**Тема: «Безпечний інтернет»**

**Віртуальний світ і особистість:** права, безпека, етика

Усім відомий метафоричний вислів: людина — це світ. Утім, точніше всетаки треба сказати: не світ, а світи. Тому, що людина перебуває принаймні у світі

реальному і світі власному (суб'єктному, особистісному). Також — у світі

художньому, створеному митцями, — світі кіно, театру, літератури, музики. Цей

світ постає як світ віртуальний (лат. virtualis — можливий, імовірний). І так

було ще донедавна — допоки не з'явився Інтернет і допоки інформаційні

технології не створили гігантський цифровий світ (кіберпростір) — віртуальну

реальність. У ній сучасна людина проводить дедалі більше часу.

Для багатьох віртуальний світ став аналогом світу реального, його замінником.

Як у реальному, так і у віртуальному світі життя людини поділяється на

* публічне (лат. publicus — суспільний, громадський), тобто відкрите для інших,
* приватне (лат. privatus — особистий, несуспільний). І в реальному, і у

віртуальному світі діє право людини на приватність, або на приватне життя, на

приватну сферу.

**Приватність** — це недоторканність приватного життя особи, невтручання в

її особисту сферу. Як фундаментальне право людини, право на приватність

закріплене в міжнародних і національних правових актах. Поряд із поняттям

«приватність», «приватне життя», у них уживаються синонімічні терміни

**«конфіденційність»** (лат. confidentia — довір’я) для позначення того, що не

підлягає розголошенню, «таємниця особистого життя», «недоторканність

приватного життя» та деякі інші.

Про те, яким має бути право на приватність у цифрову епоху, сказано в

спеціальній резолюції Генеральної Асамблеї ООН від 2013 року. Основна думка

цього документа звучить так: «Ті ж права, що люди мають у офлайн- режимі,

також повинні бути захищені онлайн, серед них і право на приватність».

**Кіберзлочини** — це різні види й форми злочинів, які здійснюються в мережі за

допомогою комп’ютера. До кіберзлочинів належать порушення авторського

права, шахрайство (несправжні інтернет-аукціони, онлайн-магазини, сайти тощо), заволодіння персональною інформацією користувачів для викрадення

грошових коштів, створення й розповсюдження вірусів і шкідливого програмного забезпечення, протиправний контент, тобто контент, який пропагує тероризм,

екстремізм, наркоманію, порнографію, насильство.

Останнім часом в соціальних мережах серед неповнолітніх користувачів набуло поширення таке явище, як **хепі слепінг** (дослівно з анг. happy slapping — радісне побиття) — насильство задля розваги. Через розміщення в мережі відеозаписів (відеороликів) демонструється реальне побиття, приниження, учасниками яких виступають неповнолітні.

Ваша безпека в Інтернеті великою мірою залежить від розважливості,

культури поведінки в соцмережах, етики спілкування. Не забувайте про це. Як і

про те, що ви ніколи достеменно не знаєте, де може з’явитися ваша інформація і

яку роль вона відіграє у вашому особистому житті, майбутній кар’єрі. Тому

розміщуйте в мережі ту інформацію, за яку вам пізніше не доведеться червоніти.

***Варто знати:***

Як зробити користування Інтернетом безпечним для себе:

1. Вибираючи соціальну мережу для спілкування, уважно ознайомтеся з її

політикою конфіденційності. Пам’ятайте, що соцмережі збирають про своїх

користувачів дані, які можуть бути використані, наприклад, для таргетованої

реклами.

2. Обмежуйтеся кількома соціальними мережами, насамперед тими, які не

заборонені в Україні та які гарантують вам безпеку. Маючи менше акаунтів,

вам легше буде контролювати інформацію і власні дані. У разі вибору кількох

соцмереж, логіни на кожен акаунт мають бути різними, а паролі – складними й

не містити персональних даних.

3. Заповнюючи профіль у мережі, обов’язково прочитайте відповідну інструкцію.

При цьому особливу увагу звертайте на налаштування приватності, зокрема

щодо доступу до вашої інформації.

4. Спілкуючись (публікуючись) у мережі, уникайте конкретики щодо ваших

особистих даних, використовуйте загальні формулювання.

5. Будьте обережні з розміщенням фотографій, адже вони можуть видавати ваші

дані.

6. Розвивайте в собі здоровий скептицизм щодо інформації в соцмережах, не

піддавайтеся на провокації неадекватних користувачів. Не втрачайте пильності.

***Інформаційний аркуш***

**Як безпечно слухати і завантажувати музику та як уникнути небезпеки, граючи в онлайн ігри.**

Зробіть відповідні висновки (письмово) і представте їх на обговорення групи.

 Музика – одна з ваших найулюбленіших розваг у вільний час. Не забудьте про правила безпеки, коли ви працюєте з музичними файлами в Інтернеті:

- завжди читайте інформацію, написану в оголошенням дрібним шрифтом, перш ніж програти чи завантажити якусь мелодію чи рингтон;

- перш ніж завантажити пісню, прочитайте відгуки інших користувачів;

- якщо ви використовуєте якісь програми обміну файлами, переконайтесь, що вони встановлені вірно і не дозволяють стороннім особам отримувати доступ до всіх файлів вашого комп’ютера;

- поважайте авторське право. Якщо автор пісні не виклав її на своєму офіційному сайті для вільного завантажування, ви можете опинитися у категорії порушників авторських прав.

 Ігри бувають найрізноманітнішими – від коротких і простих, до складних, у яких беруть участь багато гравців. Усі вони дуже різні, але якою б гра не була і на чому б ви не грали (комп’ютер, телефон, ігрова консоль), правила безпеки залишаються однаковими:

- вивчіть спеціальну мову ігор;

- якщо у процесі гри хтось почне використовувати нецензурні вирази у вашу адресу, ви можете зробити скріншот і надіслати скаргу адміністрації сайту, використавши скріншот як доказ;

- якщо гра несе для вас небезпеку, повідомте дорослих.

- не забувайте про мережевий етикет. Завжди будьте ввічливими у спілкуванні;

- переконайся, що при реєстрації у грі ви не видали особистої інформації.

- прочитайте терміни гри й умови використання даних сайтів, перевірте, чи є спеціальні функції безпеки неповнолітніх;

- нехай ваші батьки знають ваш псевдонім, як перевірити ваш онлайн акаунт на предмет безпеки, якщо раптом щось піде не так;

- встановіть часові обмеження для себе. Використайте, наприклад, будильник у мобільному телефоні, щоб слідкувати за часом.

Для завершення теми:

 Що таке соціальні мережі ?

 Як ви розумієте значення слів «Ті ж права, що люди мають у офлайнрежимі, також повинні бути захищені онлайн» ?

 Які основні види масових комунікацій в інтернет-середовищі?

– Наведіть приклади ризиків, які несуть неконтрольовані обсяги інформації в

Інтернеті.

– Порівняйте поняття «віртуальний світ» та «кіберпростір».

 Проаналізуйте власну поведінку як відповідального користувача соцмереж.

Виправте недоліки, якщо виявите загрози чи ризики порушення вашої

приватності та безпеки.

 Підготуйте повідомлення «Можливості Інтернету поза соціальними

мережами».

Завдання: Заповніть таблицю.

|  |  |  |
| --- | --- | --- |
| **№** | **Фактор користування Інтернетом** | **Оцінка з точки зору безпеки і доцільності** |
| 1 | Інтернет – безмежний простір для отримання інформації. |  |
| 2 | В Інтернеті можна скачувати і розміщувати ігри , фотографії, фільми, музику, відео. |  |
| 3 | Через Інтернет ми можемо замовити і оплатити різні товари. |  |
| 4 | В соціальних мережах можна вільно спілкуватися, знайомитися без обмежень. |  |
| 5 | Інтернет містить велику кількість реклами. |  |
| 6 | Інтернет – простір, де ти можеш бути ким завгодно. |  |
| 7 | Віртуальний світ часто буває небезпечним. |  |