

Завдання для самостійної роботи

1. Опрацювати методику «Особистісна шкала прояву тривоги» Дж. Тейлора.

Інструкція: «Вам пропонується 60 тверджень. Прочитайте кожне твердження і вирішіть, вірно, воно чи не вірно по відношенню до вас. Не витрачайте час на роздуми. Якщо ви згодні з твердженням поруч з його номером поставте «+» (так), якщо ні то поставте знак «-» (немає) ».

2. Опрацювати тест на тривожність Спілбергера – Ханіна. (за електронним посиланням <http://studentam.net.ua/content/view/10952/86/>)

3. Опрацювати матеріал за підручником Варій М.Й. Психологія особистості: навч. посібник / М.Й. Варій. – К.: Центр учбової літератури, 2008. – 178-187с.

Приходькіна Н.О.

Тема: Медіабезпека особистості: теоретичний аспект

***Ключові поняття теми:** інформація, медіа, медіаосвіта, медіабезпека, кібербезпека, кібербулінг, булінг, грумінг, кібершахрайство.*

Використана та рекомендована література:

1. Безпека інформації: навч. посіб. [Електронний ресурс] / Інститут масової інформації. – Режим доступу до посіб.: <http://imi.org.ua/bezpeka/spravochnik-po-bezopasnosti> (Назва з екрану).

2. Концепція впровадження медіаосвіти в Україні [Електронний ресурс]. - Режим доступу : http://osvita.mediasapiens.ua/mediaprosvita/mediaosvita/kontseptsiya_vprovadzhennya_mediaosviti_v_ukraini/

3. Медіаграмотність та критичне мислення на уроках суспільствознавства: посібник для вчителя / Т. Бакка, О. Бурім, О. Волошенюк, Р. Євтушенко, Т. Мелешенко, О. Мокрогуз; За ред. В. Іванова, О. Волошенюк. – К.: ЦВП, АУП, 2016. – 243 с.

4. Медіаосвіта та медіаграмотність: підручник для студентів педагогічних коледжів / Ред.-упор. В. Ф. Іванов, О. В. Волошенюк; За науковою редакцією В. В. Різуна. — Київ: Центр Вільної Преси, 2014. — 431 с.

5. Найдьорова Л. Кібер-булінг або агресія в інтернеті: способи розпізнання і захист дитини / Л. Найдьорова // Методичні рекомендації / Серія: На допомогу вчителю. Вип. 4. – К., 2011. – 34 с.

6. Фёдоров А. В. Медиаобразование и медиаграмотность. Учебно-пособие для вузов / А.В. Фёдоров. - Таганрог: Изд-во Кучма, 2004. - 340 с.

7. Livingstone S. Intheirownwords: whatbotherschildrenonline? [Елек-

тронный ресурс] / S. Livingstone, L. Kirwil, C. Ponte & E. Staksrud // EU KidsOnline, London School of Economics & Political Science, London, UK. — 2013c. — Режим доступа : <http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/Home.aspx>.

Матеріал до теми

Епоха інформаційного суспільства характеризується величезними інформаційними потоками. Інформація є ресурсом, який прямо впливає на економічне, соціальне, політичне і культурний розвиток суспільства. З розвитком мережі Інтернет і медіа каналів на перше місце вченими висувається питання оцінки якості інформації, яку отримують користувачі - споживачі інтернет-контенту, в тому числі, підлітки. Не існує універсальних комплексних рішень, які могли б забезпечити аудиторію тільки якісним контентом, або програмних засобів, здатних відрізнити фейкові новини (fakenews). У даному контексті актуальною є проблема вивчення можливостей медіаосвіти - виховання культури споживання інформаційних потоків, сприйняття інформації як продукту людської діяльності.

Чи зможемо протистояти інформаційному шуму, осмислювати і направляти в правильне русло потік інформації через соціальні мережі, відсіювати «фейкові» новини, настільки ми впораємося з сучасними викликами інформаційного суспільства - це ті виклики, з якими стикається користувач, як окрема особистість, і суспільство - як група споживачів інформації. Окремим завданням, крім перерахованих, є можливість навчання користувачів мережі Інтернет, у яких не виходить обробляти та верифікувати отриману інформацію в режимі реального часу.

Проблема медіабезпеки особистості має широкий контекст і пов'язана з предметом досліджень багатьох наук - від соціо-комунікативних до психолого-педагогічних. У системному взаємозв'язку «медіа», «особистість», «безпека», проблема медіабезпеки особистості має вивчатись як комплексна, міждисциплінарна проблема.

Медіа - це широке поняття, що включає в себе всю сукупність інформаційних засобів і прийомів для передачі конкретному споживачеві повідомлення (друковане слово, музична композиція, радіопередача тощо) в тій чи іншій формі.

Медіа - це сукупність всіх ЗМІ. У свою чергу, ЗМІ - це спосіб перенесення інформації для мас.

Медіа різноманітні і численні, включають в себе: мас-медіа - засоби масової інформації (телебачення, періодична преса, радіо, кабельні телевізійні мережі); директ-медіа - комунікаційні системи передачі інформації (інтернет, телефон, пошта); медіа-носії - окремі носії інформації (листи, записи на аудіо- та відеоносіях, відео-, аудіо-мультимедіа-презентації); соціальні медіа - засоби комунікації груп, спільнот між собою (соціальні мережі, блоги, персональні сайти тощо).

В ЮНЕСКО під медіаосвітою розуміється «навчання теорії і практичним умінням для оволодіння сучасними засобами масової комунікації, які розглядаються як частина специфічної, автономної галузі знань у педагогічній теорії і практиці». Це частина основного права кожного громадянина будь-якої країни на свободу самовираження і отримання інформації.

Згідно з Концепцією впровадження медіаосвіти в Україні одним з основних завдань медіаосвіти є сприяння формуванню медіаімунітету особистості та здатності протистояти агресивному медіасередовищу, забезпечити психологічний комфорт у процесі споживання медіапродукції, що припускає медіаобізнаність, уміння обирати потрібну інформацію, уникати інформаційного «сміття», захищатися від потенційно шкідливої інформації з урахуванням прямих і прихованих впливів.

Наразі серед дослідників (також як при визначенні поняття медіаосвіти) немає чіткого уявлення, що розуміти під медіабезпекою. Зокрема, залишається невизначеність, вважати поняття «медіабезпека» і «інформаційна безпека» синонімами.

На нашу думку, для ефективної роботи в цій галузі варто дотримуватися поглядів, що це дещо різні поняття. Зокрема, портал Securitylab, в сферу інтересів якого входить інформаційна безпека, виділяє відразу три визначення терміну «інформаційна безпека»:

- «інформаційна безпека - стан збереження інформаційних ресурсів і захищеності законних прав особистості і суспільства в інформаційній сфері»;
- «інформаційна безпека - це процес забезпечення конфіденційності, цілісності і доступності інформації»;
- «інформаційна безпека - всі аспекти, пов'язані з визначенням, досягненням, підтриманням конфіденційності, цілісності, доступності, підзвітності, автентичності і достовірності інформації або засобів її обробки».

Всі визначення можна звести до однієї ідеї: інформаційна безпека - це безпека всередині інформаційних ресурсів, захищеність самої інформації.

При визначенні поняття медіабезпеки варто погодитися з І. А. Фатеевою, яка вважає, що медіабезпека - це один з видів безпеки сучасної людини, що живе в атмосфері постійних природних і техногенних ризиків, поряд з екологічною, дорожньою, протипожежною, хімічною та іншими видами безпеки: тобто медіабезпека - це захищеність інтересів членів суспільства від загроз, які може ховати в собі медіапростір - як засоби масової інформації (друковані та традиційні аудіовізуальні), так і засоби масової комунікації в мережі Інтернет.

Безпека - стан захищеності життєво важливих інтересів особистості, суспільства, держави від потенційно і реально існуючих загроз, або відсутність таких загроз.

Медіабезпека - це стан захищеності від недостовірної або небезпечної інформації, яка завдає шкоди здоров'ю людини, її моральності та особистісному розвитку.

Таким чином, якщо інформаційна безпека - це захищеність інформації, то медіа безпека - це захищеність користувачів від недостовірної інформації.

У широкому сенсі *медіабезпека* - це діяльність, спрямована на захист інтересів громадянського суспільства від появи і поширення недостовірної інформації в мережі Інтернет, здатної негативно вплинути на соціальні процеси. Нормативно-правова база України в цьому напрямку тільки формується. Яскравий приклад - закон «Про захист дітей від інформації, що завдає шкоди їх здоров'ю та розвитку».

У вузькому сенсі медіабезпека - це діяльність щодо забезпечення особистої безпеки користувача в мережі Інтернет, яка дозволяє йому не тільки розпізнавати недостовірну інформацію, а й використовуючи механізми саморегуляції Інтернет-середовища, запобігати поширенню шкідливої інформації.

У зв'язку з цим у руслі нашого дослідження виявляються такі питання:

1. З якими ризиками і формами шкоди можуть зіткнутися юні користувачі мережі Інтернет?
2. Яке співвідношення потенційних ризиків і фактичної шкоди, що завдається соціальними мережами юним користувачам всесвітньої павутини?
3. Хто піддається більшій небезпеці: діти з більш високим рівнем

цифрових навичок і досвіду роботи в соціальних мережах чи з більш низьким рівнем медіаграмотності?

У числі найбільш поширених ризиків, пов'язаних з небезпечним медіаконтентом, зазвичай виділяються: 1) перегляд медіа контенту сексуального характеру; 2) мережевий булінг (кібербулінг); 3) реальна особиста зустріч з віртуальним знайомим; 4) отримання Інтернет-повідомлень інтимного змісту; 5) медіаконтент негативного або асоціального характеру, що містить заклики до групової агресії, суїциду, наркоманії тощо.

Кібербулінг (cyber-bullying), віртуальний терор, отримав свою назву від англійських слів bull – бик, bully – забіяка, задирака, грубіян, насильник. Це залякування, приниження, цькування, фізичний або психологічний терор, спрямований на те, щоб викликати в іншого страх і тим самим підпорядкувати його собі. Булінг, здійснюваний у віртуальному середовищі за допомогою інтернету і мобільного телефону, називають кібербулінгом.

Кібербулінг включає цілий спектр форм поведінки, на мінімальній межі якого – жарт, що не сприймаються всерйоз, на радикальному ж – психологічний віртуальний терор, що завдає непоправної шкоди, провокує до суїцидів та смерті. Основними засобами реалізації булінгу можна вважати погрози, бойкотування/ігнорування, фізичну агресію, негативні оцінки жертви та її оточення, висміювання тощо. Явище булінгу може актуалізуватися у формі гноблення, домагання, дискримінації, нанесення шкоди, упереджень, жорстокості ставлення, переслідування, конфлікту.

Ризики поділяються на чотири типи: *тематичні, комунікаційні, електронні та споживчі.*

Тематичні ризики – це різні матеріали (тексти, картинки, аудіо, відеофайли, посилання на сторонні ресурси), що містять протизаконну, неетичну і шкідливу інформацію. Зіткнутися з ними можна практично всюди: соціальні мережі, блоги, торенти, персональні сайти, відеохостингитощо – фактично все, що зараз існує в мережі інтернет – це віртуальний простір ризику.

Такий контент може бути:

- протизаконним – наприклад, поширення наркотичних речовин через інтернет, порнографічні матеріали за участю неповнолітніх, заклики до розпалювання національної ворожнечі та екстремістських дій;

- неетичним - цей текст не заборонений до розповсюдження, але може містити інформацію, здатну образити користувачів. Подібний вміст може поширюватися обмежено (наприклад, «тільки для дорослих»);

- шкідливим - такий контент може завдати прямої шкоди психічному і фізичному здоров'ю дітей і підлітків.

Комунікаційні ризики пов'язані зі спілкуванням і міжособистісними стосунками інтернет-користувачів. Прикладами таких ризиків можуть бути: кібербулінг, незаконні контакти (наприклад, грумінг), знайомства в мережі і зустрічі з інтернет-знайомими тощо. З комунікаційними ризиками можна зіткнутися при спілкуванні в чатах, онлайн-месенджерах (ICQ, Skype, MSN та ін.), соціальних мережах, на сайтах знайомств, форумах, блогах тощо.

Дослідження показують, що кібербулінг часто супроводжується традиційним буллінгом.

Рекомендації щодо запобігання кібербулінгу:

1. Поясніть дітям, що у процесі спілкування в Інтернеті вони повинні бути доброзичливими з іншими користувачами. Ні в якому разі не варто писати різкі і образливі слова - читати їх так само неприємно, як і чути.

2. Навчіть дітей правильно реагувати на образливі слова або дії інших користувачів. Не варто спілкуватися з агресором, і тим більше намагатися відповісти йому тим же. Можливо, варто взагалі покинути даний ресурс і видалити звідти свою особисту інформацію, якщо не виходить вирішити проблему мирним шляхом. Кращий спосіб зіпсувати хулігану його витівку - відповідати йому повним ігноруванням.

3. Зверніть увагу на психологічні особливості вашої дитини. Фахівці виділяють характерні риси, типові для жертв буллінгу, вони часто бувають: полохливі, чутливі, замкнуті і сором'язливі; тривожні, невпевнені в собі, нещасні; схильні до депресії і частіше за своїх ровесників думають про самогубство; не мають жодного близького друга і успішніше спілкуються з дорослими, ніж з однолітками; якщо це хлопчики, вони можуть бути фізично слабшими за своїх ровесників.

4. Якщо у вас є інформація, що хтось із друзів або знайомих вашої дитини піддається буллінгу або кібербулінгу, то повідомте про це класному керівнику або шкільному психологу - необхідно вжити заходів щодо захисту дитини.

5. Поясніть дітям, що особиста інформація, яку вони викладають в інтернеті (домашня адреса, номер мобільного або домашнього телефону, адреса електронної пошти, особисті фотографії) може бути використана агресорами проти них. Допоможіть дитині знайти вихід із ситуації - практично на всіх форумах і сайтах є можливість заблокувати кривдника, написати скаргу модератору або адміністрації сайту, вимагати видалення сторінки.

6. Підтримуйте довірливі стосунки з вашою дитиною, щоб вчасно помітити, якщо на її адресу почне надходити агресія або загрози. Спостерігайте за її настроєм під час і після спілкування в інтернеті.

7. Переконайтеся, що образи (булінг) з мережі не перейшли в реальне життя. Якщо погрози є досить серйозними, стосуються життя або здоров'я дитини, а також членів вашої родини, то ви маєте право на захист з боку правоохоронних органів, а дії кривдників можуть потрапляти під статті дії кримінального та адміністративного кодексів про правопорушення.

8. Спілкуючись в мережі, діти можуть знайомитися, спілкуватися і додавати в «друзі» абсолютно невідомих їм в реальному житті людей. У таких ситуаціях є небезпека розголошення дитиною особистої інформації про себе і свою сім'ю. Також юний користувач ризикує зазнати образ, залякування і домаганням.

Особливо небезпечним може стати грумінг - встановлення дружніх стосунків з дитиною з метою особистої зустрічі, вступу з нею у сексуальні стосунки, шантажу і експлуатації. Такі знайомства найчастіше відбуваються в чаті, на форумі або в соціальній мережі. Спілкуючись особисто («в публічному чаті»), зловмисник, найчастіше представляючись однолітком, входить у довіру до дитини, а потім намагається дізнатися особисту інформацію (адреса, телефон тощо) і домовитися про зустріч. Іноді такі люди вимагають у дітей інформацію, якою потім можуть шантажувати дитину, наприклад, просять надіслати особисті фотографії або провокують на непристойні дії перед веб камерою.

Електронні ризики - ймовірність зіткнутися з розкраданням персональної інформації або піддатися атаці шкідливих програм. Шкідливі програми - це можливість зіткнутися з розкраданням персональної інформації, ризик піддатися вірусній атаці, онлайн-шахрайству, спам-атаці, шпигунським програмам тощо. До шкідливих програм відносяться віруси, «черви» і «троянські коні» - це комп'ютерні програми, які можуть завдати шкоди вашому сімейному комп'ютеру і даним. Вони

також можуть знижувати швидкість обміну даними з Інтернетом і навіть використовувати комп'ютер для поширення своїх копій на комп'ютери друзів, родичів, колег тощо. Захист у соціальних мережах - це завдання, яке не так давно стало актуальним для їх користувачів.

Споживчі ризики - зловживання в інтернеті правами споживача. Включають в себе: ризик придбання товару низької якості, різні підробки, контрафактну та фальсифіковану продукцію, втрату грошових коштів без придбання товару або послуги, розкрадання персональної інформації з метою кібершахрайства тощо.

Кібершахрайство - один з видів кіберзлочинів, метою якого є завдання матеріальної або іншої шкоди шляхом розкрадання особистої інформації користувача (номери банківських рахунків, паспортні дані, коди, паролі тощо).

Проблемні питання, ситуації, практичні завдання.

1. Ви завжди мріяли мати програму «Фотошоп». Нарешті ви знайшли її в Інтернеті і завантажили. Активуючи програму в комп'ютері, вже перед завершенням процесу, ви прочитали наступне повідомлення: «Для отримання безкоштовного повідомлення з кодом введіть номер вашого мобільного телефону». Що ви будете робити?

2. Перебуваючи в Інтернеті, ви відкрили дуже важливу для вас сторінку. Але комп'ютер відразу ж відреагував: «Цей файл загрожує безпеці вашого комп'ютера, містить троянську програму». Які ваші подальші дії?

3. В Інстаграмі ви познайомилися з гарним хлопцем (або привабливою дівчиною). Через деякий час «новий друг» просить зустрічі з вами на «нейтральній території». Опишіть ваші дії.

Навчальні тести

1. *Імовірність зіткнутися з розкраданням персональної інформації або піддатися атаці шкідливих програм – це:*

- a) Споживчі ризики
- b) Електронні ризики
- c) Комунікаційні ризики
- d) Тематичні ризики

2. *Різні матеріали (тексти, картинки, аудіо, відеофайли, посилання на сторонні ресурси), що містять протизаконну, неетичну і шкідливу інформацію – це:*

- a) Споживчі ризики
- b) Електронні ризики
- c) Комунікаційні ризики
- d) Тематичні ризики

3. *Зловживання в інтернеті правами споживача, що включають ризик придбання товару низької якості, різні підробки, контрафактну та фальсифіковану продукцію, втрату грошових коштів без придбання товару або послуги, розкрадання персональної інформації з метою кібершахрайства тощо – це:*

- a) Споживчі ризики
- b) Електронні ризики
- c) Комунікаційні ризики
- d) Тематичні ризики

4. *Захищеність інформації – це:*

- a) Інформаційна безпека
- b) Медіабезпека
- c) Безпека
- d) Медіаграмотність

5. *Стан захищеності життєво важливих інтересів особистості, суспільства, держави від потенційно і реально існуючих загроз, або відсутність таких загроз – це:*

- a) Інформаційна безпека
- b) Медіабезпека
- c) Безпека
- d) Медіаграмотність

6. *Стан захищеності від недостовірної або небезпечної інформації, яка завдає шкоди здоров'ю людини, її моральності та особистісному розвитку – це:*

- a) Інформаційна безпека
- b) Медіабезпека
- c) Безпека
- d) Медіаграмотність

Контрольні запитання

1. Що таке «маніпуляція в медіа»? Чи впливає вона на розвиток особистості?

2. Якщо впливає, тоді чому в попередній відповіді на запитання про маніпуляції в медіа навіть не згадується?

3. Чи використовуються мотиви підсвідомого впливу в рекламі?

15. Які основні сучасні види медіа та які їх особливості?

4. Як належить розуміти такі поняття як «медіаграмотність» та «медіаосвіта»?

5. Чи можна їх ототожнювати?

6. Чи завжди відповідає побачене в мас-медіа почутому?

7. Хіба маніпулятивний терор медіа обмежується тільки невідповідністю побаченого почутому?

8. На які ж «гачки» медіа маніпулятори ловлять необачних, довірливих та медіанеобізнаних споживачів інформації?

9. А що треба знати для того, щоб не потрапити в маніпуляційні «пазури» медіатерористів?

10. А чи можна навести хоча б декілька конкретних прикладів щодо того, як належить медіанеобізанному користувачу «вживати» продукт мас-медіа?

Завдання для самостійної роботи

Створіть презентацію (за поданим нижче переліком питань) на тему:

1. Розвиток і безпека наших дітей - пріоритетні завдання для педагогів і батьків.

2. Рекомендації батькам «Мобільний інтернет і діти різного віку».

3. Бути культурним в інтернеті новий драйв сімейного спілкування.

4. Обережно - кібер-злочинці! Небезпечні «дорослі» сайти.

5. Інтернет-залежність і як з нею боротися.

6. Комп'ютерні віруси і засоби захисту.

7. Заходи безпеки при роботі з електронної поштою.

8. Рівні і заходи щодо захисту інформації.

9. Основи безпеки мобільного (мобільного) зв'язку.

10. Інформаційна етика і право.

11. Небезпеки, з якими вони можуть зіткнутися в мережі інтернет.

12. Організація правильного пошуку відповідає своїй інформації у мережі Інтернет і ЗМІ.

Феномен «інтернет-залежності». Профілактика інтернет-залежності у дітей та підлітків. Безпечне спілкування дітей в інтернеті.