населення. Цей останній пункт найголовніший за всі, а також недостатнє фінансування з боку держави, призводять до екологічної кризи, яка в свою чергу впливає на здоров'я усього людства.

Список використаної літератури

1. Андрейцев А.К. Основи екології: Підручник. – К.: Вища шк., 2001.
2. Анісімова С., Риболова О.В., Поддашкін О.В. Екологія. – К.: Грамота, 2001.
3. Білявський Г.О., Падун ММ., Фурдуй Р.С. Основи загальної екології. – К.: Либідь, 1995.
4. Бойчук Л Д., Соломенно Е.М., Бугай О.В. Екологія і охорона навколишнього середовища: Навч. посіб. – Суми: Університетська книга, 2003.
5. Гайнріх Д., Герат М. Екологія: dtv – Atlas. Пер. з 4-го нім. вид. – К.: Знання – Прес, 2001.
6. Голубець М А., Кучерявий В.П.,Генсіру к СА. таін. Конспект лекцій з курсу «Екологія та охорона природи» (теоретичні основи загальної екології, охорони природи, комплекс природоохоронних заходів). – К.: УМКВО, 1990.
7. Дятлов А.С. Чернобыль. Как это было. Полный текст публикации: http: //pripyat.com/sm/site/fileslibrary/pripyat. Com/Dyatlov.doc
8. «Постанова Верховної Ради України про основні напрями державної політики України у галузі охорони довкілля, використання природних ресурсів та забезпечення екологічної безпеки».

ВПЛИВ СОЦІАЛЬНИХ МЕРЕЖ НА БЕЗПЕКУ ЖИТТЯ У ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ ПЕДАГОГА

Ярослав Т.О.
м. Полтава

Анотація. *У статті окреслені основні ризики перебування педагогів в соціальних мережах. Показана необхідність навчання людей безпечної поведінки у віртуальному світі. Акцентується увага на формуванні професійної інформаційної культури педагогів.*

Ключові слова: *інформаційна культура, безпека, соціальні мережі, віртуальний простір, соціалізація особистості, кібербезпека.*

В Концепції нової української школи серед ключових компетентностей, які має формувати сучасна освіта, зазначено: «Інформаційно-цифрова компетентність передбачає впевнене, а водночас критичне застосування інформаційно-комунікаційних технологій (ІКТ) для створення, пошуку, обробки, обміну інформацією на роботі, в публічному просторі та приватному спілкуванні. Інформаційна й медіаграмотність, основи програмування, алгоритмічне мислення, робота з базами даних, навички безпеки в Інтернеті та кібербезпеці. Розуміння етики роботи з інформацією (авторське право, інтелектуальна власність тощо).»

Розвиток соціальних мереж сприяє тому, що їх використання вчителями збільшується. Інтернет став паралельною реальністю: спілкування, обмін досвідом та новинами, безліч цікавої, корисної інформації. Створення в соціальних мережах своїх профілів, з фотографіями, музикою, роликами, фільмами, інформацією має декілька сторін. З одного боку, педагоги як всі користувачі інтернет мереж, формують свій власний простір спілкування, використовуючи соціальні мережі як найлегший спосіб вийти на контакт з будь-якою людиною, в тому числі з учнями та батьками. З іншого боку, виникають реальні небезпеки використання викладеної інформації проти педагогічних працівників, проявам булінгу, сталінгу та іншого. Тому саме проблема правильної, безпечної поведінки в мережах дуже актуальна в сучасних умовах і

потребує детального вивчення.

В наукових дослідженнях, які проводяться в Україні, традиційно використовується поняття ІКТ-компетентності, яке за більшістю основних ознак збігається з прийнятим в країнах Європи поняттям цифрової компетентності. Проте, «цифрова компетентність – це не тільки сума загальнокористувацьких і професійних знань і умінь, які представлені в різних моделях ІКТ-компетентності, а й установка на ефективну діяльність і особисте ставлення до неї, засноване на почутті відповідальності». Таким чином, до знань про комп'ютерні пристрої і мережі та вмінь їх використовувати, крім ставлення і мотивації до використання ІКТ в понятті «цифрова компетентність» додається ще й відповідальність за те, що кожен використовує зі світу цифрових технологій і пристроїв та за публікацію власних дописів при спілкуванні. З цим поняттям тісно пов'язане розуміння прав і обов'язків громадянина цифрового світу.

В 2015-2016 роках співробітниками відділу технологій відкритого навчального середовища ІІТЗН НАПН України в рамках виконання теми «Формування інформаційноосвітнього середовища навчання старшокласників на основі технологій електронних соціальних мереж» було проведене опитування щодо виявлення обізнаності вчителів середніх загальноосвітніх шкіл з питань безпечного і відповідального використання Інтернету, в якому взяли участь 187 вчителів з різних за кількістю населення міст і сіл України

Соціальними електронними мережами в професійній діяльності користуються тільки 66,8% вчителів з числа опитаних

Кількість вчителів, які активно користуються соціальними мережами для роботи, серед мешканців малих міст і сіл (до 100 000 жителів) та великих міст (від 100000 жителів до більше 1 млн.) приблизно однакова. Цікавим є факт, що і серед вчителів-жителів малих міст/сіл і великих міст по 34% тих, хто не використовує соціальні мережі, хоча серед вчителів малих міст і сіл значно більше тих, хто не має постійного доступу до Інтернету .

На основі даних опитування можна припустити, що вчителі великих міст більш обізнані з потенційними ризиками і загрозами комунікаційних сервісів Інтернету. Вони, хоча і мають значно кращий доступ до всесвітньої мережі, проте не використовують її в навчальній діяльності і 52% з тих, хто не використовує Інтернет, серед причин окремо відмітили відповідь, що вони вважають, що «соціальні мережі несуть більше шкоди, ніж користі», і окремі респонденти зазначили серед причин те, що соціальні мережі «не контролюються», «невідомо з ким іде бесіда», або додали «розділяю спілкування в соціальних мережах та роботу з учнями». На мою думку, такий розподіл спілкування має свої переваги. Багато учнів, батьків мають бажання спілкуватись з педагогами в соціальних мережах. Найкращим для такого спілкування є створення педагогом окремих груп з визначеною цільовою аудиторією. Наприклад, «Група школи №20», або «Дитячо-юнацький клуб «Юний патріот» тощо. В функціонуванні таких груп є можливість контролю та модерації інформації, яка публікується.

З числа опитаних вчителів, хто використовує соціальні мережі в навчальній діяльності, лише 15% навчають, як налаштовувати конфіденційність облікового запису при реєстрації в соціальних мережах, а тільки 0,8% визнали, що укладають з учнями угоди щодо їх відповідальності за те, як вони використовують мережу Інтернет. І в даному напрямку також важливо, щоб педагог брав відповідальність за свої особисті сторінки в соціальних мережах. Ні в якому разі не можна забувати про те, що має існувати певна різниця між дописами приватної особи Марійки Петренко і інформацією зі сторінки педагогині Марії Іванівни Петренко. Технічно це дуже легко зробити навіть в рамках одного профілю, якщо користуватись налаштуваннями приватності. Інший доступний та легкий варіант – використовувати різні соціальні мережі для спілкування з різними людьми.

Слід зазначити, що найбільше в соціальних мережах вчителі спілкуються з колегами. Педагогічні он-лайн наради відбуваються щодня на сторінках «Фейсбук», наприклад. Потрібно пам’ятати про те, що всі наші дописи формують думу про

педагогів, і не завжди вона позитивна. На жаль, дуже часто подвійна мораль суспільства щодо педагогічних працівників формує образ неіснуючої в природі людини, такого собі педагогічного супермена з моральними якостями з минулого сторіччя. І це дуже негативно може впливати на якість життя і безпеку педагогів.

Як і будь-які інші користувачі соціальних мереж, педагоги мають загрозу зіштовхнутись з величезною кількістю інтернет-пасток. Тому є необхідність ознайомитись з можливими варіантами таких подій.

Перш за все, важливо знати як захистити свої особисті дані. Особливо потрібно звернути увагу на дії у випадку фішинг-атаки. Фішинг – один з видів шахрайства, спрямований на викрадення цінних особистих даних користувача, таких як номери кредитних карток, паролі, дані про банківські рахунки і т.д.

Шахраї можуть розсилати безліч повідомлень, які відправлені ніби надійними веб-вузлами (наприклад, від банку) і містять запит особистих даних.

Шахраї постійно вдосконалюють свої фішинг-повідомлення і вікна, що спливають. Вони часто використовують офіційні емблеми реальних організацій та інші дані, отриманні зі справжніх веб-вузлів. Як розпізнати шахрайське повідомлення електронної пошти?

Ось кілька прикладів фраз, що часто використовуються при проведенні фішинг-атак:

«Підтвердіть свій обліковий запис». Представники компаній не повинні робити запит по електронній пошті про паролі, імена користувачів, номери соціального страхування та іншу особисту інформацію. Отримавши повідомлення від корпорації Microsoft з проханням оновити інформацію про кредитну картку, не відповідайте – це шахрайське повідомлення;

«Якщо ви не дасте відповідь протягом 48 годин, ваш обліковий запис буде заблокований». Такі повідомлення викликають відчуття терміновості, щоб змусити людину відповісти не роздумуючи;

«Клацніть на посилання, наведене нижче, щоб отримати доступ до свого облікового запису». Посилання, за якими просять перейти, можуть бути повністю або частково містити реальне ім'я компанії або бути повністю замаскованими. Вони ведуть на інший веб-вузол (як правило, шахрайський).

Фішинг-повідомлення зазвичай розсилаються масово і не містять ані імені, ані прізвища отримувача.

Дії у випадку фішинг-атаки:

1. повідомте компанію, чиє ім'я було використано. Для цього створіть нове повідомлення у вашій поштовій скриньці, вкладіть у нього шахрайське повідомлення і відправте на адреси відповідних організацій;

2. терміново змініть паролі для всіх облікових записів, якими ви користуєтесь у мережі;

3. регулярно перевіряйте стан своїх рахунків;

4. встановіть на свій комп’ютер антивірусні та антишпигунські програми, постійно їх оновлюйте.

Соціальні мережі. Соціальні мережі сприяють вашій творчості, дозволяють постійно контактувати з друзями, надають багато можливостей – обмінюватися і переглядати відео, фото, слухати музику. І все це в одному місці. Але як уникнути небезпек і отримати користь і задоволення від відвідування соціальних мереж?

Фотографії і фільми – важлива частина мережевого простору. Завжди гарно подумайте, перш ніж завантажити свої фотографії чи відео. Зображення залишаються на сайтах надовго (інколи навіть після того, як ви їх видалили). Вони можуть бути скопійовані, відредаговані і використані де завгодно. Подумайте, чи хочете ви цього. Пам’ятайте, коли ви викладаєте щось у мережі, це стає доступним мільйонам людей в світі. Про що ви маєте подумати у першу чергу, коли оновлюєте свої сторінки у соціальних мережах? Про власну безпеку. Захистіть сторінки налаштуваннями приватності – так ви зможете контролювати тих, хто має доступ до вашої інформації.

Персональний профіль. Це джерело інформації про вас. Додавання деталей – цікавий і веселий процес, але краще утриматися від додавання деякої інформації. Дату народження, адресу, номер мобільного краще не публікувати.

Мільйони людей в усьому світі спілкуються у соціальних мережах. Переконайтесь, що ніхто не має доступу до персональних налаштувань ваших сторінок і сайтів.

І ще декілька порад:

- частіше перевіряйте персональні налаштування ваших сторінок, щоб захистити себе від небажаних контактів;

- попросіть друзів і членів родини повідомити вам, якщо вони помітили, що ви розмістили надто багато особистої інформації або неналежні фото, відео. Зі сторони це може бути більш помітно. Зберігайте паролі у таємниці;

- поважайте себе та інших у мережі;

Пам'ятайте, що кіберзалякування і погрози з мережі неприпустимі! На це обов'язкового необхідно реагувати:

- повідомити адміністраторам сайту;

- зберегти повідомлення-погрозу як доказ;

Спілкування он-лайн. Розмови з друзями завжди дозволять вам дізнатися останні новини. Електронна пошта, Skype – що вам більше до вподоби?

Ваше ім'я в сервісах для он-лайн спілкування має легко запам'ятовуватися, але це не повинно бути вашим реальним, повним іменем.

Повідомлення. Ви колись отримували від друзів неочікувані файли невідомого вам змісту? Двічі подумайте, перш ніж відкрити їх, вони можуть містити віруси. Якщо не впевнені, краще перепитайте друга про них по телефону або особисто.

У своїй електронній скриньці відкривайте лише повідомлення від тих людей, яких ви знаєте і яким довіряєте. Не забувайте прочитувати тему повідомлення. Якщо тема викликає підозри і не схожа на те, про що ви могли б поговорити з друзями, не відкривайте ніякі вкладення. Це можуть бути віруси.

Chain mails – повідомлення-ланцюжки, у яких просять переслати їх десятьом друзям, а інакше відбудеться щось неприємне, жахливе. Домовтесь з друзями не пересилати подібний спам.

Чати. Вони відкриті для всіх, ви можете говорити з кожним. Якщо ви спілкуєтесь в чатах, переконайтесь, що в них є модератори – люди, які слідкують за змістом спілкування. Будьте обережними і не повідомляйте особисту інформацію. Уникайте безпосередніх контактів з невідомими партнерами по спілкуванню. Якщо ви домовились з кимось про реальну зустріч, обов'язково повідомте про це інших людей.

Пам'ятайте: щоб ви не використовували для спілкування – мобільний телефон, комп'ютер тощо – правила безпеки завжди однакові.

Підбиваючи підсумки всього, що було сказано вище, можна зробити наступні висновки: суспільство, що розвивається, потребує якомога більше інформації. Інтернет є таким джерелом швидкого пошуку, швидкого і корисного спілкування, рушійною силою прогресу. Але потрібно також постійно пам'ятати, що світ медіазасобів був і залишається продуктом. І як будь-який продукт, його потрібно споживати відповідально.

Список використаної літератури

1. Концепція нової української школи (ухвалена рішенням колегії МОН 27.10.2016), [Електронний ресурс]. – Режим доступу http://mon.gov.ua/activity/education/zagalnaserednya/ua-sch-2016/konczepcziya.html

2. Овчарук О.В. Особливості запровадження компетентісного підходу: досвідУкраїни та країн Європи / Інформаційні технології в освіті – 2009 – Вип. 4 – С. 218–226.

3. Livingstone,S., Haddon, L. (2014) EU Kids Online: Final Report. LSE, London: EU Kids Online. [Електронний ресурс]. – Режим доступу http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-

9)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf
4. Медийная и информационная грамотность: программа обучения педагогов. Институт ЮНЕСКО по информационным технологиям в образовании, —2012 [Електронний ресурс]. – Режим доступу http://iite.unesco.org/pics/publications/ru/files/3214706.pdf
5. Солдатова Г.В., Шляпников В.Н., Журина М.А. Эволюция онлайнрисков: итоги пятилетней работы Линии помощи «Дети онлайн» / Консультативная психология и психотерапия, – 2015, № 3, С.50–66 [Електронний ресурс]. – Режим доступу http://psyjournals.ru/mpj/2015/n3/soldatova.shtml
6. Солдатова Г., Зотова Е, Лебешева М., Шляпников В. Интернет: возможности, компетенции, безопасность Методическое пособие для работников системы общего образования. Часть 1, М., «Гутенберг»,— 2013, 165с [Електронний ресурс]. – Режим доступу http://detionline.com/assets/fil

ПСИХОЛОГІЧНА БЕЗПЕКА І ЯКІСТЬ ЖИТТЯ ОСОБИСТОСТІ

Козуб В. Ю.
м. Полтава

***Анотація**. У статті розглянуто проблеми забезпечення психологічної безпеки в державі. З'ясовано роль засобів масової інформації у цьому явищі. Висвітлено основні рівні психологічної безпеки населення. Запропоновано індикатори визначення психологічної безпеки особистості.*

***Ключові слова:** психологічна безпека, якість життя, засоби масової інформації, інтернет, особистість, інформаційна безпека, психологічний стан.*

Кардинальні соціально-економічні перетворення в країні, що супроводжуються крахом, кризою і реструктуризацією підприємств і не супроводжуються впровадженням у масову свідомість зрозумілих та доступних більшості населення програм реформ, позначаються на психології кожної окремої людини. Значній частині громадян доводитися усвідомлювати, що стабільність і передбачуваність свого становища залишилася в частині вже прожитого життя, що набуті знання, навички та вміння раптом стали непотрібними, що подальше життя сповнене небезпек і несподіванок, що спланувати своє життя, а тим більше життя своїх дітей, вже неможливо. І в ході цього процесу усвідомлення приходить страх, невпевненість, стрес, які вкрай негативно позначаються на психологічній безпеці особистості. Більшість людей залишилися наодинці з собою в цьому швидко змінному соціально-економічному середовищі. Якість життя населення різко впало.

Засоби масової інформації (ЗМІ), на жаль, різко негативно впливають на рівень психологічної безпеки особистості. Проведений аналіз дисфункціональної і аморальної ролі ЗМІ по відношенню до аудиторії і суспільства, і робляться такі висновки[1]:

1. На зміну просвітницько-пізнавальної, морально-виховної та художньої функцій, колишнім раніше провідними у вітчизняних ЗМІ, в даний час прийшли розважальна, наркотичного-компенсаторна і маніпулятивно-рекламна функції. Загальна дисфункціональність стає характерною для ЗМІ і масового мистецтва в Україні, що явно і неявно діє як засіб відчуження людей, невротизує і стимулює агресивні імпульси, поступово психопатологізує суспільну свідомість.

2. Тенденції у діяльності ЗМІ та в масовій культурі в основному збігаються з ціннісними орієнтаціями та інтересами індивідуалістсько-капіталістичного (в його самому вульгарному варіанті), мозаїчно-прагматичного конформістського псевдоменталітета і кримінально-мафіозного менталітетів, але суперечать ментальності найбільш духовної і морально здорової частини суспільства. Особливо це становище