УДК 373.51

Єрьоменко Анастасія Іванівна,
вчитель інформатики
Одеського ліцею «Ланжеронівський»
Одеської міської ради
м. Одеса, Україна
anastasuha.erema@ukr.net

ФОРМУВАННЯ НАВИЧОК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УЧНІВ 7-Х КЛАСІВ ЗАСОБАМИ ІНТЕРАКТИВНИХ ТЕХНОЛОГІЙ

Анотація. *Стаття присвячена проблемі визначенню навичок з інформаційної безпеки учнів 7-х класів та можливостям застосування інтерактивних технологій у формуванні таких навичок учнів. З’ясовано, що навички інформаційної безпеки є сукупністю знань, умінь і стратегій поведінки, що забезпечують безпеку та ефективність використання інформаційних технологій людиною. Це передбачає розуміння принципів безпечної поведінки в Інтернеті, здатність аналізувати інформацію, виявляти шахрайство, забезпечувати захист даних та розуміти наслідки ризикованих дій у віртуальному просторі. Виявлено, що підлітковий вік супроводжується інтенсивним процесом пошуку та знаходження нових можливостей, що може призвести до збільшення інтернет-активності. Враховуючи унікальні особливості підлітків, дуже важливо адаптувати навички інформаційної безпеки до їхніх специфічних потреб. На основі теоретичного аналізу, опитування підлітків та спостереження виокремлені навички інформаційної безпеки учнів сьомих класів: усвідомлення та управління ризиками, знання про захист особистих даних, вміння використовувати безпечні практики інформаційної безпеки, здатність критично оцінювати інформацію із цифрового середовища, соціальні навички в мережі Інтернет. Встановлено, що інтерактивні технології відіграють ключову роль у формуванні навичок інформаційної безпеки учнів. Зокрема, це – інтерактивні відеоуроки, онлайн-вікторини та тести, захоплюючі ігри та симуляції, створення блогів та відеоблогів, інтернет-квести та симулятори, а також організація вебінарів з досвідченими професіоналами. З практичного досвіду наведені приклади застосування інтерактивних технологій на уроках інформатики.*

Ключові слова: *навички інформаційної безпеки, інформаційна безпека підлітків, інтерактивні технології, рекомендації.*

Постановка проблеми. В умовах сучасних перетворень в Україні потреба у захисті персональних даних стає все більш актуальною. Зі зростанням використання технологій у різних сферах важливо захистити громадян від потенційної шкоди, спричиненої небезпечною інформацією. Це стосується не лише захисту окремих осіб, але й колективної свідомості суспільства. Стрімкий розвиток інформаційних технологій і використання тактики переконання можна спостерігати не лише під час війни, але й у повсякденних ситуаціях.

У теперішній час існує безліч потенційних небезпек, пов’язаних з використанням медіа та Інтернету. Серед усіх вікових груп підлітки особливо вразливі до негативного впливу сучасних технологій. Для сучасного школяра майже немислимо обходитися без доступу до Інтернету. Хоча технології пропонують численні переваги для навчання та соціальної взаємодії, вони також становлять загрозу для їхнього фізичного та психічного здоров’я. Крім того, постійний потік інформації через засоби масової інформації може суттєво вплинути на світогляд, цінності та поведінку людини.

Забезпечення інформаційної безпеки має вирішальне значення для загальноосвітніх шкіл, особливо для захисту персональних даних як учнів, так і персоналу. Отже, поряд з інформаційною та цифровою грамотністю, освітяни надають першочергового значення забезпеченню безпеки учнів в Інтернеті. Вони повинні передавати знання про безпечну навігацію в Інтернеті, етичну поведінку, правові аспекти та захист персональних даних. Така освіта не лише підвищує цифрову безпеку користувачів, а й сприяє фізичному та емоційному благополуччю учнів.

Аналіз наукових досліджень і публікацій. Питання ефективного викладання основ інформаційної безпеки викликало жвавий інтерес з боку дослідників. Зокрема, теоретичним засадам інформаційної безпеки сучасного суспільства, дослідженню основних загроз присвячено роботи таких дослідників та педагогів практиків: В. Богуш, Л. Гаврищак, О. Герасименко, Є. Катаєв, А. Козак, С. Попов, О. Юдін та інші.

У роботах дослідників О. Берест, В. Бондаренко, Л. Дітковської, С. Доценко, В. Ковальчук, В. Костицького, О. Сагач, Д. Столбова, О. Спіріна, Т. Підгорної та інших досліджено проблему

забезпечення інформаційної безпеки дітей і підлітків в умовах закладів освіти, а також питання підготовки майбутніх вчителів інформатики до забезпечення інформаційної безпеки у закладах освіти.

Проблему розвитку інформатичної освіти, а також питання навчання основ захисту даних розглядаються у роботах деяких дослідників, а саме таких як К. Варивода, Л. Вознюк, І. Кобзєва, Б. Оранюк, О. Топчій, А. Шастіна та інші.

Однак, незважаючи на їхній значний внесок у вирішення цього питання, ці рішення часто мають суто теоретичний характер і не мають практичного застосування у формуванні навичок інформаційної безпеки в учнів. Крім того, дослідження Дж. В. Дімпсей, Н. .П. Волкової, Т. В. Воробйової, С. Г. Литвинової, Л. Ревер та інших підкреслюють, що для більш продуктивного навчання корисним є використання інтерактивних технологій, які підвищують здатність студентів ефективніше запам'ятовувати навчальний контент.

Метою статті є виокремити та обґрунтувати навички з інформаційної безпеки учнів 7-х класів та розглянути можливості застосування інтерактивних технологій у формуванні таких навичок учнів.

Виклад основного матеріалу. Поняття «навички інформаційної безпеки» ретельно досліджувалося різними вченими, кожен з яких пропонував своє унікальне бачення, розкриваючи її багатошарову природу, що включає педагогічні, технологічні та психологічні аспекти. Ці навички поєднують у собі технічну підкованість та усвідомлений погляд на потенційні ризики, а також ментальну готовність до маневрування в цифровому світі.

На думку дослідників, під навичками інформаційної безпеки можна розуміти рівень знань, умінь і навичок, необхідних для збереження персональних даних та ефективного використання інформаційних технологій. Д. Столбов зазначає, що ці компетенції включають критичне мислення, вміння відрізняти достовірну інформацію від маніпуляцій, усвідомлення ризиків онлайн-зв'язків та обізнаність з елементарними правилами кібербезпеки [7].

Психолог М. Маар стверджує, що навички, пов'язані з інформаційною безпекою, мають психологічні виміри, такі як свідоме прийняття рішень, управління ризиками, а також самоконтроль у віртуальному світі. Це включає в себе знання власних емоцій, розвиток самоопору проти соціальних інженерів, формування навичок саморегуляції для уникнення деяких ризикованих ситуацій [8].

Поняття «навички інформаційної безпеки» аналізується з точки зору різних науковців, тому воно виявляється багатовимірним явищем, що охоплює педагогічну, технічну, психологічну перспективи. Такі вміння передбачають як технічну компетентність, так і усвідомлений підхід до ризиків та психологічну підготовку до дій у віртуальному просторі [1].

Отже, зважаючи на вище зазначене визначаємо навички інформаційної безпеки як сукупність знань, умінь і стратегій поведінки, що забезпечують безпеку та ефективність використання інформаційних технологій людиною. Це передбачає розуміння принципів безпечної поведінки в Інтернеті, здатність аналізувати інформацію, виявляти шахрайство, забезпечувати захист даних та розуміти наслідки ризикованих дій у віртуальному просторі.

Існує багато компонентів, які складають навички інформаційної безпеки і використовуються для захисту інформації та забезпечення безпеки в кібернетичному світі. В. Петрик запропонував назвати їх основні складові [5].

1. Усвідомлення ризиків. Цей аспект складається зі знань про загрози та ризики, які можуть виникнути внаслідок використання електронних засобів обробки, передачі та зберігання даних. Він містить розуміння навичок зловмисників, шахрайства та інших питань, пов'язаних з кіберзагрозами.

2. Знання про захист даних. Другий елемент – це розуміння основ та підходів до забезпечення інформаційної безпеки в цифровому середовищі. Він включає в себе такі аспекти, як знання про використання паролів, шифрування, антивірусних пакетів, резервне копіювання тощо.

3. Вміння використовувати безпечні практики. Це аспект, який передбачає схильність до використання найкращих практик інформаційної безпеки. Це передбачає створення надійних паролів, використання двофакторної автентифікації, ігнорування небезпечних посилань/вкладень в електронних листах, оновлення програмного забезпечення тощо.

4. Критичне мислення. Елемент критичного мислення передбачає здатність критично оцінювати отриману інформацію в цифровому середовищі. Це передбачає знання для виявлення брехні, шахрайства та маніпуляцій, а також для відстеження джерел інформації перед тим, як ділитися нею або використовувати її.

5. Соціальні навички. Останнє передбачає вміння добре працювати з іншими в цифровому середовищі. Це передбачає здатність обговорювати цифрові питання з батьками, вчителями та однолітками, а також дотримуватися етики онлайн-спілкування.

6. Управління ризиками. Друга частина пов'язана з аналізом ризиків та реагуванням на них. Вона також

включає здатність усвідомлювати можливі небезпеки, розробляти контрзаходи та методи боротьби з ними, а також управляти інформацією на основі рівня ризику.

Аналіз наукових джерел свідчить, що характеристики та сферу застосування навичок інформаційної безпеки можна класифікувати [4]. Нижче ми розглянемо основні категорії навичок інформаційної безпеки.

1. Технічні навички:

- захист комп'ютера та мережі (знання про те, як налаштувати антивірусне програмне забезпечення, брандмауер, захист мережевих з'єднань, встановлення антивірусної програми та інші технічні навички);
- конфіденційність даних (наприклад, шифрування даних і пароль, контрольований доступ та інші технічні заходи безпеки);

2. Організаційні навички:

- управління паролями (створення надійних паролів, їх зберігання та моніторинг);
- відновлення даних (навички періодичного резервного копіювання інформації, щоб уникнути втрати даних);
- безпечні комунікації (знання про створення захищеної мережі або шифрування трафіку, або будь-які інші заходи безпеки).

3. Поведінкові навички:

- розпізнавання шахрайства (вміння розрізняти шахрайські схеми, фішинг, фейкові повідомлення та повідомлення про атаки на інформаційну безпеку);
- безпека в Інтернеті (як визначати безпечні джерела інформації, уникати небезпечних посилань, надавати лише конкретну інформацію та інші аспекти безпеки під час перебування в Інтернеті);
- соціальна інженерія (навички розпізнавання маніпуляцій та контролю над соціальними інженерами, щоб уникнути розголошення конфіденційної інформації).

4. Етичні навички:

- навички відповідального використання технологій (навички розуміння та дотримання етичних норм та норм права щодо інформаційної безпеки);
- навички дотримання конфіденційності та протидії неправомірному доступу до конфіденційної інформації інших осіб.

Розвиток навичок інформаційної безпеки у дітей 7-го класу передбачає врахування їхніх унікальних особливостей та стан психологічного розвитку.

Аналіз наукових джерел засвідчив, що підлітковий вік супроводжується інтенсивним процесом пошуку та знаходження нових можливостей, що може призвести до збільшення інтернет-активності. Враховуючи унікальні особливості підлітків, дуже важливо адаптувати навички інформаційної безпеки до їхніх специфічних потреб:

- створення та використання надійних паролів, включаючи допомогу в процесі створення та заохочення до регулярної зміни;
- підвищення обізнаності про шкідливе програмне забезпечення та маніпуляції в інтернеті, навчання методам виявлення та захисту від вірусів і кібершахрайства;
- безпечне та відповідальне використання соціальних мереж, наголошуючи на обережному поширенні особистої інформації та дотриманні протоколів управління акаунтами;
- вміння оцінювати достовірність інформації в інтернеті, розвивати критичне мислення та перевіряти надійність джерел;
- ефективне реагування на потенційні загрози інформаційній безпеці, включаючи кібербулінг та інші форми агресії в інтернеті, а також звернення за допомогою до педагогів або батьків у разі потреби;
- почуття поваги до особистого життя та захисту персональних даних в інтернеті, підкреслюючи важливість збереження приватності та захисту особистої інформації.

Для вивчення стану комп'ютерної безпеки учнів сьомих класів (50 осіб) на основі спостереження за поведінкою учнів у віртуальному середовищі було виявлено, що:

1. Використання пошукових систем. Під час спостереження більшість виявили схильність до використання пошукових систем, в основному Google, для пошуку інформації в Інтернеті.

2. Серфінг веб-сайтів. Деякі користуються сайтами, що містять надмірну кількість рекламних банерів і шкідливих оголошень. Вони часто відвідують такі ресурси, що може становити загрозу безпеці та конфіденційності їхніх пристроїв.

3. Визначення достовірності інформації. Встановлено, що багато учнів не завжди перевіряють правдивість інформації, яку знаходять в Інтернеті. Найчастіше вони приймають за достовірну інформацію інформацію, подану за першими посиланнями в результатах пошуку, не перевіряючи додатково її джерела та достовірність.

4. Збереження шкідливого контенту. Траплялося, що діти зберігали фотографії або документи,

що містять шкідливий матеріал. Це може бути недоречний або небажаний контент, який може вплинути на їхню психологічну та духовну безпеку.

5. Встановлення шкідливого програмного забезпечення. У деяких випадках діти намагалися встановити програмне забезпечення або додатки з неофіційних джерел, що могло призвести до потенційної загрози безпеці їхніх пристроїв і даних.

6. Безпека особистої інформації. Деякі учні відзначають проблеми, пов'язані з безпекою віртуального середовища. Зокрема, деякі діти забувають пароль від свого облікового запису або не повністю виходять з нього на комп'ютерах, що використовуються іншими освітянами. Це може становити небезпеку доступу до особистої інформації та користувацьких даних.

Анкетування учнів 7 класів дало змогу виявити важливі питання щодо ставлення школярів до цінності персональних даних в Інтернеті та їхньої готовності вживати заходів щодо забезпечення конфіденційності. Учні демонструють певну обізнаність про ризики, пов'язані з розголошенням особистої інформації, і вживають заходів щодо її захисту. Більшість знають про важливість надійних паролів, антивірусного програмного забезпечення та двофакторної аутентифікації. Однак їхні знання та навички в галузі комп'ютерної безпеки потребують подальшого розвитку. Очевидно також, що вони готові робити кроки щодо захисту свого приватного життя і розуміють ризики, пов'язані з розкриттям персональних даних у соціальних мережах. Однак деякі аспекти потребують подальшого розвитку, наприклад, здатність розпізнавати фішингові атаки та вміння розпізнавати небезпечні посилання.

Отже, зважаючи на вищевикладане, виокремимо такі навички інформаційної безпеки: усвідомлення та управління ризиками, знання про захист особистих даних, вміння використовувати безпечні практики інформаційної безпеки, здатність критично оцінювати інформацію із цифрового середовища, соціальні навички в мережі Інтернет.

Аналіз наукової та фахової літератури свідчить, що для успішного формування навичок інформаційної безпеки учнів необхідно враховувати кілька чинників [2; 6]:

1. Вік та особливості розвитку учнів. Під час формування навичок інформаційної безпеки слід враховувати вік, рівень розвитку та психологічні особливості учнів. Навчальні програми та методики мають бути адаптовані до віку учнів, щоб забезпечити їхню зрозумілість та ефективність.

2.Практичні вправи та розбір конкретних ситуацій. Важливо, щоб навчання інформаційної безпеки включало практичні заняття та розбір конкретних ситуацій, які дозволяють учням застосувати свої знання в реальних ситуаціях. Це допомагає закріпити отримані навички, розвинути самостійність і стати впевненими у вирішенні проблем інформаційної безпеки.

4. Практичні приклади та сценарії. Використання реальних прикладів і сценаріїв, пов'язаних з інформаційною безпекою, допомагає учням краще зрозуміти потенційні загрози в цифровому середовищі та наслідки неправильної поведінки. Це підвищує їхню обізнаність і готовність до безпечної поведінки в Інтернеті.

5. Робота з батьками та громадськістю. Для успішного формування навичок інформаційної безпеки необхідна співпраця з батьками, викладачами та громадськістю. Просвітництво батьків про важливість інформаційної безпеки та заохочення їхньої активної участі в освітньому процесі допомагають створити сприятливе середовище для навчання навичок інформаційної безпеки.

Визначивши навички учнів 7-го класу з інформаційної безпеки, стає очевидним, що впровадження сучасних інструментів може значно підвищити їхню залученість та пильність. У цьому сценарії інтерактивні технології відіграють ключову роль. Вони не лише роблять навчальний процес цікавим, але й сприяють успішному засвоєнню навчального матеріалу.

Аналіз наукових доробок, фахової літератури та власний досвід свідчить, що інтерактивні технології відкрили для здобувачів освіти нові можливості взаємодії з навчальним матеріалом. Ці інструменти, такі як електронні презентації, відеоуроки та інтерактивні вправи [3], дозволяють не тільки отримувати доступ до інформації, але й активно співпрацювати, вирішувати проблеми та аналізувати різні аспекти інформаційної безпеки. Крім того, інтерактивні технології можна використовувати для моделювання реальних сценаріїв і проведення тренувальних вправ, озброюючи навичками виявлення та реагування на потенційні ризики, пов'язані з інформаційною безпекою. Наприклад, симуляції можуть відтворювати такі ситуації, як шахрайство, кібербулінг та поширення фейкової інформації, надаючи учням практичне розуміння цих небезпек в онлайн-світі.

Сучасні інструменти надають учням 7-х класів широкі можливості для поглиблення знань з інформаційної безпеки, що підтверджується багатьма дослідженнями та висновками експертів. Більш глибоке занурення у використання інтерактивних технологій для поглиблення розуміння цього предмету вимагає визнання різних таких інструментів. Серед них – інтерактивні відеоуроки, онлайн-вікторини та тести, захоплюючі ігри та симуляції, створення блогів та відеоблогів, інтернет-квести та симулятори,

а також організація вебінарів з досвідченими професіоналами, серед іншого. Кожен інструмент має свої унікальні характеристики та переваги, сприяючи активному залученню учнів та поглибленню їхнього розуміння концепцій інформаційної безпеки.

Крім того, інтерактивні технології можна використовувати для моделювання реальних сценаріїв і проведення тренувальних вправ, озброюючи навичками виявлення та реагування на потенційні ризики, пов'язані з інформаційною безпекою. Наприклад, симуляції можуть відтворювати такі ситуації, як шахрайство, кібербулінг та поширення фейкової інформації, надаючи учням практичне розуміння цих небезпек в онлайн-світі.

Ці сучасні інструменти надають учням 7-го класу широкі можливості для вдосконалення їхніх навичок інформаційної безпеки, що підтверджується різними дослідженнями та дослідженнями, проведеними експертами. Заглиблюючись у використання інтерактивних технологій для розвитку навичок інформаційної безпеки, необхідно визначити різні їх типи. Приклади включають інтерактивні відеоуроки, онлайн-вікторини і тести, інтерактивні ігри та симуляції, створення блогів або відеоблогів, веб-квести та онлайни тренажери, а також організацію вебінарів з експертами тощо. Кожен з цих інструментів має свої унікальні особливості та переваги, сприяючи активному залученню учнів і покращуючи їхнє розуміння інформаційної безпеки.

Щоб навчати інших про кібербезпеку в ефективний і водночас цікавий спосіб, ми виступаємо за використання практичних технологій, які допомагають засвоїти фундаментальні концепції безпеки в Інтернеті, водночас викликаючи інтерес і демонструючи актуальність у реальному світі. Інтерактивні інструменти дозволяють експериментувати та робити відкриття, розвиваючи як розуміння, так і бажання прагнути до безпеки.

Прикладами цікавих відеоуроків про інформаційну безпеку є такі платформи, як «Google: Be Internet Awesome», «Дія: Освіта» та «Netsmartz Workshop». Вони надають дітям можливість у веселій ігровій формі вивчити основи безпеки в Інтернеті. Уроки також інтерактивні. Використання подібних відео на веб-сайтах може допомогти в навчанні кібербезпеки учнів середніх і старших класів. Дітям не лише сподобається навчатися в такий спосіб, але й це може допомогти їм почати розвивати важливі навички безпеки в ранньому віці.

Такі популярні веб-сайти, як Kahoot!, Quizizz та Socrative, дають вчителям чудову можливість розробити ефективний план викладання інформаційної безпеки для учнів. Ці цікаві сервіси не лише надають зручні інструменти для створення тестів, але й пропонують простий у використанні інтерфейс для їх проведення та перевірки. Використання цих платформ у класі дозволяє вчителям застосовувати нові та цікаві методи навчання, щоб сформувати в учнів базові навички інформаційної безпеки. Ці інтерактивні інструменти сприяють активній участі учнів, роблять предмет більш цікавим і покращують навички безпеки в Інтернеті.

Доцільними в контексіт питання, що розглядається є цікаві ігри та симуляції з інформаційної безпеки, які сприяють навчанню: «Spoofy» допомагає боротися з реальними онлайн-небезпеками, «CRDF GLOBAL» формує міцні навички безпеки, а «Online Safety for Teens» пропонує симуляції, орієнтовані на молодь. Ці захоплюючі навчальні інструменти справді зацікавлюють учнів і допомагають їм краще зрозуміти кібер-ризики.

Такі сайти, як «Kidblog», «Edublogs» і «Blogger», дозволяють знаходити і використовувати уроки про захист інформації через написання блогів. На цих динамічних веб-сайтах учні можуть поділитися своїми думками про безпеку в Інтернеті та поспілкуватися з іншими. Створюючи безпечну та корисну онлайн-групу, ці місця сприяють важливому та цікавому навчанню.

Серед блогерів та експертів, які обговорюють безпеку підлітків в Інтернеті, виділяється блог «Дія: Цифрова освіта». У ньому беруть участь авторитетні фахівці з кібербезпеки та відомі в Україні медійники. Ще один корисний ресурс – «Хакер, що біжить» експерта з кібербезпеки Володимира Стирана. Також варто звернути увагу на онлайн-курс «Основи кібербезпеки для школярів». Він був створений CRDF Global в Україні спільно з «Смарт Освіта» та Technomatix. Ці джерела демонструють велику майстерність у залученні молоді. Вони розповідають про важливі теми кібербезпеки та дають практичні поради щодо безпечного користування інтернетом.

Висновки. Отже, зазначені інтерактивні технології і ресурси вчителі можуть успішно використовувати у педагогічній практиці, що сприятиме семикласникам сформувати навички інформаційної безпеки за допомогою цікавих технологій. Варто зазначити, що ключем до успіху є створення захопливої та живої атмосфери навчання. Впроваджуючи інтерактивні технології, вчитель не просто розповсюджує інформацію, а й надає учням навички, життєво необхідні для безпечного дослідження Інтернету та цифрових платформ.

Перспективи подальших розвідок вбачаємо у розробці та впровадженні навчальної програми «Безпека в інформаційному просторі».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Авер'янова, Н., & Воропаєва, Т. (2020). Інформаційна безпека України: соціально-філософські аспекти. *Молодий вчений*, (10(86)), 297-303. https://doi.org/10.32839/2304-5809/2020-10-86-61

Бондарук, І. П. (2011). Методика розвитку критичного мислення учнів у процесі навчання всесвітньої історії. *Психолого-педагогічні проблеми сільської школи: збірник наукових праць Уманського державного педагогічного університету імені Павла Тичини*, (39, частина 2), 88-95. URL: http://nbuv.gov.ua/UJRN/Ppps_2011_39%282%29__15 (дата звернення: 18.06.2023)

Кобзєва, І. М., & Бєлєніннік, О. Є. (2020). Формування у підлітків та молоді навичок безпечної поведінки в інформаційному просторі. У *Восьма міжнародна науково-методична конференція «Критичне мислення в епоху токсичного контенту»* (С. 444–448). Київ: Центр Вільної Преси, Академія української преси. URL: https://www.academia.edu/download/62475867/Zbirnyk_8_konf_202020200325-20133-18s23km.pdf#page=444 (дата звернення: 18.06.2023)

Овчарук, О. В. (2020). Цифрові інструменти підтримки середовища школи для реалізації освіти для демократичного громадянства. *Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: методологія, теорія, досвід, проблеми*, (60), 90-98. URL: https://lib.iitta.gov.ua/727694/ (дата звернення: 18.06.2023)

Петрик, В. М. (2009). Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал*, (5), 122-135.

Стешиц, І. В. (2022). Педагогічне партнерство як ключова компетентність вчителів-початківців нової української школи. *Наукові інновації та передові технології*, (8(10)). https://doi.org/10.52058/2786-5274-2022-8(10)-145-155 (дата звернення: 22.10.2023)

Столбов, Д. В. (2014). Сутність і зміст поняття Інтернет-безпеки сучасного школяра. *Науковий вісник Ужгородського національного університету: Серія: Педагогіка. Соціальна робота*, (33), 187-189. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/11555 (дата звернення: 18.06.2023)

Maar, M. C. (2013). *An examination of organizational information protection in the era of social media: A study of social network security and privacy protection* (дисертація). Capella University. URL: https://www.proquest.com/openview/e9b75bfd34260e5cb7e392214de4f100/1?pq-origsite=gscholar&cbl=18750 (дата звернення: 18.06.2023)

REFERENCES

Averianova, N., & Voropaieva, T. (2020). Informatsiina bezpeka Ukrainy: sotsialno-filosofski aspekty. Molodyi vchenyi, (10(86)), 297-303. https://doi.org/10.32839/2304-5809/2020-10-86-61

Bondaruk, I. P. (2011). Metodyka rozvytku krytychnoho myslennia uchniv u protsesi navchannia vsesvitnoi istorii. Psykholoho-pedahohichni problemy silskoi shkoly: zbirnyk naukovykh prats Umanskoho derzhavnoho pedahohichnoho universytetu imeni Pavla Tychyny, (39, chastyna 2), 88-95. URL: http://nbuv.gov.ua/UJRN/Ppps_2011_39%282%29__15 (data zvernennia: 18.06.2023)

Kobzieva, I. M., & Bielieninnik, O. Ye. (2020). Formuvannia u pidlitkiv ta molodi navychok bezpechnoi povedinky v informatsiinomu prostori. U Vosma mizhnarodna naukovo-metodychna konferentsiia «Krytychne myslennia v epokhu toksychnoho kontentu» (S. 444–448). Kyiv: Tsentr Vilnoi Presy, Akademiia ukrainskoi presy. URL: https://www.academia.edu/download/62475867/Zbirnyk_8_konf_202020200325-20133-18s23km.pdf#page=444 (data zvernennia: 18.06.2023)

Ovcharuk, O. V. (2020). Tsyfrovi instrumenty pidtrymky seredovyshcha shkoly dlia realizatsii osvity dlia demokratychnoho hromadianstva. Suchasni informatsiini tekhnolohii ta innovatsiini metodyky navchannia u pidhotovtsi fakhivtsiv: metodolohiia, teoriia, dosvid, problemy, (60), 90-98. URL: https://lib.iitta.gov.ua/727694/ (data zvernennia: 18.06.2023)

Petryk, V. M. (2009). Sutnist informatsiinoi bezpeky derzhavy, suspilstva ta osoby. Yurydychnyi zhurnal, (5), 122-135.

Steshyts, I. V. (2022). Pedahohichne partnerstvo yak kliuchova kompetentnist vchyteliv-pochatkivtsiv novoi ukrainskoi shkoly. Naukovi innovatsii ta peredovi tekhnolohii, (8(10)). https://doi.org/10.52058/2786-5274-2022-8(10)-145-155 (data zvernennia: 22.10.2023)

Stolbov, D. V. (2014). Sutnist i zmist poniattia Internet-bezpeky suchasnoho shkoliara. Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu: Seriia: Pedahohika. Sotsialna robota, (33), 187-189. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/11555 (data zvernennia: 18.06.2023)

Maar, M. C. (2013). An examination of organizational information protection in the era of social media: A study of social network security and privacy protection (dysertatsiia). Capella University. URL: https://www.proquest.com/openview/e9b75bfd34260e5cb7e392214de4f100/1?pq-origsite=gscholar&cbl=18750 (data zvernennia: 18.06.2023)

Anastasiia Yeromenko,
teacher of computer science
of Odesa Lyceum «Lanzheronivskyi»
Odesa City Council
Odesa, Ukraine
anastasuha.erema@ukr.net

FORMATION OF INFORMATION SECURITY SKILLS OF 7TH GRADE PUPILS BY MEANS OF INTERACTIVE TECHNOLOGIES

Abstract. *The article is devoted to the problem of determining the information security skills of 7th grade students and the possibilities of using interactive technologies in the formation of such students' skills. It was found that information security skills are a set of knowledge, skills and behavior strategies that ensure the safety and efficiency of the use of information technologies by a person. This involves understanding the principles of safe behavior on the Internet, the ability to analyze information, detect fraud, ensure data protection and understand the consequences of risky actions in the virtual space. It was found that adolescence is accompanied by an intensive process of searching and finding new opportunities, which can lead to an increase in Internet activity. Considering the unique characteristics of teenagers, it is very important to adapt information security skills to their specific needs. On the basis of theoretical analysis, interviews of teenagers and observation, the information security skills of seventh-graders are singled out: risk awareness and management, knowledge of personal data protection, the ability to use safe information security practices, the ability to critically evaluate information from the digital environment, social skills on the Internet. It has been established that interactive technologies play a key role in the formation of students' information security skills. In particular, these are interactive video lessons, online quizzes and tests, exciting games and simulations, creation of blogs and video blogs, Internet quests and simulations, as well as the organization of webinars with experienced professionals. Examples of the use of interactive technologies in computer science lessons are given from practical experience.*

Keywords: *information security skills, information security of adolescents, interactive technologies, recommendations.*

Дата надходження до редакції .10.12.2023

УДК 37.014.61:005.6

Круглянко Вікторія Петрівна,
методист науково-методичної лабораторії управлінської діяльності
та забезпечення якості освіти, викладач кафедри філософії освіти
КЗВО «Одеська академія неперервної освіти Одеської обласної ради»,
м. Одеса, Україна
v-1l-2a-3d-45@ukr.net

ПЕДАГОГІЧНИЙ РОЗВИТОК ЯК СТРАТЕГІЧНИЙ НАПРЯМ УДОСКОНАЛЕННЯ УПРАВЛІНСЬКИХ ПРОЦЕСІВ У ЗАКЛАДАХ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ ЗАСОБАМИ САМООЦІНЮВАННЯ

Анотація. *У статті розкрито роль професійного зростання педагогів як стратегічного напряму удосконалення управлінських процесів у закладах загальної середньої освіти. Сфокусовано увагу на результатах самооцінювання управлінських справ та їх впливі на фаховий розвиток освітян засобами самооцінювання. Запропоновано комплексний підхід до педагогічного розвитку через розроблений комплекс навчально-методичних заходів й практичні рекомендації, спрямований на підвищення професійної майстерності та результативності управлінських процесів у сфері загальної середньої освіти.*

Ключові слова: *управлінські процеси, самооцінювання, професійний розвиток педагогічних працівників.*

У контексті реформування освіти та стрімкої цифровізації управлінських процесів у закладах загальної середньої освіти, постають конкретні вимоги до рівня професійного розвитку педагогічних працівників. Якісна підготовка педагогів та постійне оновлення їх фахових компетенцій є важливою передумовою для успішного вирішення педагогічних завдань. Відтак, педагогічним працівникам відкрилися нові можливості для посилення власного професійного зростання та розвитку фахової майстерності впродовж усього життя.