтернет або інших видів електронних комунікацій, що мають транснаціональний характер. Закон України про кримінальну відповідальність розповсюджує свою дію на кримінальні правопорушення, пов'язані з сексуальною експлуатацією та сексуальним насильством щодо дітей, які вчинено із використанням електронних засобів комунікації, в таких випадках:

- суб'єкт кримінального правопорушення знаходиться на території України (наприклад особа, яка розповсюджує дитячу порнографію в інтернеті, або особа, яка одержала до неї доступ);
- потерпіла особа знаходиться на території України (наприклад неповнолітній, якому в режимі особистого спілкування в мережі інтернет було зроблено пропозицію взяти участь у видовищному заході сексуального характеру);
- кримінальне правопорушення вчинено за кордоном громадянином України або особою без громадянства, що постійно проживає в Україні.

Додаток 2.2.2.4

Кримінально-правова характеристика кримінальних правопорушень, пов'язаних із сексуальною експлуатацією та сексуальним насильством щодо дітей, які вчиняються із використанням електронних засобів комунікації

Розглянемо ознаки кримінальних правопорушень, пов'язаних із сексуальною експлуатацією та сексуальним насильством щодо дітей, які вчиняються із використанням електронних засобів комунікації. Деякі із зазначений кримінальних правопорушень у своєму складі передбачають ознаку «з використанням інформаційно-телекомунікаційних систем або технологій» як альтернативний спосіб вчинення кримінального правопорушення. Інші кримінальні правопорушення або їх окремі форми, хоча й не містять вказівки на специфічний спосіб вчинення, проте нерідко вчиняються саме з використанням електронних засобів комунікації.

Торгівля людьми (ст. 149 КК України)

Форма кримінального правопорушення: вербування неповнолітнього або малолітнього, вчинене з метою сексуальної експлуатації з використанням електронних засобів комунікації (частини 2 і 3 ст. 149 КК України).

Основним безпосереднім **об'єктом** кримінального правопорушення є воля неповнолітнього або малолітнього. Безпосереднім додатковим об'єктом є суспільна мораль, здоров'я та життя дитини, її нормальний, психічний, фізичний та соціальний розвиток.

Потерпілим є неповнолітня (ч. 2) або малолітня особа (ч. 3).

Об'єктивна сторона кримінального правопорушення може виражатися в одній з альтернативних дій: торгівля людиною, вербування, переміщення, переховування, передавання або одержання людини.

Торгівля людиною – це передавання людини однією особою (продавцем) та відповідне її одержання іншою особою (покупцем) безповоротно або на певний строк, за грошову винагороду або з іншої корисливою метою.

Під **вербуванням** з метою сексуальної експлуатації розуміють схиляння особи працювати чи надавати послуги сексуального характеру зазвичай здійснюваного за матеріальну винагороду. Форми самого схиляння можуть бути різними – запрошення, умовляння, переконання, обіцянка матеріальної винагороди тощо. Зазначені дії можуть бути вчинено з використанням будь-яких телекомунікаційних платформ. Наслідки і результативність таких дій на кваліфікацію не впливають.

Враховуючи особливу вразливість дітей, законодавець визначив, що відповідальність за вербування малолітнього чи неповнолітнього для експлуатації настає незалежно від того, чи вчинені такі дії з використанням примусу, викрадення, обману, шантажу чи уразливого стану зазначених осіб або із застосуванням чи погрозою застосування насильства, використання службового становища, або особою, від якої потерпілий був у матеріальній чи іншій залежності, або підкупу третьої особи, яка контролює потерпілого, для отримання її згоди на експлуатацію людини (п. 3 Примітки до ст. 149 КК України).

Суб'єктом аналізованої форми кримінального правопорушення визнається фізична осудна повнолітня особа.

Суб'єктивна сторона характеризується прямим умислом. Щодо віку потерпілої особи, то винний достовірно знає або припускає, що така особа є неповнолітньою або малолітньою, або повинен був і міг це усвідомлювати.

Спеціальною **метою** цього кримінального правопорушення є експлуатація, під якою зокрема розуміють всі форми сексуальної експлуатації, використання в порнобізнесі, примусову вагітність, примусове одруження тощо.

Примушування до шлюбу (ст. 151-2 КК України)

Форма кримінального правопорушення: примушування особи, яка не досягла шлюбного віку згідно із законодавством, до вступу в шлюб, до вступу у співжиття без укладання шлюбу, або до продовження такого співжиття, або спонукання з цією метою особи до переміщення на територію іншої держави, ніж та, в якій вона проживає, вчинене з використанням електронних засобів комунікації (ч. 2 ст. 151-2 КК України)

Основним безпосереднім **об'єктом** кримінального правопорушення є воля дитини, додатковим – суспільна мораль, нормальний, психічний, фізичний та соціальний розвиток дітей.

Потерпілим є особа, яка не досягла шлюбного віку згідно із законодавством. Шлюбний вік для чоловіків та жінок в Україні становить вісімнадцять років (ст. 22 Сімейного кодексу України).

Об'єктивна сторона кримінального правопорушення полягає в одному з альтернативних дій:

- примушуванні до вступу в шлюб;
- примушуванні до вступу у співжиття без укладання шлюбу або до продовження такого співжиття;
- спонуканні з цією метою особи до переміщення на територію іншої держави, ніж та, в якій вона проживає.

На відміну від вербування з метою сексуальної експлуатації дитини (частини 2 і 3 ст. 149 КК України), примушування до шлюбу з застосуванням електронних засобів комунікації здійснюється із застосуванням психологічного насильства – психологічного тиску, погроз, шантажу, залякування тощо.

Суб'єктом цієї форми кримінального правопорушення визнається фізична осудна повнолітня особа. Винний усвідомлює, що вчиняє кримінальне правопорушення щодо особи, яка не досягла шлюбного віку.

Суб'єктивна сторона характеризується прямим умислом. Щодо віку потерпілої особи, то винний достовірно знає або припускає, що така особа є неповнолітньою або малолітньою, або повинен був і міг це усвідомлювати.

Розбещення неповнолітніх (ст. 156 КК України)

Об'єктом розбещення неповнолітніх є статева недоторканність дитини, її нормальний, психічний, фізичний та соціальний розвиток.

Потерпілим цього кримінального правопорушення є особа, якій не виповнилося 16 років (ч. 1), у кваліфікованому складі – малолітня особа (ч. 2). Для кваліфікації не має значення попередня поведінка потерпілої особи (зокрема її попереднє статеве життя й досвід) та чи давала потерпіла згоду на вчинення щодо неї розпусних дій.

Об'єктивна сторона цього кримінального правопорушення полягає у вчиненні розпусних дій щодо особи, яка не досягла шістнадцятирічного віку. Розпусні дії мають сексуальний характер і спрямовані на задоволення винною особою статевої пристрасті або на збудження у потерпілої особи статевого інстинкту. Розпусні дії поділяють на фізичні та інтелектуальні (п. 17 Постанови Пленуму Верховного Суду України «Про судову практику у справах про злочини проти статевої свободи та статевої недоторканості особи» від 30.05.2008 р. № 5). До інтелек-

туального розбещення, наприклад, відносять цинічні розмови з потерпілою особою на сексуальні теми, ознайомлення дитини із порнографічними зображеннями, спонукання спостерігати за сексуальним насильством або діяльністю сексуального характеру або відповідними відеоматеріалами. Усі вказані дії можуть бути вчинені з використанням електронних засобів комунікації. Водночас злочинці, які використовують електронні засоби комунікації, також спонукають та навчають дітей вчиненню різних дій і практик сексуального характеру: демонструють здійснення акту онанізму, спонукають потерпілих самостійно здійснити дії сексуального характеру і розповісти про свої відчуття, зробити власні відверті фотографії або відверті фотографії інших неповнолітніх членів родини, вчиняти інші дії, що збуджують статевий інстинкт. Зазначені дії можна визнати дистанційним фізичним розбещенням неповнолітніх.

Розбещення вважається закінченим з моменту вчинення розпусних дій, незалежно від результативності.

Суб'єктом кримінального правопорушення є фізична осудна особа, яка досягла 16 років. У випадку вчинення розбещення членами сім'ї чи близькими родичами потерпілого або особою, на яку покладено обов'язки щодо його виховання або піклування про нього, відповідальність настає за ч. 2 ст. 156 КК України.

Суб'єктивна сторона кримінального правопорушення характеризується прямим умислом стосовно вчинення розпусних дій. Щодо віку потерпілої особи, то винний достовірно знає або припускає, що така особа не досягла 16 років, або повинен був і міг це усвідомлювати.

Домагання дитини для сексуальних цілей (ст. 156-1 КК України)

Це кримінальне правопорушення отримало назву «грумінг» – налагодження довірливих стосунків з дитиною з метою сексуального насильства над нею; у випадку вчинення вказаний дій з використанням електронних засобів комунікації зазначені дії називають «кібергрумінгом». Стаття 156-1 КК України закріплює відповідальність за грумінг і містить в собі два самостійних склади кримінальних правопорушень, які мають різну мету.

Об'єктом домагання дитини для сексуальних цілей є статева недоторканність особи, її нормальний, психічний, фізичний та соціальний розвиток, суспільна мораль.

Потерпілим є особа, яка не досягла шістнадцятирічного віку (частини 1 і 2), і малолітня особа в кваліфікованому складі (ч. 3).

Об'єктивна сторона кримінального правопорушення є складною і містить в собі поєднання двох обов'язкових діянь: 1) пропозиції зустрічі, зробленої суб'єктом злочину потерпілій особі; 2) вчинення хоча б однієї дії, спрямованої на те, щоб така зустріч відбулася.

Альтернативним **способом** вчинення цього кримінального правопорушення є використанням інформаційно-телекомунікаційних систем або технологій. Так пропозиція зустрічі може бути здійснена з використанням мобільного телефону чи комп'ютера через надсилання повідомлення через соціальні мережі, месенджери тощо. Окрім того, запропонована злочинцем зустріч також може бути запланована для проведення не в реальному житті, а в режимі онлайн. Так, відповідно до п. 1 Примітки до цієї статті під зустріччю слід розуміти, зокрема, зустріч, проведення якої передбачає використання інформаційно-телекомунікаційних систем або технологій (наприклад засобів відеозв'язку). Фактично ця стаття встановлює більш високий стандарт захисту, ніж розбещення, передбачене у ст. 156 КК України: злочин вважається закінченим після того, як винний запропонував зустріч потерпілій особі і вчинив хоча б одну дію, спрямовану на те, щоб така зустріч відбулася (наприклад надіслав потерпілій особі запрошення для відеозустрічі), незалежно від того, чи вона відбулася в подальшому.

Суб'єктом кримінального правопорушення є фізична осудна повнолітня особа.

Суб'єктивна сторона кримінального правопорушення характеризується прямим умислом. Щодо віку потерпілої особи, то винний достовірно знає або припускає, що така особа не досягла 16 років, або повинен був і міг це усвідомлювати.

Кримінальне правопорушення має **спеціальну мету**:

- вчинення стосовно потерпілого будь-яких дій сексуального характеру або розпусних дій (ч. 1);
- втягнення потерпілого у виготовлення дитячої порнографії (ч. 2).

Під **дитячою порнографією** розуміють зображення у будь-який спосіб дитини чи особи, яка виглядає як дитина, у реальному чи змодельованому відверто сексуальному образі або задіяної у реальній чи змодельованій відверто сексуальній поведінці, або будь-яке зображення статевих органів дитини в сексуальних цілях (п. 2 Примітки до ст. 156-1 КК України).

У випадку поєднання аналізованого складу з іншими кримінальними правопорушеннями, пов'язаними із сексуальною експлуатацією та сексуальним насильством щодо дітей (зґвалтування, сексуальне насильство, вчинення дій сексуального характеру з особою, яка не досягла шістнадцятирічного віку, розбещення неповнолітніх, виготовлення дитячої порнографії тощо), вчинене кваліфікується за правилами сукупності кримінальних правопорушень.

Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження (ст. 301-1 КК України)

Об'єктом незаконних дій з дитячою порнографією є моральні засади суспільства в сфері сексуальних відносин, нормальний, психічний, фізичний та соціальний розвиток дітей.

Предметом кримінального правопорушення є дитяча порнографія (п. 2 Примітки до ст. 156-1 КК України). За формою вираження дитяча порнографія може мати будь-яку візуальну форму – порновідео, порнозображення, порнографічні комп'ютерні програми тощо.

Потерпілим у примушуванні до участі у створенні дитячої порнографії є неповнолітня (ч. 3) або малолітня особа (ч. 4).

Об'єктивна сторона кримінального правопорушення виражається в одній з альтернативних дій:

- одержання доступу до дитячої порнографії. У цій формі обов'язковим є спосіб вчинення злочину – використання інформаційно-телекомунікаційних систем чи технологій (ч. 1). Вказані дії вважають умисними, якщо доведено, що особа усвідомлювала, що у такий спосіб вона отримає доступ до дитячої порнографії (наприклад доведено, що особа отримала такий доступ повторно або за допомогою внесення плати тощо) (Примітка до ст. 301-1 КК України);
- придбання або зберігання дитячої порнографії (ч. 1);
- ввезення в Україну, перевезення чи інше переміщення дитячої порнографії чи її розповсюдження (ч. 1, 2);
- виготовлення, розповсюдження, збут дитячої порнографії (ч. 3);
- примушування дитини до участі у створенні дитячої порнографії (ч. 3, 4). Таке примушування може бути як фізичним, так і психологічним, зокрема й з використанням інформаційно-телекомунікаційних систем чи технологій.

Такі форми аналізованого кримінального правопорушення як придбання, зберігання, розповсюдження, збут, виготовлення, так само, як і примушування до участі у створенні дитячої порнографії, можуть бути вчинено з використанням інформаційно-телекомунікаційних систем чи технологій.

Суб'єкт кримінального правопорушення загальний – фізична осудна особа, яка досягла 16 років.

Суб'єктивна сторона характеризується прямим умислом. У тих випадках, коли у злочині наявний потерпілий, винний має достовірно знати або припускати, що така особа є неповнолітньою або малолітньою, або повинен був і міг це усвідомлювати.

Обов'язковою ознакою суб'єктивних сторони є **мета**:

- без мети збуту чи розповсюдження щодо діянь, передбачених в ч. 1;
- з метою збуту чи розповсюдження щодо діянь, передбачених в ч. 2.

Законодавець встановив дві підстави виключення кримінальної відповідальності за діяння, пов'язані з дитячою порнографією:

- не підлягає кримінальній відповідальності неповнолітня особа за виготовлення, зберігання, перевезення чи інше переміщення дитячої порнографії, якщо такі дії вчинені без мети збуту чи розповсюдження (ч. 5).
- не підлягає кримінальній відповідальності за діяння, передбачені ч. 1 ст. 301-1 КК України, особа, яка вчинила їх з метою виконання покладених на неї повноважень на підставах і в порядку, передбачених законодавством (ч. 6).

Проведення видовищного заходу сексуального характеру за участю неповнолітньої особи (ст. 301-2 КК України)

Об'єктом кримінального правопорушення є моральні засади суспільства в сфері сексуальних відносин, нормальний, психічний, фізичний та соціальний розвиток дітей.

Потерпілим є неповнолітня (частини 1-3) або малолітня особа (частини 2, 4).

Об'єктивна сторона кримінального правопорушення виражається в одній з альтернативних дій:

- проведення видовищного заходу сексуального характеру, у якому задіяно неповнолітню особу (ч. 1);
- відвідування видовищного заходу сексуального характеру з метою його перегляду, у якому очевидно для відвідувача задіяно малолітню чи неповнолітню особу (ч. 2);
- втягнення неповнолітньої чи малолітньої особи до участі у видовищному заході сексуального характеру, що проходить (частини 3, 4);
- примушування неповнолітньої чи малолітньої особи до участі у такому заході з використанням обману, шантажу, уразливого стану особи або із застосуванням чи погрозою застосування насильства (частини 3, 4).

Під **видовищним заходом сексуального характеру** у цій статті слід розуміти публічний показ у будь-якій формі продукції сексуального характеру або сценічні дії, метою яких є втілення сексуальних дій (Примітка до ст. 301-2 КК України). Під **продукцією сексуального характеру** розуміють будь-які матеріальні об'єкти, предмети, друкована, аудіо-, відеопродукція, зокрема реклама, повідомлення та матеріали, продукція засобів масової інформації, електронних засобів масової інформації, призначені для задоволення сексуальних потреб людини. Сценічні дії, метою яких є втілення сексуальних дій, зокрема, охоплюють випадки примушування дітей позувати перед вебкамерою на вебресурсах чи у приватних чатах з метою відтворення сексуальних дій або реальне вчинення щодо дітей актів сексуального насильства. У таких випадках кваліфікація здійснюється за сукупністю кримінальних правопорушень, що передбачають відповідальність за сексуальне насильство щодо дитини.

Альтернативним **способом** вчинення цього кримінального правопорушення є використання інформаційно-телекомунікаційних систем або технологій. Діяння, що охоплюються об'єктивною стороною цього кримінального правопорушення, можуть відтворюватися з певних цифрових носіїв або транслюватися у певний час наживо через приватні чи секретні чати або сайти.

Суб'єкт кримінального правопорушення загальний – фізична осудна особа, яка досягла 16 років.

Суб'єктивна сторона кримінального правопорушення характеризується прямим умислом. Щодо віку потерпілої особи, то винний достовірно знає або припускає, що така особа є неповнолітньою або малолітньою, або повинен був і міг це усвідомлювати.

Сутенерство або втягнення особи в заняття проституцією (ст. 303 України)

Форма кримінального правопорушення: втягнення неповнолітнього або малолітнього в заняття проституцією або примушування їх до зайняття проституцією, вчинене з використанням електронних засобів комунікації (частини 3 і 4 ст. 303 КК України).

Під **проституцією** розуміють платне надання сексуальних послуг. Відмітними ознаками проституції є безособовий (відчужений) характер відносин між суб'єктами сексуальних відносин, корисливий і систематичний характер надання сексуальних послуг. Указані критерії дають змогу відмежувати проституцію як від корисливих подружніх відносин, шлюбу з розрахунку, так і від позашлюбних сексуальних зв'язків, заснованих на особистих симпатіях і потягах, а також від безладних сексуальних відносин у підлітковому віці, які хоча й можуть носити безособовий характер, обумовлені некорисливою мотивацією.

Об'єктом кримінального правопорушення є моральні засади суспільства в сфері сексуальних відносин, нормальний, психічний, фізичний та соціальний розвиток дітей.

Потерпілим є неповнолітня (ч. 3) або малолітня особа (ч. 4).

Об'єктивна сторона кримінального правопорушення полягає в:

- втягненні дитини в заняття проституцією. Форми самого втягнення можуть бути різними – запрошення, умовляння, переконання, обіцянка матеріальної винагороди, обман тощо. Зазначені діяння можуть бути вчинено через будь-які телекомунікаційні платформи. Наслідки і результативність таких дій на кваліфікацію не впливають;
- примушуванні дитини до зайняття проституцією. Зазначена форма кримінального правопорушення також може бути вчинена з використанням електронних засобів комунікації і полягає у застосуванні психологічних форм насильства щодо дітей з метою примусу до надання сексуальних послуг третім особам (погрози, шантаж, залякування фізичною розправою над потерпілим чи його близькими, розголошенням відомостей, які потерпілий бажає залишити у таємниці тощо).

Враховуючи особливу вразливість дітей, законодавець визначив, що відповідальність за втягнення малолітнього чи неповнолітнього в заняття проституцією чи примушування їх до заняття проституцією за цією статтею має наставати незалежно від того, чи вчинені такі дії з використанням обману, шантажу, уразливого стану зазначених осіб або із застосуванням чи погрозою застосування насильства, використанням службового становища, або особою, від якої потерпілий був у матеріальній чи іншій залежності.

Суб'єктом аналізованої форми кримінального правопорушення визнається фізична осудна повнолітня особа.

Суб'єктивна сторона характеризується прямим умислом. Щодо віку потерпілої особи, то винний достовірно знає або припускає, що така особа є неповнолітньою або малолітньою, або повинен був і міг це усвідомлювати.

Додаток 2.2.2.5

Роздатковий матеріал для Групи 1

У липні минулого року Пилипенко, знаходячись у себе вдома та використавши власний ноутбук, зареєструвався у соціальній мережі Фейсбук під ніками XXL74 і OlexanderOlexander. Використавши створений обліковий запис OlexanderOlexander, у соціальній мережі Фейсбук він познайомився і певний час переписувався з п'ятнадцятирічною Соколовою. Через декілька тижнів обміну повідомленнями він запросив Соколову зустрітися на пляжі озера в населеному пункті, де вони проживали. Пилипенко прийшов на зустріч зі своїм приятелем Охтирком, якого він познайомив з Соколовою. Після півторагодинного спільного відпочинку на пляжі, коли Соколова пішла до переодягальні, Пилипенко запропонував їй вступити в статеві зносини з Охтирком. Спочатку Соколова не погоджувалася, однак Пилипенко умовив її, запевнивши, що про це ніхто не дізнається. Їх з Охтирком статеві зносини він зняв на камеру мобільного телефону. Потім він переслав Охтирку вказаний відеоролик, знову запевнивши Соколову, що ніхто про це більше не дізнається. Наступного дня Пилиненко, використавши мережу Фейсбук, під ніком XXL74 розіслав вищезазначений відеоролик п'яти неповнолітнім особам. У подальшому з одним з них Пилипенко вступив у переписку і через деякий час запропонував створювати такі ж «прикольні дорослі відео». Проте здійснити зустріч з неповнолітнім Пилипенко не встиг, оскільки був затриманий працівниками кіберполіції.

Роздатковий матеріал для Групи 2

Родіонова, дізнавшись про існування у мережі інтернет вебсайтів, на яких користувачі зі всього світу за допомогою комп'ютерної техніки з вебкамерами задовольняють свої статеві потреби за допомогою віртуального спілкування з дівчатами, які за винагороду на вимогу клієнтів оголюють своє тіло в режимі реального часу, вирішила організувати такий бізнес. З цією метою вона орендувала офісне приміщення та уклала договір про надання послуг доступу до мережі інтернет, після чого облаштувала його меблями та комп'ютерною технікою. Родіонова через соціальні мережі та мобільні застосунки підшукувала дівчат 15-17 років, пропонуючи роботу в офісі «вебмоделями». Під час особистої зустрічі вона доводила до їхнього відома принципи роботи, а саме – спілкування з клієнтами з України та іноземних держав на сексуальні теми, в умовах реального часу із застосуванням вебкамер. Родіонова знала, що реєстрація у мережі інтернет на вебсайтах, де здійснюється спілкування між чоловіками та жінками, можлива лише повнолітньої особи. Отримавши від дівчат добровільну згоду на участь у своєму бізнесі, з метою приховання віку останніх, вона здійснила виготовлення фальшивих паспортів громадянина України (ID - картки), схожих на справжні, в яких змінювала рік народження особи. Надалі Родіонова фотографувала дівчат із зміненим паспортом громадянина України й табличкою з датою подачі заявки на реєстрацію на вказаних сайтах та надавала кожній виконавиці персональний логін і пароль для входу (авторизації) на сайті «coomeet.com», водночас реєстрацію на сайті проводила особисто. В подальшому «моделі» приходили у створений «Вебінтимколл центр», де, використовуючи ноутбуки, обладнані вебкамерами, авторизувалися на вищезазначених сайтах і в режимі онлайн спілкувалися з користувачами цих сайтів, на їхні побажання оголялися, здійснювали маніпуляції зі статевими органами. За вчинення вказаних дій на відповідні акаунти неповнолітніх дівчат нараховувались грошові кошти, доступ до яких мала лише Родіонова. Кожного тижня Родіонова виплачувала дівчатам певну суму із зароблених ними таким способом грошей.

Роздатковий матеріал
для Групи 3

32-річний Ломов, зареєструвавши обліковий запис в соціальній мережі Інстаграм, почав спілкування з 15-річною Ласкіною. Протягом декількох тижнів він вів з нею бесіди на відверті сексуальні теми, а потім за допомогою прохань, обіцянок та погроз почав вимагати від Ласікіної, щоб остання виготовила та надала йому власні фотознімки інтимного характеру. Через погрози Ласкіна за допомогою власного мобільного телефону виготовляла та в соціальній мережі Інстаграм пересилала Ломову власні відверті фотознімки, на яких були зображені її оголені статеві органи. Після цього Ломов продовжив спілкування з Ласкіною в мережі Інстаграм і, погрожуючи оприлюдненням її відвертих фотознімків, схилив її здійснити з ним особисту зустріч у себе дома для продовження стосунків. Наступного тижня Ласкіна прийшла на побачення до квартири Ломова, де він торкався її інтимних частин тіла, збуджуючи її статевий інстинкт, і сам займався онанізмом. Через тиждень він знову запросив Ласкіну на побачення до себе додому, де за її згодою вступав з неї у природній статевий акт.

2.3. ОСОБЛИВОСТІ ДІЯЛЬНОСТІ КІБЕРПОЛІЦЕЙСЬКИХ

ТЕМА 2.3.1. Організаційно-тактичні основи розслідування кіберзлочинів

Мета: відпрацювати навички організації і тактики розслідування кіберзлочину.

Загальна тривалість: 4 академічні години (180 астрономічних хвилин).

План:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Правила проходження квесту	Інформаційне повідомлення	10 хв	Мультимедійне обладнання
2.	Вебквест	Індивідуальна робота	160 хв	Комп'ютери для учасників з доступом до інтернету, Додаток 2.3.1.1, Додаток 2.3.1.2
3.	Висновки	Запитання – відповіді	10 хв	

ХІД ЗАНЯТТЯ

1. Інформаційне повідомлення «Правила проходження квесту»

Мета: ознайомити з правилами проходження вебквесту, надати відповідні інструкції.

Час: 10 хв.

Необхідні матеріали: мультимедійне обладнання.

Хід проведення:

Тренер/тренерка звертається до учасників: «*Особливостями проходження квесту є те, що під час вирішення відповідних завдань учасникам:*

- *дозволяється користуватися будь-якими джерелами інформації;*
- *потрібно надати відповідь на конкретні питання, без яких неможливо пройти подальші завдання;*
- *на основі шаблонів документів складаються конкретні процесуальні документи;*
- *засвоюються типові алгоритми дій в різних оперативно-тактичних ситуаціях.*

Для створення вебквесту використовувалися інструменти Google Classroom.

Учасники можуть бути запрошені до класу через приватний код чи автоматично імпортуватися з навчального сайту. Кожен клас створює окрему папку на Google диску відповідного користувача GoogleDrive, куди учасник може подати роботу, яку оцінює тренер.

Під час проведення квесту:

- *доступ до завдань відкриватиметься послідовно та супроводжуватиметься поясненнями помилок на кожному етапі;*
- *тестові питання будуть завданнями, після завершення виконання яких потрібно ввести результат як відповідь;*
- *усі документи, використані в завданнях, відповідають реальним за формою, але не за змістом;*
- *квест охоплює велику кількість елементів реального розслідування за відповідними категоріями кримінальних проваджень.*

2. Індивідуальна робота «Вебквест»

Мета: відпрацювання вмінь розслідування кіберзлочину.

Час: 160 хв.

Необхідні матеріали: комп'ютери для учасників з доступом до інтернету, Додаток 2.3.1.1, Додаток 2.3.1.2.

Хід проведення:

Тренер/тренерка дає завдання учасникам, зокрема:

1. Авторизуватись у системі Google Classroom та долучитись до класу, вказаного тренером.

2. З використанням відомих інструментів проаналізувати наявні матеріали, скласти пакет документів, пройти тестові завдання.

До уваги тренера/тренерки!

Завдання квесту викладено в Додатку 2.3.1.1.

Тренер/тренерка має створити та адаптувати під себе Google Classroom для відпрацювання цієї вправи. Приклад такого віртуального класу міститься за посиланням: https://classroom.google.com/c/NjE3MTA4NzIwMzgy?cjc=65pltff.

Перелік інструментів, які можна запропонувати використовувати учасникам, міститься в Додатку 2.3.1.2.

3. Висновки

Мета: підбити підсумки заняття та поділитись враженнями.

Час: 10 хв.

Хід проведення:

Тренер/тренерка просить учасників дати відповіді на запитання:

- *Що важливого ви сьогодні зрозуміли для себе?*
- *Чому новому навчились?*
- *Як будете використовувати набуті знання?*

Тестові питання до теми:

1. Які пошукові системи вказано не правильно?

А) Google;

Б) Yahoo;

В) Hama;

Г) Meta.

2. Які технології найімовірніше могли використовувати злочинці для зберігання в мережі 2 Тб протиправного контенту?

А) ICQ-пейджер;

Б) хмарні технології;

В) Вайбер;

Г) VPN.

3. Який вид розвідки називають OSINT?

А) агентурна розвідка;

Б) радіотехнічна розвідка;

В) розвідка з відкритих джерел;

Г) оперативна розвідка.

4. Який з наведених ресурсів дозволяє виявити розташування точок доступу Wi-Fi за MAC-адресою або назвою?

А) wigle.net;

Б) stalkscan.com;

В) yasiv.com/vk;

Г) youcontrol.com.ua.

5. Якою з наведених електронних поштових адрес слід скористатися для запиту інформації через форми взаємодії з правоохоронними органами на мережних сервісах (Фейсбук, Твіттер, Гугл тощо)?

А) зареєстрованою на поштовому сервері cybercrime.gov.ua;

Б) зареєстрованою на поштовому сервері gmail.com;

В) зареєстрованою на поштовому сервері mail.ru;

Г) зареєстрованою на поштовому сервері i.ua.

Ключі-відповіді:

1. В; 2. Б; 3. В; 4. А; 5. А.

Додаток 2.3.1.1

Перший блок квесту присвячено висвітленню теоретичних питань онлайн-ґрумінгу. В межах цього блоку слід розтлумачити учасникам основні поняття, а також навести загальний алгоритм вирішення завдань квесту.

Завдання № 1 має на меті навчити учасників окремим елементам тактики розслідування та закріпити базові навички пошуку інформації в мережі. Для цього надається фабула та тестові завдання. Крім того, учасникам пропонується скласти декілька документів, які допоможуть у подальшому русі розслідування.

Завдання 1

До правоохоронного органу надійшла низка заяв про те, що невстановлена особа регулярно вступає в листування з неповнолітніми під вигаданими даними. Через зловживання довірою правопорушник виманює у неповнолітніх фото та відео інтимного характеру за їхньою участю.

Після шантажує неповнолітніх, примушуючи їх переказувати йому кошти, надсилати нові матеріали інтимного характеру, залучати інших неповнолітніх до створення порнографічного контенту. Відомо, що шуканий суб'єкт одержує кошти через систему EasyPay на гаманці:

?

77777770; 77777771; 77777772; 77777773;

77777774; 77777775; 77777776; 77777778.

Спілкування зі сторонніми особами вказаний суб'єкт здійснює через програму Телеграм, у якій відомий його псевдонім.

Вжити заходи для ідентифікації особи правопорушника, встановлення місць його регулярного перебування та затримання. Відповісти на питання квесту. Скласти запити: 1) про отримання інформації щодо відповідних гаманців EasyPay; 2) призупинення руху коштів по гаманцях.

У завданні № 2 змодельована ситуація, коли учасник одержав відомості за результатами опрацювання складених ним на попередньому етапі документів. Відтак, тепер потрібно проаналізувати надані відповіді, скласти протокол та відповісти на питання тактичного характеру в тесті. На підставі результатів аналізу учасникам потрібно буде підготувати документ для отримання відповіді від провайдера телекомунікацій та звернутися до банку для одержання відомостей про рух коштів за певними платіжними картками.

Завдання 2

Після звернення до EasyPay до правоохоронного органу надійшла інформація в електронному вигляді із супровідним листом. Провести аналіз відомостей, що надійшли, та скласти протокол.

?

Скласти запит до провайдера про одержання відповідних відомостей.

Підготувати змістову частину звернення до банку про одержання відповідних відомостей.

Прийняти рішення щодо подальших дій.

Завдання № 3 містить відповіді провайдера та банку, які потрібно проаналізувати та оформити це процесуально. У наданих документах містяться зачіпки, які можуть призвести до встановлення особи підозрюваного, які потрібно знайти та вказати у тестовому завданні.

Завдання 3

До правоохоронного органу надійшли відповіді з банківської установи та від провайдера про належність запитуваної IP-адреси. Потрібно проаналізувати вказані відповіді та визначити подальший рух розслідування.

Скласти протокол огляду документу, який надійшов з банківської установи. Відповісти на питання квесту.

Завдання № 4 передбачає відпрацювання учасниками навичок криміналістичного аналізу електронних зображень, а також пошуку інформації за різними ідентифікаторами в інтернеті. Завдання можна вирішити декількома способами.

Завдання 4

Належність IP-адреси збігається із місцем роботи особи, номер телефону якої було виявлено у відповіді банківської установи. В результаті подальших дій правоохоронних органів було висунуто обґрунтоване припущення, що саме ця особа причетна до вчинення відповідних правопорушень. Відчувши зростання уваги з боку правоохоронних органів, підозрюваний виїхав за кордон. Поточне місце перебування підозрюваного встановити не вдалося.

У результаті проведення обшуку за місцем його проживання не було виявлено відповідного апаратно-програмного забезпечення, за допомогою якого підозрюваний вчиняв протиправну діяльність. Водночас у помешканні було знайдено мобільний пристрій, з якого було вилучено фотографію підозрюваного, а також встановлено назву декількох точок доступу Wi-Fi, до яких підключався підозрюваний.

Крім наведеного, правоохоронці дізналися, що підозрюваний вів активне листування з володільцем одного облікового запису.

Встановити ймовірне місцезнаходження підозрюваного та додаткові відомості про його співрозмовника. Відповісти на питання квесту.

Завдання № 5 орієнтовано на використання неочевидних онлайн-інструментів типу відновлення квитанції за її номером, а також дає змогу відпрацювати навички зворотного пошуку за зображенням.

Завдання 5

У межах взаємодії з правоохоронними органами США фотознімок підозрюваного було показано в кафе, де працівники цього закладу впізнали свого постійного відвідувача. Вирішувалося питання про його екстрадицію до України. Але, вийшовши під заставу, підозрюваний зник у невідомому напрямку.

Через місяць, здійснюючи моніторинг мережі інтернет, правоохоронці виявили активність у профілі соціальної мережі підозрюваного. Серед іншого він розмістив декілька світлин з міста, де зараз мешкає. Також на одному із фотознімків оперативні працівники змогли розгледіти та відновити фрагмент чеку за сплату комунальних послуг, який лежав на столі.

Встановити можливе місце перебування підозрюваного. Відповісти на питання квесту.

У завершальному блоці квесту викладено результати проведеного розслідування.

Додаток 2.3.1.2

Набір інтрументів для проходження вебквесту

Bellingcat's Online Investigation Toolkit	docs.google.com/spreadsheets/d/18rtqh8EG2q1xBo2cLNyhIDuK9jrPGwYr9DI2UncoqJQ/edit#gid=930747607
Search Investigative and Forensic Toolbar	search.org/resources/search-investigative-and-forensic-toolbar
Awesome OSINT	github.com/jivoi/awesome-osint
Curious OSINT Resource List	docs.google.com/document/d/14li22wAG2Wh2y0UhgBjbqEvZJCDsNZY8vpUAJ_jJ5X8/edit
IntelTechniques	inteltechniques.com
Internet Crimes Against Children	icaccops.com/users/OSINT
List of Resource Links from Open-Source Intelligence Summit 2021	sans.org/blog/list-of-resource-links-from-open-source-intelligence-summit-2021
Research Clinic Research and investigation links	researchclinic.net/links.html
The Ultimate OSINT Collection	start.me/p/DPYPMz/the-ultimate-osint-collection
Tools: OSINT & Internet Investigations	netbootcamp.org/osinttools
CTI & OSINT resources	docs.google.com/spreadsheets/d/1klugQqw6POlBtuzon8S0b18-gpsDwX-5OYRrB7TyNEw/htmlview
101+ OSINT Resources for Investigators	i-sight.com/resources/101-osint-resources-for-investigators
20+ OSINT resources for breach data research	osintme.com/index.php/2021/04/18/20-osint-resources-for-breach-data-research
Social Media Hacker List	github.com/MobileFirstLLC/social-media-hacker-list
OSINT Collection	github.com/sinwindie/OSINT
OSINT Tools	github.com/mattwright324
OSINT Toolkit	comskills-ukraine.co.uk/resources/osint-toolkit
Online Research Cheat Sheets	toddington.com/resources/cheat-sheets
The Open Source Intelligence resource discovery	rr.reuser.biz
Offensive Security Cheatsheet	cheatsheet.haax.fr/open-source-intelligence-osint
Hackers-Arise: The Best Intro to Hacking!	hackers-arise.com/osint
Formulas for Searching Facebook	plessas.net/facebookmatrix
OSINT tools collection	cipher387.github.io/osint_stuff_tool_collection
Awesome-Telegram-OSINT	github.com/ItIsMeCall911/Awesome-Telegram-OSINT

Awesome Threat Intelligence resources	github.com/threat-hunting/awesome-threat-intelligence
OH SHINT!	ohshint.gitbook.io/oh-shint-its-a-blog/
OSINT Jobs	osint-jobs.com
APIs for OSINT	github.com/cipher387/API-s-for-OSINT
Top OSINT & Infosec Resources for You and Your Team: 100+ Blogs, Podcasts, YouTube Channels, Books, and more!	maltego.com/blog/top-osint-infosec-resources-for-you-and-your-team/
All you can read	allyoucanread.com
BIRN Investigative Resource Desk	bird.tools/tools
Malfrat's OSINT Map	map.malfrats.industries

ТЕМА 2.3.2. Використання спеціальних знань під час розслідування кіберзлочинів

Мета: навчитися особливостям використання спеціальних знань під час вивчення електронних доказів.

Загальна тривалість: 4 академічні години (180 астрономічних хвилин).

План:

№	Назва вправи	Форма проведення вправи	Час	Необхідні матеріали
1.	Особливості огляду засобів комп'ютерної техніки	Інформаційне повідомлення	40 хв	Мультимедійне обладнання, Додаток 2.3.2.1
2.	Огляд стандартних засобів комп'ютерної техніки. Додаткові інструменти криміналістичного аналізу	Індивідуальна робота	130 хв	Комп'ютери для учасників з доступом до інтернету та пристроями для читання компакт-дисків, LiveCD на базі ОС Linux Ubuntu CyberPack/ALF
3.	Висновки	Запитання – відповіді	10 хв	

ХІД ЗАНЯТТЯ

1. Інформаційне повідомлення «Особливості огляду засобів комп'ютерної техніки»

Мета: надати знання щодо особливостей огляду засобів комп'ютерної техніки відповідно до вимог законодавства.

Час: 40 хв.

Необхідні матеріали: мультимедійне обладнання, Додаток 2.3.2.1.

Хід проведення:

Тренер/тренерка звертається до учасників: «*Основними засобами комп'ютерної техніки, із якими доводиться мати справу працівникам правоохоронних органів, на теперішній час є: стаціонарні персональні комп'ютери (робочі станції або сервери); ноутбуки та нетбуки; планшети; бортові комп'ютери автомобілів; телевізори із функцією SMART; GPS-навігатори; носії цифрової інформації (диски, флешносії тощо); периферійне обладнання (принтери, сканери тощо); мобільні комп'ютерні пристрої із функцією телефону*», після чого презентує інформацію, яка міститься у Додатку 2.3.2.1.

2. Індивідуальна робота «Огляд стандартних засобів комп'ютерної техніки. Додаткові інструменти криміналістичного аналізу»

Мета: навчитися автоматизації аналізу електронних даних для складання протоколів слідчих (розшукових) дій.

Час: 130 хв.

Необхідні матеріали: комп'ютери для учасників з доступом до інтернету та пристроями для читання компакт-дисків, LiveCD на базі ОС Linux Ubuntu CyberPack/ALF.

Хід проведення:

Перед проведенням заняття тренеру/тренерці необхідно створити низку завантажуваних дисків CyberPack. Відповідний образ та інструкцію по роботі з ним можна завантажити за посиланням https://ualinux.com/uk/ubuntu-cyberpack. Вказаний дистрибутив містить набір основних засобів для базового огляду комп'ютерної системи.

Тренер/тренерка звертається до учасників із завданням:

1. Налаштувати у системі BIOS досліджуваного ПК пріоритетне завантаження з оптичного диску.
2. Завантажити LiveCD.
3. Для початку документування дій оглядача запустити програму відеофіксації зображення екрану.
4. Перевірити, що після завантаження системи за умовчанням усі диски змонтовано тільки для читання. Змінити параметри монтування, вказавши дозвіл на запис, після чого підключити флешкарту, на яку будемо записувати відповідні дані огляду.
5. Під час огляду дізнатися параметри системи за допомогою вбудованих інструментів. Видану інформацію потрібно внести до протоколу.
6. За необхідності потрібно підготувати налаштування мережі. Оглянути віддалену вебсторінку.
7. Скористатися однією з вбудованих утиліт для одержання відповідної інформації про домен.
8. Відпрацювати інші інструменти огляду в системі.
9. З використанням каталогу Computer Forensics Tool Catalog (http://toolcatalog.nist.gov) обрати інструменти, потрібні для аналізу зображень, які працюють в ОС Windows та дозволяють аналізувати GPS теги зображень з відображенням їх на карті. Визначити, які з інструментів є безоплатними та які мають найновіші релізи.
10. З використанням одного з безоплатних застосунків, обраних у попередньому пункті, проаналізувати декілька зображень з інтернету.

3. Висновки до заняття

Мета: підбити підсумки заняття та поділитись враженнями.

Час: 10 хв.

Хід проведення:

Тренер/тренерка просить учасників дати відповіді на запитання:

- *Що важливого ви сьогодні зрозуміли для себе?*
- *Чому новому навчились?*
- *Як будете використовувати набуті знання?*

Тестові питання до теми:

1. У чому полягає сенс контрольної суми (Cheksum) для стерилізованого носія інформації?

А) логічна сума за допомогою операції «або»;

Б) логічний добуток за допомогою операції «та»;

В) логічне віднімання за допомогою операції «ні»;

Г) сума перших 32 та останніх 32 байтів в кожному секторі.

2. Що з наведеного НЕ належить до основних інструментів, які можуть знадобитися працівнику правоохоронних органів для огляду засобів комп'ютерної техніки?

А) накопичувачі інформації, серед яких обов'язково має бути носій, ємністю більшою від ємності накопичувача, який підлягає огляду;

Б) пульвіризатор;

В) викрутка;

Г) блокувач жорсткого диску та/або набір дублікаторів.

3. Що потрібно долучити як додаток до протоколу огляду засобів комп'ютерної техніки, якщо він здійснюється із використанням Live-CD під керуванням Linux?

А) ліцензійний ключ до програми;

Б) чек, який підтверджує законність придбання програмного забезпечення;

В) відповідну копію програми із ґеш-сумою диску;

Г) згоду компанії Microsoft на використання непропрієтарного програмного забезпечення.

4. Що таке волатильні дані?

А) дані, які зберігаються в енергозалежних запам'ятовувальних пристроях: оперативній пам'яті, кеші, регістрах;

Б) дані, які зберігаються з тильного боку вінчестера;

В) дані файлу реєстру Windows;

Г) дані на флешкарті.

5. Які з наведених програмно-апаратних рішень не використовуються для криміналістичного дослідження мобільних телефонних пристроїв?

А) ABBYY FINERADER;

Б) MPE+;

В) UFED;

Г) XRY.

Ключі-відповіді:

1. А; 2. Б; 3. В; 4. А; 5. А.

Додаток 2.3.2.1

Враховуючи особливості роботи із наведеними пристроями, а також відповідне апаратне та програмне забезпечення, використовуване для їх огляду, відповідний процес можна умовно розділити на чотири види:

1) огляд стандартних ЗКТ носіїв та периферійних пристроїв;
2) огляд мобільних ЗКТ:
   - із функцією телефону;
   - автомобільних пристроїв;
3) огляд побутових ЗКТ («розумних речей»);
4) огляд інших ЗКТ.

Перед проведенням відповідного огляду важливо правильно підібрати інструментарій оглядача. Водночас слід пам'ятати, що швидкий розвиток технологій, а також велика кількість умов, які виникають під час огляду ЗКТ, з практичного погляду унеможливлюють так звану сертифікацію відповідних апаратних та/або програмних засобів. Це підтверджується і правозастосовною практикою провідних західних країн. В Україні така сертифікація також не проводиться, зважаючи на її недоречність. Так само в процесі огляду потрібно намагатися уникати використання програм, наявних у системі, що підлягає огляду, адже потім буде складно підтвердити правильність їх роботи.

Тому, враховуючи українське законодавство, видається правильним акцентувати увагу на двох важливих аспектах. По-перше, використовувані засоби мають бути з відповідною відкритою ліцензією або такими, що перебувають на балансі правоохоронного органу, аби можна було у будь-який час перевірити коректність їх роботи. По-друге, якщо використовується відкрите програмне забезпечення, наприклад Live-CD під керуванням Linux, то відповідну копію із ґеш-сумою диску потрібно долучити як додаток до протоколу огляду.

Основні інструменти, які можуть знадобитися працівнику правоохоронних органів для огляду ЗКТ, є такими: портативний комп'ютер з автономним джерелом живлення; привод CD-ROM (DVD-ROM); викрутки та інший інструмент; комплекти запасних батарей; диски з операційними системами та іншими програмними засобами, накопичувачі інформації, серед яких обов'язково має бути носій, ємністю більшою від ємності накопичувача, який підлягає огляду, блокувач жорсткого диску та/або набір дублікаторів, польовий комплект експерта криміналіста тощо.

Взагалі, перелік інструментарію залежить від конкретної ситуації. У цьому сенсі в процесі його підбору вельми корисними стають регулярно оновлювані каталоги криміналістичних програмних та апаратно-програмних засобів. Наприклад, перелік криміналістичного програмного забезпечення, протестованого Американським інститутом стандартизації (NIST), можна зайти за посиланням: toolcatalog.nist.gov.

Після підготовки відповідного інструментарію, який можна вважати підготовчим етапом огляду, проведення інших підготовчих заходів, працівники правоохоронного органу переходять до безпосередньо збирання даних на місці події. З урахуванням вивчення сучасної зарубіжної та вітчизняної практики і критичного осмислення цього матеріалу, сам алгоритм огляду ЗКТ у загальному вигляді можна представити як на Рис. 1.

Коментуючи окремі елементи цього алгоритму, потрібно зауважити, що на сьогодні в Україні практично не відбувається збирання та документування нестійких волатильних даних (зберігаються в енергозалежних запам'ятовувальних пристроях: оперативній пам'яті, кеші, регістрах), хоча саме волатильні дані часто містять ключі до різних криптоконтейнерів, останні

повідомлення у мережі та відкриті документи тощо. Так само потрібно звернути увагу на мережні технології віддаленого зберігання даних (хмари, термінали тощо).

Щодо копіювання неволатильних даних, то на теперішній час у світі застосовується три головних способи одержання копій цифрових носіїв, що містять слідову інформацію:

1) створення образу відповідного носія;
2) створення дублікату носія;
3) логічне копіювання окремих даних.

Перший спосіб є більш повільним, водночас за його допомогою працівник правоохоронних органів одразу одержує готовий для дослідження програмними засобами матеріал, який можна достатньо легко тиражувати для здійснення розподіленого дослідження декількома фахівцями одночасно.

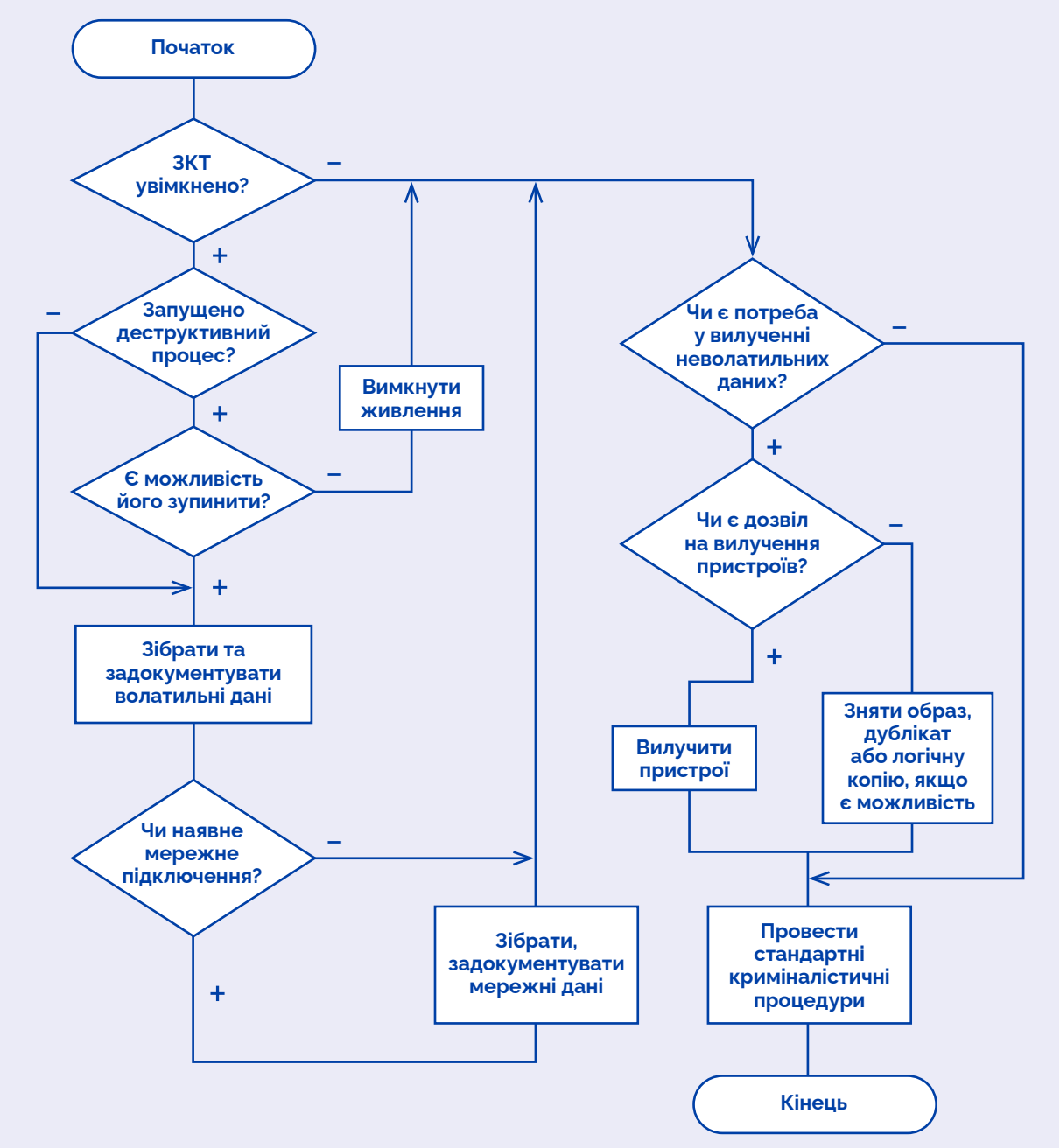


Рис. 1. Загальний алгоритм техніки огляду ЗКТ

У будь-якому разі для убезпечення електронних доказів рекомендується робити дві копії цифрового носія, одна з яких є контрольною (еталонною) та зберігається на випадок втрати або пошкодження іншої – робочої копії цифрового носія. Вилучені пристрої та носії потрібно належним чином зберігати та досліджувати. Наприклад, для дослідження мобільних пристроїв потрібно використовувати клітку Фарадея.

Перед зняттям копії більшості цифрових носіїв потрібно одержати ґеш-значення для вихідного носія інформації (джерела) за алгоритмом SHA-1 або SHA-2. Підрахунок ґешу за допомогою алгоритму MD5 проводити не рекомендується, враховуючи можливості знаходження колізій з прийнятною обчислювальною складністю, що неодноразово демонструвалися дослідниками для цього алгоритму.

Слід пам'ятати, що особливості зберігання даних на окремих носіях (флешкарти, SSD-вінчестери), а також вирівнювання ступеню їх зношеності, призводять до того, що посекторне ґеш-значення такого носія може не збігатися під час наступного підрахунку. У цьому випадку можна говорити лише про можливість підтвердження ґеш-значеннями так званих «логічних» структур даних, наприклад окремих файлів тощо.

Перед одержанням дублікату цифрового носія інформації (джерела) потрібно простерилізувати носій, на який будуть копіюватися відповідні дані (приймач). Цей носій, по-перше, має бути за ємністю більшим від джерела, по-друге, перед створенням дублікату його потрібно заздалегідь стерилізувати, тобто заповнити усі сектори нулями. Окремі дослідники пропонують лише частково стерилізувати носій вже після копіювання даних в частині, що не зайнята скопійованими даними.

У подальшому скопійовані дані найчастіше передаються для дослідження експерту, проте слідчий може самостійно оглянути їх у межах процедури огляду речей і документів, результати чого зафіксувати у відповідному протоколі.

Якщо слідчий має необхідну кваліфікацію або залучив спеціаліста, то за допомогою відповідних засобів він може, наприклад, дослідити робочу копію образу.

У загальному вигляді такий огляд з урахуванням певних міркувань можна представити так:

- Аналіз даних, одержаних з оперативних запам'ятовуючих областей, зокрема буферу обміну.
- Аналіз залишкових слідів в елементах ОС, які вказують на дані, що оброблювались системою:
  - дослідження використовуваного програмного забезпечення;
  - дослідження елементів системних файлів;
  - дослідження та перевірка назв і реквізитів ярликів;
  - дослідження файлів історій відповідних програмних засобів;
  - дослідження налаштувань інтернет-браузерів;
  - дослідження атрибутів та метаданих файлів, що викликали інтерес під час перевірки.
- Аналіз безпосередньо файлів з даними за допомогою контекстного пошуку за ключовими фразами:
  - дослідження файлів, які зберігаються на цифрових носіях, зокрема:
  - пошук прихованих та зашифрованих даних;
  - пошук та перевірка тимчасових файлів;

- аналіз специфічних даних, передбачених структурою файлової системи, наприклад альтернативних потоків даних;
- аналіз файлів, що пов'язані з мережною активністю;
- відновлення з подальшим аналізом видалених файлів, зокрема:
- дослідження залишків файлів в кластерах;
- перевірка вільного простору носіїв інформації;
- перевірка файлів підкачки, якщо вони є.

Огляд мобільних ЗКТ має свої особливості. Найбільш складним елементом у цьому процесі є зняття дампу даних мобільного пристрою, оскільки для цього потрібно мати спеціальні права доступу до нього. Дамп зазвичай знімається програмним шляхом, проте окремі апаратно-програмні комплекси дають змогу проводити зняття фізичного дампу пристроїв безпосередньо з відповідних чіпів (наприклад UFED, XRY).

Одним з джерел доказової інформації можуть бути автомобільні засоби комп'ютерної техніки. Для їх дослідження використовується спеціальне програмне забезпечення, наприклад iVe (https://www.berla.co/).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антифейкова інтелектуальна гра «НотаЄнота». URL: https://notaenota.com/.
2. Василевич В. Профілактика віктимологічна/Велика українська кримінологічна енциклопедія. У 2 т. Т. 2: М-Я/редкол. : В.В. Сокуренко (голова), О.М. Бандурка (співголова) та ін.; наук. Ред.. О.М. Литвинов. Харків: Факт, 2021. 397 с.
3. Глобальний посібник із удосконалення законодавчої бази для захисту дітей від сексуальної експлуатації та насильства в Інтернеті. URL: https://www.unicef.org/reports/legislating-digital-age.
4. Директива ЄС 2011/93/ЄС щодо протидії сексуальному насильству та сексуальній експлуатації дітей та дитячій порнографії. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093.
5. Запобігання та протидія сексуальній експлуатації та насильству щодо дітей (СЕНД). Типова державна система реагування. URL: https://rm.coe.int/vc-1840-weprotect-model-national-response-translated-ukr-web-pdf-pdf/1680992d8f.
6. Зарядка з медіаграмотності. URL: https://filter.mkip.gov.ua/wp-content/uploads/2021/08/zaryadka-z-mediagramotnosti.pdf.
7. Захист дітей у цифровому середовищі: рекомендації для органів державної влади. URL: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/1/za-initsiativi-mintsifri-pidgotuvali-rekomendatsii-shchodo-zakhistu-ditey-u-tsifrovomu-seredovishchi/COP-Guidelines%20for%20Policy%20Makers_UA_fin%20(2).pdf.
8. Захист прав дітей у цифровому світі – один із стратегічних пріоритетів Європейської Комісії. URL: https://www.nrada.gov.ua/zahyst-prav-ditej-u-tsyfrovomu-sviti-odyn-iz-strategichnyh-priorytetiv-yevropejskoyi-komisiyi/.
9. Звіт дослідження: Швидка оцінка ситуації щодо кібербезпеки дітей 10-18 років. Київ, 2022.С. 31-33. URL: http://surl.li/nwkfn.
10. Іванцова А. Інтернет-тролі на службі в олігархів та політиків. URL: https://www.radiosvoboda.org/a/27042051.html.
11. Інфомедійна грамотність онлайн: посібник для тренера / за заг. ред. Тараненко О. / Розроблено в рамках проєкту «Вивчай та розрізняй: інфо-медійна грамотність». Київ: IREX, 2021. 400 с. URL: https://filter.mkip.gov.ua/wp-content/uploads/2022/04/l2d-e_online_curriculum_6s_8-1.pdf.
12. Кампанія «Уважні батьки». URL: https://childfund.org.ua/diialnist/kampaniia-uvazhni-batky.
13. Керівні приницпи Комітету міністрів Ради Європи щодо правосуддя, дружнього до дітей. URL: https://rm.coe.int/16804c2188.
14. Керівні принципи політики Ради Європи щодо комплексних національних стратегій із захисту дітей від насильства. URL: https://rm.coe.int/168046eb82.
15. Кодекс України про адміністративні правопорушення. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text.
16. Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.
17. Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства. URL: https://zakon.rada.gov.ua/laws/show/994_927#Text.

18. Кримінальний кодекс України.
URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

19. Лансаротська конвенція. Глобальний інструмент захисту дітей від сексуального насильства. URL: https://rm.coe.int/prems-095619-ukr-2576-lanzarote-convention-leaflet-web-a-5-1-/168096674b/.

20. Манжай О.В., Носов В.В. Навчальний посібник з кібергігієни для закладів вищої освіти зі спеціальними умовами навчання МВС України. Київ, 2024. 230 с.

21. Методичні рекомендації для працівників поліції щодо організації роботи з дитино, яка перебуває у конфлікті з законом. Ковальова О.В., Сухарєва А.О., Проценко О.О., Одеса: Одеський державний університет внутрішніх справ. 2022. 50 с.

22. Методичні рекомендації щодо організації роботи з дітьми за методикою «Зелена кімната» для слідчих та ювенальних поліцейських. URL: https://www.unicef.org/ukraine/media/16976/file/Green%20Room%20Methodology%20for%20Police%20Offciers.pdf.

23. Набір для класної та позакласної роботи «Як аналізувати медіа критично».
URL: https://filter.mkip.gov.ua/wp-content/uploads/2021/08/l2d-s_universal_handouts-1.pdf.

24. Національний проект з медіаграмотності «Фільтр». Ігри та квести.
URL: https://filter.mkip.gov.ua/dlya-vsih/igry-ta-kvesty/.

25. Онлайн курс для молоді «Кіберпростір та кібербезпека».
URL: https://cyber.volunteer.kyiv.ua/#/.

26. Online сексуальне насильство над дітьми (кібер грумінг).
URL: https://www.youtube.com/watch?v=b-gaa9ZI2JE&ab_channel=StopSextingUkraine.

27. Освіта в сфері прав людини в Інтернеті. Методичний посібник. Мурашкевич О.А., Черних О.О. К.: ВАІТЕ. 2015. 70 с. URL: https://rescentre.org.ua/images/Uploads/Files/internet_safety_dl/education_HR_in_internet.pdf.

28. Підготовка працівників Національної поліції України у частині забезпечення та захисту прав дітей: навчально-методичний посібник.
URL: https://drive.google.com/file/d/12KmkngjjomaD_MGZEnMVndRlWagK7Uw2/view?fbclid=IwAR1QiPWF8dDkoDYeyic-qhyXE6xl4qsSK9VX5beK3Jio88d2s6Ud0HGmlrQ.

29. Посібник для інтернет-користувачів. URL: https://rm.coe.int/16802e3e96.

30. Посібник з питань прав дитини в цифровому середовищі для органів державної влади.
URL: https://rm.coe.int/prems-091920-gbr-2576-it-handbook-ukr-web/1680a2dbeb.

31. Посібник з прав людини для інтернет-користувачів та пояснювальний меморандум.
URL: https://rm.coe.int/16802e3e96.

32. Посібник із безпеки дітей в Інтернеті.
URL: https://services.google.com/fh/files/events/bia_curriculum_2021_ua.pdf.

33. Пояснювальний висновок щодо застосовності Лансаротської конвенції до сексуальних злочинів щодо дітей, яким сприяє використання інформаційно-комунікаційних технологій (ІКТ).
URL: https://rm.coe.int/lc-opinion-on-csea-facilitated-by-icts-uk-/1680a13215.

34. Про освіту: Закон України від 05 вересня 2017 року № 2145-VIII.
URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text.

35. Правила дитячої безпеки в Інтернеті – поради кіберполіції. URL: https://cyberpolice.gov.ua/article/pravyla-dytyachoyi-bezpeky-v-interneti--porady-kiberpolicziyi-8250/.

36. Про внесення змін до деяких законодавчих актів України щодо імплементації Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротської конвенції): Закон України від 18 лютого 2021 року. URL: https://zakon.rada.gov.ua/laws/show/1256-20#Text.

37. «Проєкти»: URL: https://dn.npu.gov.ua/activity/ekspertna-radainnovaczijnix-idej/proekti.html.

38. Про забезпечення соціального захисту дітей, які перебувають у складних життєвих обставинах: постанова Кабінету Міністрів України від 01 червня 2020 року № 585. URL: https://zakon.rada.gov.ua/laws/show/585-2020-%D0%BF#Text.

39. Про затвердження Інструкції з організації роботи підрозділів ювенальної превенції Національної поліції України: наказ Міністерства внутрішніх справ України від 19 грудня 2017 року № 1044. URL: https://zakon.rada.gov.ua/laws/show/z0686-18#Text.

40. Про затвердження критеріїв віднесення продукції до такої, що має порнографічний характер: наказ Міністерства культури України від 16 березня 2018 року №212. Офіційний вісник України. 2018. № 33. Ст. 1178.

41. Про медіа: Закон України від 13 грудня 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2849-20#n2354.

42. Про Національну поліцію: Закон України від 02 липня 2015 року № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

43. Про основні засади забезпечення кібербезпеки в Україні: Закон України від 05 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

44. Про охорону дитинства: Закон України від 26 квітня 2001 року. URL: https://zakon.rada.gov.ua/laws/show/2402-14#n2.

45. Про План реалізації Стратегії кібербезпеки України: рішення Ради Національної безпеки і оборони України від 30 грудня 2021 року. Введено в дію Указом Президента України від 1 лютого 2022 року № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text.

46. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 року № 447/221. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

47. Протидія залучення дітей російськими військовими до протиправної діяльності через Інтернет. URL: https://stop-sexting.in.ua/wp-content/uploads/2022/06/zaluchennya_do_protypravnoi%CC%88_povedinky-1.pdf.

48. Протидія кібербулінгу та кібергрумінгу в Україні: попередній аналітичний огляд. URL: https://cyber.bullyingstop.org.ua/storage/media-archives/docuweek_analytical-report.pdf.

49. Профілактика деструктивної поведінки підлітків (Т. Журавель & Ю. Удовенко, ред.). Видавництво ФОП Буря О.Д. Київ, 2022. 144 с.

50. Психолого-педагогічні та правові засади діяльності поліції із захисту прав дитини: навч. посіб. / за заг. ред. д-ра юрид. наук, доц. Д. В. Швеця; [Д. В. Швець, О. М. Бандурка, О. І. Федоренко та ін.]; МВС України, Харків. нац. ун-т внутр. справ. Харків: ХНУВС, 2020. 284 с. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/d46b32f2-0308-4811-978d-12994f309521/content.

51. Рекомендації для директивних органів щодо захисту дитини в цифровому середовищі. URL: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/1/za-initsiativi-mintsifri-pidgotuvali-rekomendatsii-shchodo-zakhistu-ditey-u-tsifrovomu-seredovishchi/COP-Guidelines%20for%20Policy%20Makers_UA_fin%20(2).pdf.

52. Рекомендації CM/Rec (2018)7Комітету міністрів державам-членам про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі. URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168086193.

53. Рекомендація Комітету міністрів Ради Європи Rec(2001)16 щодо захисту дітей від сексуальної експлуатації. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805e2c81.

54. Рекомендація Комітету міністрів Ради Європи CM/Rec(2009)5 про заходи щодо захисту дітей від шкідливого контенту та поведінки та сприяння їх активній участі в новому інформаційному та комунікаційному середовищі. URL: https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2009)5&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.

55. Рекомендація Комітету міністрів Ради Європи CM/Rec(2018)7 щодо керівних принципів поваги, захисту та реалізації прав дитини в цифровому середовищі. URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168086193.

56. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20.01.2012 № 2-рп/2012. Офіційний вісник України. 2012. № 9 (10.02.2012), стор. 106, стаття 332.

57. Розробка шкільного уроку на тему безпеки підлітків від сексуальних ризиків в мережі Інтернет. URL: https://stop-sexting.in.ua/wp-content/uploads/2020/02/urok2019.pdf.

58. Сексуальне насильство над дітьми та сексуальна експлуатація дітей в Інтернеті в Україні: аналітичний звіт. URL: https://drive.google.com/file/d/1qPWJZ140hv24dZJcClmJv7yVwbrMVIEK/view.

59. Сексуальне насильство та експлуатація дітей в цифровому середовищі. URL: https://stop-sexting.in.ua/wp-content/uploads/2022/03/rekomendacziyi_slidchym_prokuroram_suddyam_zahyst_ditej_onlajn.pdf.

60. Спільна програма Європейського Союзу та Ради Європи «Зміцнення інформаційного суспільства в Україні». Загальні питання. URL: https://hr-online.org.ua/ua/faq/zagalni_pitannya

61. Стаття 20. Правопорушення, що стосуються дитячої порнографії. URL: https://rm.coe.int/leaflet-on-article-20-of-the-lanzarote-convention-offences-concerning-/16809fc76d.

62. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/ show/685/2021#Text.

63. Стратегія Ради Європи з прав дитини на 2022-2027 роки «Права дитини на практиці: від стабільної реалізації до спільного новаторства». URL: https://rm.coe.int/coe-strategy-for-the-rights-uk/1680a774c4.

64. Уважні онлайн або як запобігти спокушанню дітей онлайн: сценарій зустрічі з батьками. URL: https://childfund.org.ua/Uploads/Files/campaing_materials/scenario_parents.pdf.

65. Убезпечення від неправдивих повідомлень: інформаційна безпека як складова національної безпеки: метод. рекоменд./О.В. Ковальова, А.Г. Пишна. Одеса: ОДУВС, 2022. 74 с.

66. Цифрове десятиліття для дітей та молоді: нова європейська стратегія кращого Інтернету для дітей (BIK+).
URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN.

67. Черних О.О. Онлайк: навчально-методичний посібник., К.: BAITE, 2020. – 108 с. URL: https://rescentre.org.ua/images/Uploads/Files/internet_safety_dl/Manual_Onlike.pdf.

68. Щодо захисту дітей від сексуальної експлуатації та сексуального насильства. Лист МОН від 10 листопада 2022.
URL: https://mon.gov.ua/storage/app/media/pozashkilna/bezpeka/2022/15.11.2022/Lyst.vid.10.11.2022-4.3250-22.Shchodo.zakhystu.ditey.vid.seksualnoyi.ekspluatatsiyi.ta.seksualnoho.nasylstva.pdf.

69. Як батькам убезпечити дітей від онлайн-небезпеки – рекомендації кіберполіції.
URL: https://cyberpolice.gov.ua/article/yak-batkam-ubezpechyty-ditej-vid-onlajn-nebezpeky---rekomendacziyi-kiberpolicziyi-4406/.

70. Як відбувається грумінг в інтернеті? Історія української родини.
URL: https://www.youtube.com/watch?app=desktop&v=yGYKGa6J9eY&ab_channel=StopSextingUkraine.

71. Як працює пропаганда і чому люди потрапляють під її вплив.
URL: https://ua.hive-mind.community/blog/345,yak-pracyuje-propaganda-i-comu-lyudi-potraplyayut-pid-yiyi-vpliv?fbclid=IwAR2co5mgvHrunlkj0dSFIDgziYVEXq3woA7QYjeeTJDDTD5zUw5qIYpAhCs.

72. Appropriate terminology.
URL: https://www.interpol.int/en/Crimes/Crimes-against-children/Appropriate-terminology.

73. Blocking and categorizing content. URL: https://www.interpol.int/en/Crimes/Crimes-against-children/Blocking-and-categorizing-content.

74. BREAKING THE SILENCE AROUND SEXTORTION. The links between power, sex and corruption. URL: https://images.transparencycdn.org/images/2020_Report_BreakingSilenceAroundSextortion_English.pdf.

75. Child Online Protection.
URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP/COP.aspx.

76. Child Sexual Exploitation. URL: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/child-sexual-exploitation.

77. Children and parents: media use and attitudes report 2016.
URL: https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf.

78. Children and parents: media use and attitudes report 2022.
URL: https://www.ofcom.org.uk/__data/assets/pdf_file/0024/234609/childrens-media-use-and-attitudes-report-2022.pdf.

79. COP 2020 Guidelines.
URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP-2020-Guidelines.aspx.

80. Digital Engagement and Protection.
URL: https://www.unicef-irc.org/research/child-rights-in-the-digital-age/.

81. Find the Fake. URL: https://www.internetmatters.org/issues/fake-news-and-misinformation-advice-hub/find-the-fake/choose-quiz/.

82. Guidelines for Law Enforcement First Responders in Child Sexual Abuse and Exploitation Cases. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Grace%20Guidelines%202022_Public_0.pdf.

83. How can you stay safe online during a global crisis? URL: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/how-can-you-stay-safe-online-during-global-crisis.

84. How does fake news spread? URL: https://www.bbc.co.uk/bitesize/articles/z6kxxyc.

85. How to report misinformation online. URL: https://www.who.int/campaigns/connecting-the-world-to-combat-coronavirus/how-to-report-misinformation-online/.

86. Internet literacy handbook.
URL: ttps://rm.coe.int/internet-literacy-handbook/1680766c85.

87. Internet World Stats. 2022. URL: https://www.internetworldstats.com/stats.htm.

88. International Child Sexual Exploitation database. URL: https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database.

89. K.U. v. Finland (application no. 2872/02).
URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-89964%22]}.

90. Lanzarote Committee key monitoring findings on: «The protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs): addressing the challenges raised by child self-generated sexual images and/or videos (CSGIV)». URL: https://rm.coe.int/factsheet-lanzarote-committee-key-monitoring-findings-on-the-protectio/1680a61c7c.

91. Luxembourg Guidelines. URL: https://ecpat.org/luxembourg-guidelines/.

92. Michigan Teen Latest Casualty of Sextortion.
URL:https://cyberbullying.org/sextortion-michigan-teen.

93. Our response to crimes against children. URL: https://www.interpol.int/Crimes/Crimes-against-children/Our-response-to-crimes-against-children.

94. Online sexual coercion and extortion as a form of crime affecting children. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf.

95. Palfrey J. Digital natives and the three divides to bridge [Електронний ресурс]/Palfrey J., Gasser U., Maclay C., Beger G. // In The State of the World's Children. – 2011. – Chapter 1: The emerging generation. – P. 14 – 15. – URL: http://www.unicef.org/sowc2011/pdfs/SOWC-2011-Main-Report_EN_02092011.pdf.

96. Right to the protection of one's image.
URL: https://www.echr.coe.int/Documents/FS_Own_image_ENG.pdf.

97. Sextortion. URL: https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/sextortion.

98. Söderman v. Sweden (application no.5786/08).
URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-128043%22]}.

99. Teenage Sexting Statistics. URL: https://www.guardchild.com/teenage-sexting-statistics/.

100. Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. URL: https://www.inhope.org/media/pages/the-facts/download-our-whitepapers/terminology-guidelines/97e0f829f7-1647827870/terminology-guidelines-396922-en-1.pdf.

101. The Annual Report 2021. URL: https://annualreport2021.iwf.org.uk/.

102. The 4Cs: Classifying Online Risk to Children.
URL: https://core-evidence.eu/posts/4-cs-of-online-risk.

103. View Yellow Notices.
URL: https://www.interpol.int/en/How-we-work/Notices/View-Yellow-Notices.

104. What are you concerned about? Classifying children's and parents' concerns regarding online communication.
URL: https://leibniz-hbi.de/uploads/media/default/cms/media/hl9lir5_2018-11-01_ECREA_Hasebrink%20et%20al_What%20are%20you%20concerned%20about.pdf.

105. Zaman B., Nouwen M. Parental controls: advice for parents, researchers and industry. URL: https://www.academia.edu/29049259/Parental_controls_advice_for_parents_researchers_and_industr.

106. 2nd monitoring round «The protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs)».
URL: https://www.coe.int/en/web/children/2nd-monitoring-round.

107. 4 arrested in takedown of dark web child abuse platform with some half a million users (Europol, 2021). URL: https://www.europol.europa.eu/newsroom/news/4-arrested-in-takedown-of-dark-web-child-abuse-platform-some-half-mil-lion-users 04/05/2021.

ПІДГОТОВКА ПОЛІЦЕЙСЬКИХ ПІДРОЗДІЛІВ ПРЕВЕНТИВНОЇ ДІЯЛЬНОСТІ, СЛІДСТВА ТА ДІЗНАННЯ, КІБЕРПОЛІЦЕЙСЬКИХ З ПИТАНЬ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДІТЕЙ У КІБЕРПРОСТОРІ

НАВЧАЛЬНО-МЕТОДИЧНИЙ ПОСІБНИК

Рекомендовано до друку рішенням Вченої ради Одеського державного університету внутрішніх справ (протокол №5 від 25 листопада 2024 року).

АВТОРСЬКИЙ КОЛЕКТИВ:

Апетик Анастасія Миколаївна, юристка, незалежна консультантка з цифрової безпеки, керівниця Apetyk consult, членкиня правління, керівниця з стратегічного розвитку ГО «Мін3мін» (Тема 1.1, Тема 1.5). **Дьякова Анастасія Дмитрівна,** голова правління #stop_sextинг (Тема 1.1, Тема 1.3, Тема 2.1.3). **Ковальова Олена Володимирівна,** кандидатка юридичних наук, старша наукова співробітниця, доцентка, професорка кафедри адміністративної діяльності поліції Одеського державного університету внутрішніх справ (Тема 1.7, Тема 1.9, Тема 1.10, Тема 1.12, Тема 2.1.3, Тема 2.1.4). **Козлова Анна Георгіївна,** докторка філософії у галузі психології; доцентка кафедри психології та педагогіки професійної освіти факультету лінгвістики та соціальних комунікацій Національного авіаційного університету (Тема 1.11). **Манжай Олександр Володимирович,** кандидат юридичних наук, професор, підполковник поліції, завідувач кафедри протидії кіберзлочинності ННІ №4 Харківського національного університету внутрішніх справ (Тема 1.4, Тема 1.6, Тема 1.8, Тема 2.1.1, Тема 2.2.1, Тема 2.3.1, Тема 2.3.2). **Мердова Ольга Миколаївна,** кандидатка юридичних наук, доцентка, завідувачка кафедри адміністративно-правових дисциплін факультету №2 Донецького державного університету внутрішніх справ (Тема 1.1, Тема 1.2, Тема 2.1.2.). **Мілорадова Наталія Едуардівна,** докторка психологічних наук, професорка кафедри педагогіки та психології ННІ №3 Харківського національного університету внутрішніх справ (Тема 1.1, Тема 1.2, Тема 1.3, Тема 1.11, Тема 2.1.2.). **Пашко Наталія Олександрівна,** психологиня, психотерапевтка, координаторка по роботі з дітьми та підлітками ГО «Інститут психології здоров'я», модераторка дивізіону ювенальної психології (Тема 1.3, Тема 1.11). **Юртаєва Ксенія Володимирівна,** кандидатка юридичних наук, доцентка, LL.M, доцентка кафедри кримінального права і кримінології ННІ №1 Харківського національного університету внутрішніх справ (Тема 2.2.2). **Філоненко Василь Іванович,** тренер-методолог Громадської організації #stop_sextинг (Тема 1.1, Тема 1.2, Тема 2.1.3).

РЕЦЕНЗЕНТИ:

Богдан Василь Володимирович, начальник управління ювенальної превенції Департаменту превентивної діяльності Національної поліції України, полковник поліції.

Вітвіцький Руслан Олегович, т.в.о. заступника начальника 4-го відділу 1-го управління Департаменту кіберполіції Національної поліції України, майор поліції.

Корнієнко Максим Вікторович, проректор Одеського державного університету внутрішніх справ, д.ю.н., професор, полковник поліції.

ЗАГАЛЬНА РЕДАКЦІЯ:

Журавель Тетяна Василівна, кандидатка педагогічних наук, виконавча директорка Громадської організації «Всеукраїнський громадський центр "Волонтер"».

Ковальова Олена Володимирівна, кандидатка юридичних наук, старша наукова співробітинця, доцентка, професорка кафедри адміністративної діяльності поліції Одеського державного університету внутрішніх справ.

КООРДИНАЦІЯ РОЗРОБЛЕННЯ ПРОГРАМИ:

Янковець Вікторія Вікторівна, магістерка соціальної роботи, координаторка проєктів Громадської організації «Всеукраїнський громадський центр "Волонтер"».

Навчально-методичний посібник призначений для викладачів, які здійснюють професійне навчання поліцейських, та спрямований на посилення навчально-методичного інструментарію підготовки поліцейських підрозділів превентивної діяльності, слідства та дізнання, кіберполіцейських з питань забезпечення безпеки дітей у кіберпросторі. Навчально-методичний посібник може використовуватись для проведення навчальних занять під час первинної професійної підготовки поліцейських, підготовки у закладах вищої освіти зі специфічними умовами навчання, післядипломної освіти та службової підготовки поліцейських.

Диайн і верстка: ФОП Буря О.Д.
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавництва ДК №4749.

Підписано до друку: 06.12.2024. Формат: 45×64/16.
Ум. друк. арк.: 42,9. Обл.-вид. арк.: 41,7.
Папір офсетний. Гарнітура: Raleway.
Друк офсетний. Наклад 500.