ДЕПАРТАМЕНТ ОСВІТИ І НАУКИ ОДЕСЬКОЇ ОБЛАСНОЇ ДЕРЖАВНОЇ АДМІНІСТРАЦІЇ
КОМУНАЛЬНИЙ ЗАКЛАД ВИЩОЇ ОСВІТИ
«ОДЕСЬКА АКАДЕМІЯ НЕПЕРЕРВНОЇ ОСВІТИ ОДЕСЬКОЇ ОБЛАСНОЇ РАДИ»
Кафедра педагогіки та освітнього менеджменту

Кваліфікаційна робота

ПЕДАГОГІЧНІ УМОВИ ФОРМУВАННЯ НАВИЧОК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УЧНІВ 7-Х КЛАСІВ ЗАКЛАДІВ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ ЗАСОБАМИ ІНТЕРАКТИВНИХ ТЕХНОЛОГІЙ

Pedagogical conditions for the formation of information security skills of 7th grade students of general secondary education institutions by means of interactive technologies

на здобуття ступеня вищої освіти «магістр»

Виконала: здобувачка вищої освіти
другого (магістерського) рівня
спеціальності 011 Освітні, педагогічні науки
Освітньо-професійної програми
«Педагогіка середньої освіти»
Єрьоменко Анастасія Іванівна
Науковий керівник: д. пед. наук,
професор Ягоднікова В.В.
Рецензент: доктор педагогічних наук,
професор Муковіз Олексій Павлович

Рекомендовано до захисту:
протокол засідання кафедри
педагогіки та освітнього менеджменту
№ ___ від_____
Завідувачка кафедри
_____Неля КУЗНЄЦОВА

Захищено на засіданні ЕК
протокол № ___ від_____
Оцінка_____/___/_____
(за національною шкалою, шкалою ECTS, бали)
Голова ЕК
_____Тетяна ОСИПОВА

Одеса – 2024

АНОТАЦІЯ

В роботі на основі теоретичного аналізу та емпіричного дослідження визначено й обґрунтовано педагогічні умови формування навичок інформаційної безпеки в учнів 7-х класів засобами інтерактивних технологій. Визначено навички інформаційної безпеки в залежності від особливостей їх формування в учнів даного віку: усвідомлення та управління ризиками, знання про захист особистих даних, вміння використовувати безпечні практики інформаційної безпеки, здатність критичної оцінки, соціальні навички в мережі Інтернет. Виявлено і розкрито можливості інтерактивних технологій навчання і виховання в ефективності формування навичок з інформаційної безпеки. Визначено і обґрунтовано педагогічні умови формування навичок інформаційної безпеки в здобувачів освіти 7-х класів засобами інтерактивних технологій. Розроблені методичні рекомендації щодо реалізації педагогічних умов формування навичок інформаційної безпеки в учнів 7-х класів засобами інтерактивних технологій.

Ключові слова: інформаційна безпека підлітків, навички інформаційної безпеки, формування навичок, педагогічні умови, засоби інтерактивних технологій.

ANNOTATION

The paper, based on theoretical analysis and empirical research, identifies and substantiates the pedagogical conditions for the formation of information security skills in 7th grade students using interactive technologies. The information security skills are defined depending on the peculiarities of their formation in students of this age: risk awareness and management, knowledge of personal data protection, ability to use safe information security practices, ability to critically evaluate, social skills on the Internet. The possibilities of interactive teaching and learning technologies in the effectiveness of information security skills development are identified and disclosed. The pedagogical conditions for the formation of information security skills in 7th grade students using interactive technologies are determined and substantiated. Methodical recommendations for the implementation of pedagogical conditions for the formation of information security skills in 7th grade students using interactive technologies have been developed.

Keywords: information security of adolescents, information security skills, skills formation, pedagogical conditions, interactive technologies.

Зміст

ВСТУП

Актуальність роботи. 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 наш 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.

Інформаційна безпека є основним питанням для закладів загальної середньої освіти, особливо коли йдеться про захист персональних даних учнів та працівників. Таким чином, за інформаційно-цифровою компетентністю вчитель дбає про безпеку учнів у мережі Інтернет, тому має навчати молоде покоління безпечній навігації та використанню інформаційних ресурсів, а також етичним і правовим принципам поведінки в Інтернеті та захисту персональних даних. Це не лише покращить загальну систему захисту користувачів у цифровому світі, але й допоможе зберегти фізичне та емоційне благополуччя учнів.

Проблеми навчання основ інформаційної безпеки зумовили активний інтерес вітчизняних та зарубіжних вчених. 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.

Незважаючи на вагомий внесок дослідників у розв’язанні означеної проблематики, вони несуть найчастіше лише теоретичний характер та не підкріплені практичним застосуванням у процесі формування навичок інформаційної безпеки учнями. До того ж в роботах О. Власій, Н. Волкової, Р. Гуревич, Ю. Колісник-Гоменюк та інших доведено, що для підвищення ефективності навчального процесу доцільно застосовувати інтерактивні технології, за допомогою яких учні можуть більш істотно запам’ятовувати навчальний матеріал. Це і стало підставою для вибору теми кваліфікаційної роботи «Педагогічні умови формування навичок інформаційної безпеки учнів 7-х класів закладів загальної середньої освіти засобами інтерактивних технологій».

Об'єкт дослідження – навички інформаційної безпеки.

Предмет дослідження – педагогічні умови формування навичок інформаційної безпеки учнів 7-х класів засобами інтерактивних технологій.

Мета дослідження – на основі теоретичного аналізу та емпіричного дослідження визначити й обґрунтувати педагогічні умови формування навичок інформаційної безпеки учнів 7-х класів засобами інтерактивних технологій та надати методичні рекомендації до їх реалізації.

Завдання дослідження.

1. Проаналізувати проблему формування навичок з інформаційної безпеки в наукових педагогічних джерелах.
2. Виявити можливості інтерактивних технологій навчання і виховання в ефективності формування навичок з інформаційної безпеки в учнів 7 класів.
3. Проведення емпіричного дослідження стану сформованості навичок інформаційної безпеки в учнів 7 класів.
4. Визначити й обґрунтувати педагогічні умови формування навичок інформаційної безпеки в учнів 7 класів засобами інтерактивних технологій.
5. Розробити методичні рекомендації щодо реалізації педагогічних умов формування навичок інформаційної безпеки в учнів 7 класів засобами інтерактивних технологій.

Методи дослідження. Теоретичний аналіз наукової літератури, присвяченій даній проблемі, анкетування про знання та практику створення та використання надійних паролів, тестування на визначення навички виявлення шкідливих програм, анкетування із запитаннями про знання та практику учнів щодо розпізнавання та уникнення онлайн-шахрайства, фішингу та кібербулінгу, анкетування за допомогою шкали Лайкерта щодо вмінь учня та його ставлення до використання соціальних мереж безпечно та відповідально, спостереження за поведінкою учнів у віртуальному середовищі, наприклад, за їхнім використанням пошукових систем, пошуком інформації в мережі або взаємодією з небезпечним вмістом, рейтингова шкала, що дозволить оцінити їхню позицію щодо кожного аспекту безпеки, анкетування, яка охоплює аспекти, як учні ставляться до надання персональних даних в Інтернеті, та які кроки вони вживають для збереження приватності, тестування для визначення середнього рівня навичок інформаційної безпеки учнів 7-х класів, а також для виявлення індивідуальних розбіжностей.

База емпіричного дослідження. Одеський ліцей «Ланжеронівський» Одеської міської ради.

Теоретичне значення одержаних результатів полягає в тому, що:

- узагальнені теоретичні засади формування навичок інформаційної безпеки;

- уточнено поняття «безпека», «інформаційна безпека», «навички інформаційної безпеки», «інтерактивні технології»;

- визначені і обґрунтовані педагогічні умови формування навичок інформаційної безпеки засобами інтерактивних технологій;

Практичне значення одержаних результатів полягає в тому, що:

- результати дослідження можуть бути використанні вчителями в педагогічній діяльності;

- розроблені методичні рекомендації для вчителів щодо реалізації педагогічних умов для формування навичок інформаційної безпеки, які можуть застосовуватись в освітньому процесі та сприяти відповідальному використанню цифрового світу серед учнів.

- авторські методики та рекомендації можуть служити підґрунтям для педагогів у розробці ефективних стратегій викладання та виховання з питань інформаційної безпеки серед учнів підліткового віку.

Апробації. Основні положення і результати роботи доповідалися на науково-практичних конференціях, зокрема: V Всеукраїнській науково-практичній конференції «Педагогічна наука і освіта у сучасному вимірі: проблеми та перспективи розвитку» та ІІІ Регіональноій науково-практичній конференції «Актуальні проблеми педагогічної науки в XXI столітті» комунального закладу вищої освіти «Одеська академія неперервної освіти Одеської обласної ради» – та опубліковані у матеріалах зазначених конференцій [17; 18].

РОЗДІЛ 1. ПРОБЛЕМА ФОРМУВАННЯ НАВИЧОК З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Аналіз ключових понять дослідження

Вивчення науково-педагогічних матеріалів показує, що розвиток навичок здобувачів освіти щодо їхньої інформаційної безпеки залишається серйозною проблемою. Використання інформаційних технологій та Інтернету ставить перед сучасним поколінням багато труднощів і проблем. Психічна нестабільність підлітків, незнання правил інформаційної безпеки, а також нерозуміння своїх компетенцій є бар'єром для розвитку необхідних навичок у цій сфері.

Таким чином, у цьому дослідженні важливо розкрити основні ідеї, на яких ґрунтується розвиток інформаційної безпеки учнів 7-х класів за допомогою інтерактивних технологій. Розглянемо основні поняття, що використовуються в дослідженні: «безпека», «інформаційна безпека», «навички інформаційної безпеки» та «інтерактивні технології».

Поняття «безпека» вивчалася різними вченими, з різних точок зору і на різних рівнях. Одним із загальновизнаних підходів є розуміння безпеки як захисту людей та їхнього оточення, що охоплює такі фактори, як економічна та політична стабільність. Б. Бузан, відомий своєю Копенгагенською школою безпекових досліджень, пропонує п'ятирівневий підхід: індивідуальний, міжособистісний, державний, регіональний і глобальний [66]. Ця перспектива визнає безпеку як багатогранну концепцію, що охоплює виміри політичної, економічної, соціальної та культурної безпеки. Оскільки технології продовжують стрімко розвиватися, концепція безпеки також розширилася, охопивши сферу інформаційних технологій.

Оскільки технології продовжують розвиватися швидкими темпами, важливість безпеки в сфері інформаційних технологій також зростає. Такі

відомі експерти, як Н. Фергюсон і Б. Шнайер, заглибилися в це поняття, визначивши його як захист інформації від несанкціонованого доступу і порушення конфіденційності даних, з особливим акцентом на забезпеченні цілісності системи і захищеності мережевих комунікацій. У світлі цього вони підкреслюють вирішальну роль розробки надійних методів шифрування та алгоритмів захисту даних [71; 84].

Безпека також має свої особливості в педагогічному розумінні цього слова. Безпечним вважається середовище, сприятливе для розвитку та навчання дітей. Так, у дослідженні Н. Коцур та К. Вариводи про безпеку в школі [28] йдеться про фізичне, емоційне та соціальне здоров'я дітей, захист їх від насильства та дискримінації, а також відповідне середовище, яке сприяє навчанню.

Багатогранність і умовний характер безпеки можна проілюструвати, проаналізувавши погляди різних науковців на неї. Її можна розглядати в соціальній, технологічній або освітній перспективі, залежно від дисципліни та філософії дослідження, що застосовується. Як зазначає В. Гайченко, безпека – це середовище, яке не становить небезпеки для життя, здоров'я та майна людини, її прав тощо [11]. В освіті метою безпеки є забезпечення середовища для здоров'я (фізичного, психічного та соціального).

Деякі інші науковці розглядають поняття «інформаційна безпека» з різних точок зору. Воно не є однозначним, оскільки різні науковці мають власні уявлення про нього. Аналіз вищезазначених поглядів показує, що інформаційна безпека є суб'єктивною і залежить від контексту дослідження..

Поняття інформаційної безпеки виходить за межі технічних заходів і охоплює також соціальні чинники. У своєму дослідженні Б. Кормич підкреслює вирішальну роль інформаційної безпеки у захисті встановлених норм і параметрів інформаційних процесів і відносин, визначених законом. Ці процеси та відносини є фундаментальними для стабільності та добробуту держави, окремих осіб та суспільства в цілому [26]. Дане визначення включає захист інформації від маніпуляцій, дезінформації та загроз національній

безпеці. Крім того, В. Петрик стверджує, що інформаційна безпека – це стан захищеності не лише особистості, а й суспільства та держави. Вона передбачає захист інформації для підтримання стабільності та безпеки всіх залучених сторін [47].

У сфері освіти концепція інформаційної безпеки зосереджується на забезпеченні людей знаннями та методами, необхідними для захисту інформації та підтримання безпеки в цифровій сфері. Такі відомі педагоги, як І. Кобзєва та О. Белінінник [24], підкреслюють, що розуміння учнями інформаційної безпеки виходить за рамки лише технічних знань, але також включає в себе критичне мислення, оцінку достовірності джерел, уникнення кібербулінгу та захист особистої інформації. Таким чином, вони підкреслюють необхідність впровадження ефективних педагогічних методів для розвитку в учнів навичок інформаційної безпеки.

Аналізуючи поняття «інформаційна безпека», звернемо увагу також на класифікацію цього поняття, яка включає розподіл його на основі різних критеріїв та аспектів [20].

1. За об’єктом захисту:

- інформаційна безпека особи – забезпечення захисту персональної інформації від несанкціонованого доступу, використання або розголошення;

- корпоративна інформаційна безпека – захист інформації організації від ризиків, що виникають внаслідок витоку, пошкодження або неправомірного використання даних;

- державна інформаційна безпека – захист інформаційної власності держави від загроз, здатних завдати шкоди національній безпеці, обороноздатності, економіці тощо.

2. За видами загроз:

- технологічні загрози – використовуються для отримання несанкціонованого доступу до інформації шляхом застосування технічних засобів і технологій, зміни, втрати або пошкодження інформації;

- соціальні загрози – зловживання довірою, маніпуляції, фішингові атаки тощо, які можуть призвести до несанкціонованого доступу до інформації.

3. За складністю заходів, що застосовуються:

- базові методи безпеки – це прості кроки, які можуть бути використані для захисту інформації. Вони включають такі речі, як використання складних кодів доступу, оновлення програмного забезпечення тощо;

- більш складні процедури безпеки, такі як шифрування, двофакторна перевірка, застосування унікальних систем безпеки тощо.

4. За сферою застосування:

- інформаційна безпека комп'ютерів, серверів та мереж;

- мобільна інформаційна безпека – захист інформації на мобільних пристроях, таких як, наприклад, смартфони, планшети та ноутбуки;

- інтернет-інформаційна безпека – захист інформації, що передається через Інтернет, наприклад, електронної пошти, соціальних мереж, онлайн-транзакцій тощо.

Поняття «навички» вивчається та аналізується різними науковцями з різних підходів та перспектив. На думку Р. М. Ганьє, навичка – це стійкий процес, що розвивається через практику і трактується як несвідома реакція на певний стимул. Деякі з рівнів навичок, визначених Ганьє, включають прості рухи, складні фізичні навички, когнітивні навички та інші [72].

На думку Д. Колба, навичка є результатом поєднання досвіду та рефлексії. Колб використовує концепцію «кола навчання», яка включає чотири етапи: досвід, спостереження та рефлексію, узагальнення та формування принципів, застосування та перевірка на практиці [76].

Французький дослідник Ж. П. Жо підкреслює, що навички з'являються в результаті постійної взаємодії з навколишнім середовищем і фактичного досвіду. На думку Жо, взаємодія з навколишнім середовищем, експериментування та вирішення проблем відіграє велику роль у розвитку навичок [67].

З цього приводу в роботах П. Лопеса [77] навички розглядаються як комплексний процес, що включає не лише знання та вміння, а й соціальні та емоційні компоненти. На його думку, навички – це серія дій, які людина виконує для того, щоб виконувати певні функції. К. Роджерс підкреслює, що розвиток навичок є питанням активності та автономії, що означає, що людина повинна мати можливість обирати свої дії та відчувати себе активною під час їх розвитку [83].

Поняття «навички інформаційної безпеки» ретельно досліджувалося різними вченими, кожен з яких пропонував своє унікальне бачення. У нашому дослідженні [18] ми заглибилися у погляди низки науковців. Коли йдеться про захист інформації, навички інформаційної безпеки передбачають володіння здатністю використовувати технічні методи та протоколи. Вони охоплюють такі завдання, як розробка надійних паролів, шифрування даних та захист мереж і систем від несанкціонованого втручання.

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 [55].

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 [78].

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].

Ми 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 [47].

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.

Розвиток навичок інформаційної безпеки у дітей 7-го класу передбачає врахування їхніх унікальних особливостей та психологічного розвитку. На цьому етапі в учнів спостерігається значне зростання самостійності та цікавості до вивчення нової інформації та технологій [32]. Процес формування навичок інформаційної безпеки у дітей цього віку має свої особливості.

Аналіз наукових джерел свідчить, що характеристики та сферу застосування навичок інформаційної безпеки можна класифікувати [43]. 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.

Озброєння учнів цими важливими навичками є вирішальним кроком у формуванні компетентної цифрової грамотності та забезпеченні їхньої безпеки в цифровому світі.

О. Овчарук у своєму дослідженні підкреслює ключові аспекти концепції, заглиблюючись у розвиток навичок інформаційної безпеки [41]. По суті, цей шлях передбачає отримання та відточування знань, навичок та вмінь для ефективного захисту особистої інформації в цифровому ландшафті. Це передбачає розуміння основних загроз, протоколів безпеки та методів захисту інформації. У сучасному суспільстві, де технології проникають у повсякденне життя, здатність підтримувати безпеку в Інтернеті та відповідально використовувати цифрові ресурси має вирішальне значення. Розвиваючи навички інформаційної безпеки, учні отримують можливість активно захищати себе в цій цифровій сфері, що постійно розвивається.

Для успішного формування навичок інформаційної безпеки необхідно враховувати кілька чинників [4; 56].

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. Активні та інтерактивні методи навчання. Використання активних та інтерактивних методів навчання сприяє активному залученню учнів до процесу навчання. Рольові ігри, групові дискусії, вправи та розбір конкретних ситуацій створюють можливості для практичного застосування навичок інформаційної безпеки та розвитку критичного мислення.

3. 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.

Переходячи від дитинства до підліткового віку, учні 7-го класу перебувають у вирішальній точці свого розвитку [45]. Вони перебувають у процесі формування своєї індивідуальної ідентичності та відточують навички критичного мислення, ставлячи під сумнів та аналізуючи інформацію.

Навчаючи їх інформаційної безпеки, дуже важливо враховувати їхні унікальні інтереси, мотивації та потреби.

У своєму дослідженні [56] О. Струтинська підкреслює той факт, що молодь дуже активна на різних платформах соціальних медіа, таких як соціальні мережі, форуми та чати. На жаль, ці платформи також можуть наражати їх на небезпечні ситуації, такі як кібербулінг, взаємодія з незнайомцями та обмін особистою інформацією. Тому дуже важливо розуміти соціальні аспекти навичок інформаційної безпеки, щоб забезпечити їхню безпеку в цифровому світі. Оскільки учні 7-го класу активно проходять цей перехідний етап, важливо спрямувати їх і забезпечити цими важливими навичками.

Учні 7-го класу активно розвивають свої когнітивні навички, включаючи міркування, увагу, пам’ять і критичне мислення [13; 19; 87].

Вивчення стадії розвитку учнів 7-го класу та її впливу на їхні навички інформаційної безпеки є дуже важливим завданням. Цей період знаменує собою час зростання і трансформації, оскільки ці учні переходять до підліткового віку не лише фізично, але й психічно, соціально та інтелектуально.

Впровадження інтерактивних методів навчання має вирішальне значення для сприяння залученню та участі учнів у навчальному процесі. Ці методи не лише допомагають розвивати аналітичні, критичні та творчі здібності учнів, але й мають виняткову перевагу – вони захоплюють і мотивують до навчання [86]. Створюючи захоплююче і стимулююче навчальне середовище, інтерактивні технології заохочують активну участь у навчальному процесі. Завдяки можливості розробляти навчальні ігри, віртуальні симуляції та інші інтерактивні вправи, ці технології забезпечують приємний і захоплений підхід до засвоєння матеріалу.

Крім того, інтерактивні технології відіграють вирішальну роль у розвитку критичного мислення та навичок розв’язання проблем серед учнів [87]. Створюючи динамічний навчальний процес, ці технології спонукають

учнів аналізувати, оцінювати та приймати рішення, сприяючи розвитку їхніх когнітивних здібностей, таких як логічне мислення, аналітичне мислення та креативність.

Використання інтерактивних технологій також сприяє соціальному розвитку учнів. Завдяки командній роботі, спілкуванню та співпраці на спеціальних платформах та інструментах учні можуть обмінюватися ідеями та вдосконалювати свої навички спілкування, співпраці та лідерства [8].

Враховуючи віхи розвитку учнів сьомого класу, інтерактивні технології можуть бути адаптовані до їхніх конкретних потреб та рівня розвитку. Таким чином, вони можуть ефективно розвивати свою незалежність і життєво важливі навички.

1.2 Аналіз можливостей інтерактивних технологій навчання і виховання

Наступним звернемо увагу на використання інтерактивних технологій, оскільки вони є цінним ресурсом для залучення учнів та створення сприятливого навчального середовища.

Вивчення «інтерактивних технологій» привернуло увагу відомих науковців та експертів у галузі педагогіки та технологій. Вивчаючи це поняття, ми можемо отримати уявлення про те, як ці технології впливають на процес навчання і допомагають у розвитку таких важливих навичок, як інформаційна безпека.

Інтерактивними технологіями навчання, на думку Н. Волкової, називають використання різних методів, інструментів і форм організації для сприяння активній взаємодії учасників навчального процесу, щоб допомогти учням досягти своїх освітніх цілей [9]. А О. Власій відмічає, що вони охоплюють різноманітні цифрові ресурси та платформи, які дають учням змогу брати активну участь у навчанні. Сприяючи взаємодії, співпраці та самостійному навчанню, ці технології забезпечують динамічний і цікавий

навчальний процес [87]. Впроваджуючи інтерактивні технології у навчання та розвиток учнів сьомого класу, педагоги можуть сприяти формуванню цінних навичок інформаційної безпеки.

Дж. Дімпсей, відомий дослідник у цій галузі, визначає інтерактивні технології як інструменти, що полегшують взаємодію з навчальним матеріалом і забезпечують негайний зворотний зв'язок [70].

Інший впливовий науковець, Л. Ревір, у своєму дослідженні [82] визначає інтерактивні технології як інструменти, що допомагають зробити навчання більш захоплюючим і сприяють активному залученню учнів до освітнього процесу.

Більше того, дослідження, проведені Дж. МакБраєн та С. Сисоєвою, демонструють великий потенціал інтерактивних технологій у підвищенні якості освіти. Вони підкреслюють їхню здатність не лише покращувати засвоєння знань, але й стимулювати зацікавленість як в учнів, так і в дорослих [52; 81].

Інтерактивні технології відкрили для здобувачів освіти нові можливості взаємодії з навчальним матеріалом. Ці інструменти, такі як електронні презентації, відеоуроки та інтерактивні вправи [25], 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.

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.

Впровадження інтерактивних відеоуроків визнано ефективним підходом до навчання інформаційної безпеки [36]. Поєднуючи відео та інтерактивні види діяльності, цей метод пропонує учням можливість покращити свій навчальний досвід за допомогою цікавих вправ та тестів під час самого уроку. Як зазначається в дослідженнях таких вчених, як Р. Майєр [80], відеоуроки – це аудіовізуальні навчальні матеріали, призначені для викладання певної теми або навички. Вони можуть включати лекції, демонстрації, графіку та інші візуальні матеріали для ефективного донесення інформації. Досліджуючи вплив візуальних та аудіо компонентів у відеоматеріалах, розглядається їхня роль у розумінні та запам'ятовуванні інформації. У цьому дослідженні дослідник О. Москаленко заглиблюється у важливе питання про те, як найкраще структурувати відеоуроки, щоб підвищити їхню ефективність як навчального інструменту. Зокрема, основна увага приділяється інтерактивним відеоурокам та їхньому потенціалу для сприяння активному залученню учнів [40].

Завдяки використанню інтерактивних відеоуроків учні мають змогу не лише засвоювати інформацію про інформаційну безпеку, а й повністю взаємодіяти з матеріалом завдяки поєднанню наочних посібників та інтерактивних завдань. Такий підхід дозволяє візуалізувати складні ідеї, полегшуючи їх сприйняття, а також надає унікальну можливість безпосередньої взаємодії в межах самого відеоуроку. Завдяки таким елементам, як підказки з питаннями та виконання завдань, цей педагогічний інструмент сприяє персоналізованому навчанню, пристосовуючи досвід до

потреб особистості та дозволяючи їй обирати власний шлях розвитку знань [36].

Для того, щоб ефективно розвивати навички інформаційної безпеки в учнів 7-го класу, важливо включити онлайн-вікторини та тести в навчальний процес. Ці інтерактивні завдання не лише оцінюють розуміння учнями ключових концепцій кібербезпеки, але й сприяють активному залученню до вивчення предмета.

Забезпечуючи негайний зворотній зв'язок і сприяючи прямій взаємодії через відповіді на запитання і виконання завдань, ці вікторини і тести слугують цінними інструментами для швидкого і об'єктивного оцінювання знань [63]. Цей підхід пропонує численні переваги для оцінювання рівня навчання, заохочення учнів та налаштування рівнів складності. Інтерактивні вікторини та тести дають змогу оцінювати результати та вносити необхідні корективи в навчальний процес.

На думку Н. Дементієвської [16], Г. Кравчук [29] та І. Кулаги [31], комп’ютерні ігри та симуляції мають величезний потенціал в академічних дослідженнях. Крім того, вони також мають практичне значення для розвитку навичок інформаційної безпеки. Ці інтерактивні середовища надають учням можливість моделювати реальні життєві сценарії, швидко реагувати на загрози та приймати обґрунтовані рішення щодо захисту своєї особистої інформації. Крім того, вони сприяють розвитку критичного мислення, аналітичних навичок та саморегуляції. Серед ключових переваг цих технологій – заохочення до активного навчання, розвиток критичного та творчого мислення, а також сприяння практичному застосуванню знань.

Захоплюючі симуляції та цифрові інтерактивні ігри є важливими компонентами у формуванні ефективних навичок інформаційної безпеки в учнів 7-го класу. Такий підхід дозволяє учням брати участь в експериментах і вирішенні проблем у контрольованому віртуальному середовищі. Їх вивченню приділяв увагу М. Смульсон [22], і ось, що він визначав. Інтерактивні ігри, незалежно від того, чи проводяться вони на комп'ютері, чи в Інтернеті,

передбачають активну участь і дозволяють гравцям впливати на хід гри. Маючи на меті занурити гравців у віртуальне середовище за допомогою різноманітних завдань і сценаріїв, ці ігри вийшли за рамки простої розваги і тепер визнані цінними освітніми інструментами, які сприяють розвитку важливих навичок. У контексті освіти інтерактивні ігри забезпечують платформу для активного залучення та участі. Поява інтерактивних ігор припадає на 1970-1980-ті роки, а сплеск їхньої популярності припадає на 2000-ні.

Видатною постаттю в галузі використання ігор в освіті є Дж. П. Гі, шанований американський педагог. Його революційна ідея включення ігор у навчання [73] відкрила нові можливості для використання ігрових елементів у навчальному процесі, що в кінцевому підсумку призвело до покращення навчання та розвитку учнів.

Симулятор – це дуже універсальний програмний інструмент, який відтворює реальні або змодельовані процеси, забезпечуючи контрольоване середовище для експериментальних досліджень. Р. С. Хоуї [74] проливає світло на його значення. Симулятори надають учням безпечне віртуальне середовище для розвитку практичних навичок, особливо в тих сферах, де реальні умови можуть бути небезпечними або недоступними.

С. Коен-Гаттон, відома британська дослідниця, що спеціалізується на ролі сучасних технологій в освіті, проливає світло на цінність включення симуляторів у навчальний процес [68]. Такі інструменти є високоефективним засобом навчання, занурюючи учнів у віртуальні сценарії та практичні експерименти з кібербезпеки. Ці інструменти варіюються від ігор, що імітують сценарії онлайн-ризиків, до симуляцій, які дозволяють учням застосувати свої нові знання. Завдяки активній участі в інтерактивних іграх та симуляціях учні отримують цінні навички та підвищують свою компетентність у предметі.

Тому ігри на комп’ютері стали неймовірно популярним способом інтерактивного навчання. Граючи, учні розвивають цінні когнітивні здібності,

такі як критичне мислення, прийняття рішень, спостережливість і логічне мислення [31].

На додаток до ігор, симулятори є ще одним видом інтерактивних технологій, які пропонують величезний навчальний потенціал. Дозволяючи учням моделювати та відтворювати сценарії реального життя у віртуальному середовищі, вони пропонують безпечний та контрольований простір для відпрацювання навичок та отримання знань [31].

На думку К. Осадчої [42] та В. Остапенко [44], веб-квести та онлайн-тренажери виявляються дуже ефективними у формуванні навичок інформаційної безпеки. Ці динамічні інструменти заохочують учнів до активної взаємодії з матеріалом, відточуючи їхні вміння знаходити та ретельно перевіряти інформацію, виявляти шкідливе програмне забезпечення та захищати свої дані. Ці технології пропонують численні переваги, такі як можливість адаптувати навчальний процес, легкий доступ до ресурсів, розвиток критичного мислення та навичок вирішення проблем.

Веб-квести – це захоплюючі віртуальні ігри, розроблені для учнів, щоб кинути виклик їхньому розумінню та здібностям за допомогою інтригуючих запитань і завдань [46]. Ці квести охоплюють різні навчальні предмети й теми, заохочуючи учнів оцінювати свої знання, отримувати корисний зворотний зв’язок і підвищувати свою успішність.

З іншого боку, онлайн-тренажери сприяють практичному навчанню, дозволяючи учням брати участь в інтерактивних завданнях, які імітують реальні життєві сценарії, моделюють процеси та вирішують проблеми в динамічному середовищі [68]. Завдяки цим динамічним інструментам навчання вони розвивають глибоке розуміння матеріалу та вдосконалюють практичні навички.

Основна перевага веб-квестів та онлайн-тренерів полягає в їхній зручності та доступності – їх можна легко інтегрувати в навчальний процес у будь-який час і в будь-якому місці [44; 68].

В основі цього методу лежить ідея, що він надихає на творче навчання та викладання кібербезпеки. Таким чином, створення блогів покращує навички самовираження учнів, розвиває їхні здібності до письма та дозволяє їм навчати інших, ділячись своїми думками та відкриттями [60].

Включення блогів або відеоблогів є важливим елементом у формуванні навичок інформаційної безпеки серед учнів 7-го класу. О. Чала відмічає цей підхід [60], адже він передбачає заохочення активної участі учнів, оскільки вони створюють власний контент, який заглиблюється в різні аспекти безпеки в Інтернеті та заохочує обмін думками. Створюючи середовище, де учні створюють блоги, вони розвивають навички критичного мислення, аналізуючи актуальні кібер-теми та події, пишучи огляди та обговорюючи власні дослідження та досвід з безпеки в Інтернеті.

Включення вебінарів, які проводять профільні фахівці, є важливим елементом у формуванні навичок інформаційної безпеки серед учнів 7-го класу. Залучаючи висококваліфікованих фахівців у сфері кібербезпеки, такий підхід забезпечує віртуальні заняття, присвячені більш глибокому вивченню тем інтернет-безпеки. Проведення вебінарів дає учням можливість отримати персоналізовані рекомендації та поради експертів, надаючи їм платформу для того, щоб ставити запитання та звертатися за порадами безпосередньо до професіоналів галузі. Це не лише спрощує передачу теоретичних знань, але й надає можливість почути розповіді та реальні приклади з перших вуст, що допомагає їм зрозуміти, як їх застосовувати на практиці [3; 35].

Однією з головних переваг включення вебінарів з експертами в навчальний процес є те, що вони дозволять учням отримати знання від провідних лідерів у сфері кібербезпеки. Це додає інформації, що подається, рівня достовірності та своєчасності. Крім того, вебінари, що проводяться молодими фахівцями та за участю медійних особистостей, вносять динамічний елемент в навчальний процес [21]. Такі вебінари не лише надають необхідні знання, але й дають цінні поради та можливість ознайомитися з практичним досвідом цих молодих експертів. Заохочуючи відкриті та доступні

дискусії, вебінари створюють сприятливе середовище для ефективного навчання.

На кінець, у дослідженнях В. Климнюка [21] та Ю. Трач [57] підкреслюється, що інтерактивні технології відіграють вирішальну роль у формуванні навичок інформаційної безпеки. Завдяки використанню мультимедійних засобів та ресурсів віртуальної реальності учні можуть не лише зрозуміти проблеми безпеки в цифровому просторі, а й емоційно долучитися до них. Ці технології надають можливість взаємодіяти з реалістичними сценаріями, здобувати знання про протоколи безпеки та розвивати практичні навички захисту від онлайн-загроз.

Висновки до розділу 1

Проаналізувавши фундаментальні поняття нашого дослідження та розглянувши унікальні аспекти формування навичок в учнів 7-го класу, ми з’ясували, що це важливий етап в осмисленні проблеми та розробці заходів, які сприятимуть формуванню навичок інформаційної безпеки засобами інтерактивних технологій. Проведений нами аналіз інтерактивних методів навчання підтверджує їх успішність у формуванні навичок інформаційної безпеки в учнів 7-х класів. Використання комп’ютерних ігор, веб-квестів, онлайн-тренажерів, мультимедійних ресурсів та віртуальної реальності ефективно залучає учнів до активного навчання, розвиває навички безпеки в цифровому середовищі та надає можливість на практиці застосувати отримані знання. Інтерактивні технології викладання та навчання пропонують величезний потенціал для ефективного розвитку навичок інформаційної безпеки серед учнів 7-х класів. Активно залучаючи учнів, ці інструменти сприяють розвитку навичок безпечного користування цифровими технологіями. Важливо ретельно оцінити ці можливості та розробити ефективні педагогічні методи, які сприятимуть підвищенню рівня знань учнів з інформаційної безпеки.

РОЗДІЛ 2. СТАН СФОРМОВАНОСТІ НАВИЧОК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УЧНІВ

2.1 Організаційно-методичні засади емпіричного дослідження стану сформованості навичок інформаційної безпеки в учнів 7 класів

У цьому розділі ми розглянемо організаційні та методичні аспекти проведення емпіричного дослідження щодо розвитку навичок інформаційної безпеки учнів 7 класу. Щоб оцінити поточний стан, ми спочатку проведемо аналіз їх навичок. Проте, перед цим розберемося з поняттям «оцінювання». Для досягнення цих цілей і результативностей процесу важливо застосовувати об'єктивні методи та методології, які сприятимуть досягненням мети.

Системи, що оцінюють стан сформованості навичок інформаційної безпеки учнів, можуть використовувати різноманітні методи, в тому числі різні методики оцінювання.

У роботі С. Цимбалюк вказано, що метод оцінювання включає в себе теоретичні та методологічні підходи до оцінювання особистості, поведінки та діяльності учасника [59]. Вибір конкретного методу залежить від особливостей системи оцінювання. Методика оцінювання – це спосіб збору, реєстрації та аналізу інформації, яка є основою для визначення оцінки. Вона передбачає використання відповідних методичних рекомендацій, які дають змогу застосовувати інструменти для збору, реєстрації та аналізу даних [59].

Для діагностики стану сформованості навичок інформаційної безпеки в учнів ми використовували специфічні методи, що включають різні форми оцінювання інформації. Для оцінки стану сформованості цих навичок використовувалися такі методи: анкетування, тестування, спостереження та рейтингові шкали. Кожен з цих методів має свої особливості, переваги та обмеження.

Згідно з дослідженням Т. Лукіної [37], анкетування – це метод збору даних, який використовується для отримання інформації від респондентів шляхом заповнення анкети або опитувальника. Цей метод дозволяє збирати інформацію від великої кількості людей одночасно і з широкого кола важливих питань.

Особливості анкет роблять їх важливим інструментом для отримання об'єктивних відповідей від респондентів. Т. Лукіна використала деякі з них у своєму дослідженні, як показано нижче [37].

1. Стандартизація. Вона гарантує, що кожному респонденту ставлять одні й ті самі запитання, що дає змогу порівнювати відповіді та об'єктивно аналізувати результати.

2. Анонімність. Анонімність опитувань дає змогу респондентам висловлювати свої думки і думки, не побоюючись порушення недоторканності приватного життя. Це сприяє отриманню більш відкритих і чесних відповідей, що робить дані більш надійними.

3. Ефективність. Анкети ефективні для одночасного збору даних від багатьох респондентів. Тому вони є важливим інструментом у великомасштабних дослідженнях, де важливий великий обсяг інформації.

4. Документація. Результати анкет легко документувати й аналізувати. Анкети дають змогу отримати структуровані дані, які легко використовувати на більш пізньому етапі.

5. Можливість порівняння. Дані, отримані від різних респондентів, можна легко порівнювати. Це дає змогу виявити закономірності та тенденції і зрозуміти, як різні групи відповідають на одні й ті самі або схожі запитання.

Огляд наукових джерел виявив різноманітні способи [37; 38] класифікації анкет залежно від різних параметрів. Для кращого розуміння цього методу розглянемо різні категорії анкетування та їхні основні властивості [37].

1. За способом заповнення анкети:

- самостійне анкетування (респонденти заповнюють анкету без присутності дослідника);

- анкетування інтерв'юером (інтерв'юер проводить інтерв'ю та фіксує відповіді респондентів).

2. За характером запитань:

- закриті запитання (респонденти обирають відповіді з набору варіантів (наприклад, «так» або «ні»));

- відкриті запитання (респонденти дають відповіді у вільній формі).

3. За метою опитування:

- дослідження знань і думок (аналіз рівня засвоєння інформації та висловлення особистих поглядів на певну тему або предмет дослідження)

- дослідження ставлення та практик (орієнтоване на вивчення учасниками опитування свого відношення, вподобань та реальних практик в розглянутій сфері.)

4. За способом розповсюдження

- онлайн-анкети (анкети заповнюються через Інтернет);

- паперові анкети (анкети розповсюджуються фізично та збираються на папері).

Однак точність відповідей в анкетах може бути обмежена, оскільки учасники можуть давати кращі або соціально прийнятні відповіді. Також важливо, щоб запитання були сформульовані чітко і зрозуміло, інакше може виникнути непорозуміння.

Отже, анкетування – один із найпоширеніших методів збору даних. У дослідженні стану навичок інформаційної безпеки учнів 7-го класу можна використати анкету для збору відомостей щодо їхніх знань, сприйняття та практичного досвіду в сфері інтернет-безпеки та використання комп'ютера. Цей метод може включати запитання, пов'язані зі створенням і управлінням паролями, виявленням потенційно небезпечного програмного забезпечення, ставленням до ризиків кібербезпеки, захист від інтернет-шахрайства, фішингу

та кібербулінгу, а також використання соціальних мереж і розкриття особистої інформації в Інтернеті.

Ще одним методом, який ми обрали для стану сформованості підготовки учасників дослідження, було тестування. У своїх роботах це питання освітлювали Л. Кухар та В. Сергієнко [33], Завдяки ньому відбувається оцінювання знань шляхом виконання стандартизованих завдань. Тести можна використовувати на різних етапах навчального процесу.

В. Бронетко відзначав, що система комп'ютерного тестування виявляється дуже зручною для оцінки знань респондентів [5]. Вона дозволяє ефективно визначити знання без необхідності витрачати час на прослуховування усних відповідей. У разі наявності комп'ютерної мережі можна організувати централізований збір і обробку результатів тестування. У порівнянні з традиційними методами контролю, численні переваги комп'ютерного тестування виявляє також Н. Голубєва [12]:

- оперативне отримання результатів та відсутність необхідності в співробітника, що проводить оцінювання, витрачати час на важку роботу з обробки результатів тестування;

- можливість індивідуалізації процесу (автономність);

- забезпечення психологічного комфорту для учнів під час тестування;

- вища оперативність;

- підвищення об’єктивності процесу оцінювання знань;

- забезпечення конфіденційності при анонімному тестуванні;

- більший інтерес учнів до тестування порівняно з традиційними методами опитування;

- можливість використання технічних засобів;

- уникнення негативного впливу на результати тестування таких факторів, як настрій і рівень кваліфікації тощо;

- універсальність, що охоплює всі етапи робочого процесу;

- контроль над великим обсягом матеріалу;

- зменшення затрат часу на 50% порівняно з традиційним опитуванням.

Натомість О. Ляшенко виділяє такі категорії тестових завдань [39]:

- вибір правильної відповіді із набору запропонованих варіантів (одного або декількох);

- введення відповіді з клавіатури (чисте або заповнене текстом поле);

- встановлення відповідності;

- визначення правильної послідовності;

- вибір фрагмента запропонованої графічної ілюстрації та інші подібні види завдань.

Досвід використання тестів для оцінювання рівня знань показує, що найважливішою проблемою є підготовка тестових завдань [84]. Тому важливо дотримуватися певних вимог до структури та змісту тестових завдань.

Враховуючи вищезазначені вимоги та принципи комп'ютерного тестування, ми розробили тестові завдання для оцінювання вміння виявляти шкідливі програми та визначення загального рівня інформаційної безпеки учнів 7 класу. Кожен тест містить від 10 до 33 питань. Одні відповіді свідчать про високий рівень знань та ефективні навички інформаційної безпеки, інші – про брак знань, неуважність або ризиковані дії. Враховуючи ці відмінності, кожному питанню було присвоєно одне із значень рівня інформаційної обізнаності: високий, достатній, задовільний, низький та незадовільний.

Третім методом для визначення сформованості навичок інформаційної безпеки обрано спостереження. Це метод збору інформації, який передбачає систематичне та об'єктивне спостереження за явищами, подіями, об'єктами або людьми з метою збору даних та отримання знань [2]. Проаналізуємо це поняття, розглянувши переваги, характеристики та категорії.

Спостереження – це ключовий метод у наукових дослідженнях і практичному аналізі, який дає змогу систематично спостерігати і реєструвати явища, події або поведінку об'єкта дослідження в режимі реального часу [53]. Оглянемо переваги використання спостереження як методу дослідження. Т. Бутинець акцентувала увагу на його цінності для збору даних, можливості

отримання об'єктивних висновків, а також на можливостях його застосування в різних наукових і практичних сферах [6].

1. Об'єктивність. Спостереження надають об'єктивну інформацію, оскільки дані збираються без впливу на об'єкт спостереження і не підлягають інтерпретації.

2. Реальний час. Цей метод особливо важливий у дослідженнях, де важлива динаміка явища, оскільки дані можна отримати в режимі реального часу.

3. Натуральність. Спостереження зазвичай проводяться в природному середовищі об'єкта, що дозволяє досліднику спостерігати за об'єктом у його природному контексті.

Спостереження як метод дослідження є складним і багатогранним. Воно передбачає уважне вивчення явищ, що досліджуються. Цей метод знаходить застосування в різних сферах, від науки до практичного застосування, що вимагає специфічних навичок і підходів. Нижче, виходячи із праць Н. Вайдич [7], ми розглянемо ключові характеристики спостереження як методу дослідження.

1. Спостереження завжди слід проводити систематично та організовано, дотримуючись заздалегідь розробленого плану.

2. Для досягнення об'єктивності дослідники повинні використовувати стандартизовані методи опису та запису інформації.

3. Суб'єктивність дослідника має важливе значення для визнання того, як його присутність може вплинути на об'єкт спостереження або сформувати його сприйняття подій.

Спостереження як метод дослідження може бути класифіковане за різними категоріями. Тому далі на основі роботи Т. Бербец [2] проаналізуємо різні категорії спостереження та їхні характеристики, що допоможуть в розумінні різновидів цього методу та його можливих застосувань.

1. За типом (мають відповідати конкретній меті дослідження):

- активне (дослідник бере активну участь у спостережуваному процесі);

- пасивне (спостереження проводиться без активної участі спостерігача).

2. За рівнем структури (залежно від ступеня контролю над спостережуваним процесом):

- природне (спостереження ведеться без заздалегідь заданих параметрів);

- структуроване (потребує визначення конкретних критеріїв).

3. За ступенем участі суб'єкта (залежно від того, чи потрібна активна участь суб'єкта):

- учасник (той, хто бере участь у спостережуваному процесі);

- неучасник (стороння людина, яка не бере участі в спостережуваному процесі).

4. За методами (може проводитись одночасно або окремо, залежно від наявних технічних засобів та об'єкта дослідження):

- онлайн-спостереження (проводиться в режимі реального часу з використанням технічних засобів);

- офлайн-спостереження (проводиться в режимі реального часу без використання техніки).

Загалом, поняття «спостереження» вказує на те, що цей метод можна використовувати як джерело даних у наукових, професійних чи соціальних дослідженнях. Проте його успіх залежить від врахування всіх можливих факторів, які можуть вплинути на об'єкт спостереження. У нашому дослідженні ми спостерігали за поведінкою учнів у віртуальному середовищі. Переваги методу спостереження полягають у тому, що він дає правдиву інформацію про реальну поведінку суб'єктів. Але воно також займає багато часу і вимагає ресурсів. До того ж може викликати ефект, коли учасники змінюють свою поведінку, коли за ними спостерігають.

У сучасному світі, де оцінювання, порівняння та ранжування різних явищ та об'єктів є неминучим, рейтингові шкали стали важливим інструментом аналізу та вимірювання [27; 48]. Використовуючи рейтингові

шкали, ми можемо висловити наші спостереження, оцінки та вподобання в чітких числових або категоріальних форматах.

Як освітлює в своїх роботах Ф. Чмиленко [61], рейтингові шкали відіграють важливу роль у різних аспектах нашого життя, таких як оцінка товарів і послуг, професійна діяльність та проведення наукових досліджень. Вони забезпечують системний підхід до оцінки різних об'єктів або явищ, дозволяючи проводити об'єктивні порівняння. Це особливо важливо в дослідженнях, які вимагають точних оцінок, наприклад, у сфері інформаційної безпеки. Крім того, рейтингові шкали спрощують порівняння об'єктів або явищ, надаючи числові або категоріальні міри, які полегшують аналіз і порівняння результатів. Ці шкали можуть мати два варіанти (бінарні), кілька варіантів, числові значення або категорії залежно від вимог дослідження.

Метод рейтингової шкали – це один зі способів оцінювання та порівняння об'єктів чи явищ, що ґрунтується на визначенні їхнього рівня або становища на шкалі, яка може мати конкретне числове або якісне вираження [14]. Характерними особливостями цього методу є [49]:

- структура шкали оцінки (може бути простою або складною залежно від конкретного застосування. Вона може включати числові оцінки, що присвоюються об'єктам за певними критеріями, або якісні оцінки, виражені в словесній формі. Структура шкали має бути чіткою і зрозумілою для оцінювачів і користувачів);

- принципи роботи (оцінювачі або експерти присвоюють бали кожному об'єкту, потім бали підраховують і порівнюють);

- кількість рівнів (шкала може мати різну кількість рівнів або категорій. Наприклад, шкала може варіюватися від 1 до 10 балів або бути якісною з такими категоріями, як «незадовільно», «задовільно», «добре» і «відмінно»);

- обрані критерії (враховуються конкретні критерії оцінки сайтів. Ці критерії можуть бути заздалегідь визначені та обговорені експертами або обрані на основі конкретного дослідження чи завдання);

- застосування до різних галузей (може застосовуватися до різних галузей, включно з бізнесом, освітою, медициною, соціальними дослідженнями тощо);

- інтерпретація результатів (для прийняття рішень необхідно інтерпретувати й аналізувати результати, отримані за допомогою рейтингової шкали. Така інтерпретація може бути різною залежно від конкретного завдання і передбачуваного використання оцінок).

Рейтингові шкали можна розділити на різні категорії залежно від їхнього призначення та методів, що використовуються для визначення показників. Розрізнення О. Пришляк цих категорій допомагає визначити, який тип рейтингової шкали підходить для конкретних завдань і досліджень [49].

1. Бінарна шкала – використовується для розподілу елементів на дві категорії, наприклад, «склав/не склав» у тесті з інформаційної безпеки.

2. Множинна шкала – може мати кілька категорій, наприклад, від «дуже погано» до «дуже добре» для оцінки знань з інформаційної безпеки.

3. Числова шкала – використовує конкретні числові значення для оцінки. Наприклад, бали за шкалою від 1 до 10 для рівня інформаційної безпеки.

4. Категорійна шкала – поділяє об'єкти на категорії або рівні за допомогою текстових міток, наприклад, «низький», «середній» і «високий» рівні інформаційної безпеки.

У нашому випадку респонденти оцінювали своє ставлення до різних аспектів інформаційної безпеки за допомогою шкали з кількома варіантами відповідей. Метод рейтингової оцінки дає змогу зібрати дані, які можна статистично обробити та порівняти між собою. Водночас шкали можуть бути суб'єктивними, оскільки ґрунтуються на індивідуальній думці респондентів. Також важливо, щоб шкала була чіткою та зрозумілою для учасників.

Для того, щоб проаналізувати та визначити рівень навичок інформаційної безпеки учнів 7-го класу, було використано низку методик та інструментів, які дозволили поглиблено дослідити їхні знання та ставлення до цієї важливої області. Кожна з обраних методик відігравала важливу роль у

конкретних аспектах, які необхідно було дослідити, щоб отримати загальну картину навичок і обізнаності учнів з безпеки.

У цьому розділі методи дослідження детально обговорюються та аналізуються для того, щоб проілюструвати характеристики та результати кожної методики. Поглиблений аналіз кожної методики дасть змогу краще зрозуміти формування навичок безпеки учнів 7 класу в онлайн-середовищі та виокремити ключові аспекти, які можуть впливати на їхню цифрову безпеку. Розглянемо кожну з них.

1. Анкетування про знання та практику створення та використання надійних паролів. Було складено авторську анкету, що містила запитання про знання і практику створення та використання надійних паролів. Запитання стосувалися використання унікальних паролів для різних облікових записів, використання довжини та різноманітності символів, а також використання двофакторної аутентифікації. Приклад одного із питань з даної анкети зображено на рисунку 2.1.

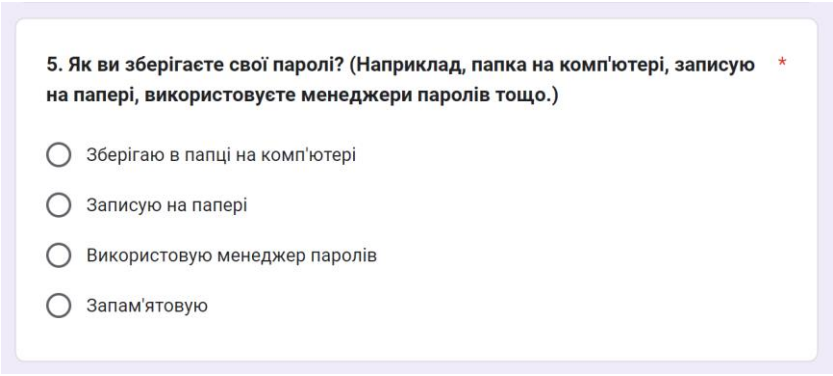


Рис. 2.1. Приклад питання з анкетування про знання та практику створення та використання надійних паролів

2. Тестування на визначення навички виявлення шкідливих програм. Учням надається авторський тест – список ситуацій або повідомлень, в яких можуть міститися посилання на шкідливі програми. Завдання учнів – виявити, які з цих ситуацій є потенційно небезпечними, і які дії вони будуть вживати, щоб уникнути завантаження шкідливих програм на свій комп'ютер). На

рисунку 2.2 зображено приклад одного із питань, що міститься у даному тестуванні.

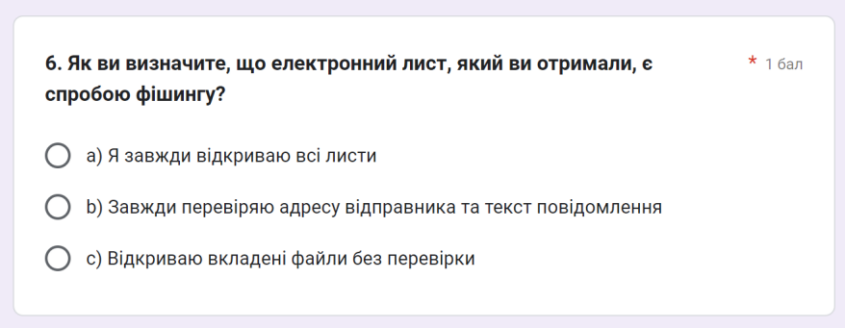


Рис. 2.2. Приклад питання із тестування на визначення навички виявлення шкідливих програм

3. Анкетування за допомогою методики «Лайкерта» із запитаннями про знання та практику учнів щодо розпізнавання та уникнення онлайн-шахрайства, фішингу та кібербулінгу. Було розроблено авторську анкету, що містить запитання, які стосуються практики освітян щодо виявлення та запобігання шахрайству, фішингу та кібербулінгу в Інтернеті. Запитання стосуються «червоних прапорців», що використовуються в шахрайських схемах, підходів до фішингу, безпеки та поведінки в Інтернеті. Рисунок 2.3 демонструє конкретний зразок питання, яке включено до цієї анкети.

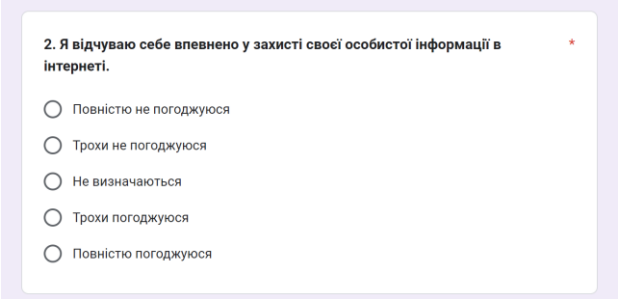


Рис. 2.3. Приклад питання із анкетування про знання та практику учнів щодо розпізнавання та уникнення онлайн-шахрайства, фішингу та кібербулінгу

4. Анкетування за допомогою методики «Лайкерта» щодо вмінь учня та його ставлення до використання соціальних мереж безпечно та відповідально. Готується авторська анкета. Учень повинен прочитати кожне твердження і вибрати відповідь за шкалою Лайкерта (зазвичай від 1 до 5), яка найкраще відображає його вподобання або навички. Після заповнення анкети можна проаналізувати відповіді учнів і зробити висновки про їхні навички та ставлення до безпечного та відповідального використання соціальних мереж. Один із зразків питань з опитування ілюструється на рисунку 2.4.

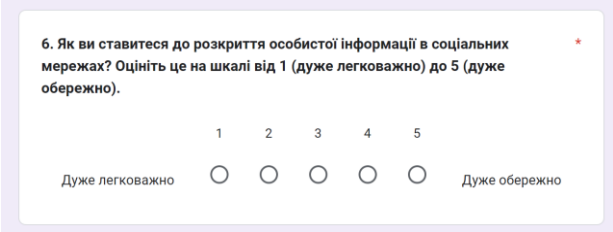


Рис. 2.4. Приклад питання із анкетування щодо вмінь учня та його ставлення до використання соціальних мереж безпечно та відповідально

5. Спостереження за поведінкою учнів у віртуальному середовищі є невід'ємною частиною дослідження, оскільки дозволяє проаналізувати їхню поведінку та взаємодію з онлайн-ресурсами. Це дозволяє глибше зрозуміти їхню цифрову поведінку та оцінити їхню здатність ефективно та безпечно користуватися інтернетом. Спостерігаючи за віртуальною діяльністю учнів, зокрема за їхньою взаємодією з пошуковими системами та переглядом веб-сторінок, проводиться систематичний аналіз їхнього ставлення до інформації, яку вони знаходять в інтернеті. Цей аспект дослідження виявляє рівень критичного мислення підліктів та їхню готовність самостійно оцінювати джерела інформації в Інтернеті.

6. Рейтингова шкала, що дозволить оцінити їхню позицію щодо кожного аспекту безпеки. Учням надається зрозумілий та структурований список тверджень, що охоплюють різні аспекти інформаційної безпеки. Кожному твердженню призначена рейтингова шкала, де респонденти повинні визначити

свою позицію, надаючи оцінку від 1 до 5. Загальні оцінки, отримані за кожним аспектом, надають змогу створити комплексний портрет позиції учня в контексті інформаційної безпеки. Рисунок 2.5 відображає, як виглядає певне питання з цієї анкети.

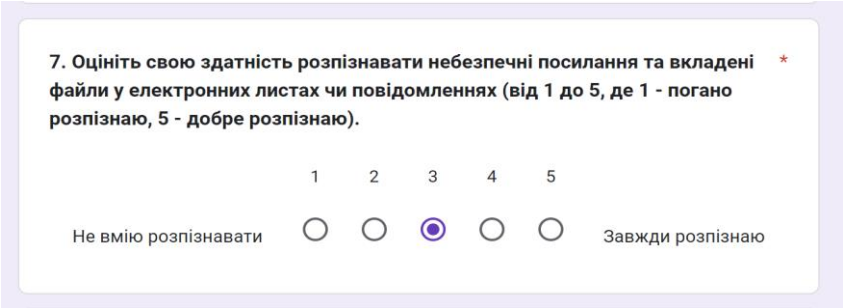


Рис. 2.5. Приклад питання із опитування «Рейтингова шкала» для оцінки позиції учня щодо кожного аспекту безпеки

7. Анкетування є важливим інструментом для дослідження сприйняття та практик учнів щодо інформаційної безпеки. Анкета охоплює кілька аспектів, таких як ставлення до надання особистої інформації в Інтернеті та їхні практики конфіденційності. Для забезпечення максимальної об'єктивності та всебічності опитування було розроблено анкету таким чином, щоб вона містила питання, спрямовані на сформованість навичок кібербезпеки. Шляхом проведення анкетування серед учнів можна буде отримати відповіді на ключові питання, пов'язані з усвідомленим та безпечним використанням Інтернету. На рисунку 2.6 наведено приклад опитувальника.

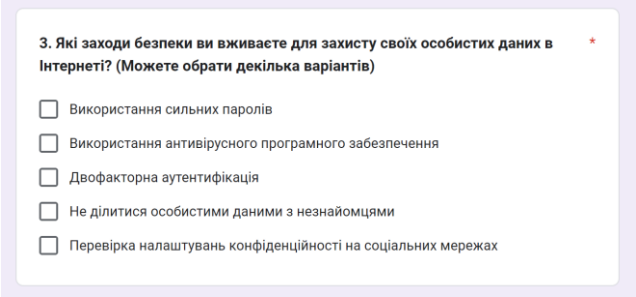


Рис. 2.6. Приклад питання із анкетування щодо надання персональних даних в Інтернеті та приватності особистих даних

7. Тестування для визначення середнього рівня навичок інформаційної безпеки учнів 7-х класів, а також для виявлення індивідуальних розбіжностей. Рисунок 2.7 надає візуальний приклад одного з питань, що стосується тестування.

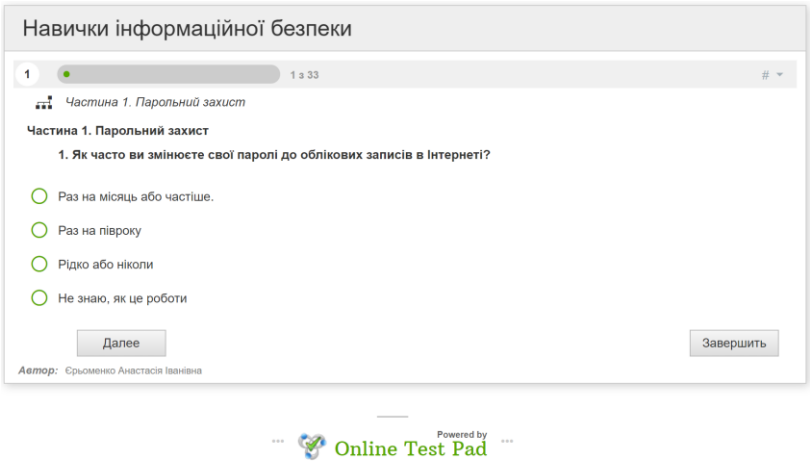


Рис.2.7. Приклад питання із тестування для визначення середнього рівня навичок інформаційної безпеки учнів 7-х класів

Даний тест вимірює середній рівень компетентності з інформаційної безпеки учнів 7-го класу та виявляє сфери, які потребують покращення. Після завершення тесту респондентам нараховуються бали за кожне запитання, а результати підраховуються для визначення загального рівня обізнаності. Респондентів пропонуємо розподіляти на п'ять категорій за рівнем обізнаності відповідно до їхніх балів, як показано в таблиці 2.1.

Таблиця 2.1. Рівні обізнаності

Рівень обізнаності	Кількісна оцінка обізнаності	Пояснення
Високий (V)	57-70	Для учнів характерно, що вони знають про принципи безпеки. Повсякденна поведінка відповідає правилам і рекомендаціям з інформаційної безпеки
Достатній (IV)	43-56	Учні добре розуміють основні аспекти інформаційної безпеки та можуть застосовувати їх у

		більшості ситуацій. Вони мають непогані знання та навички в цій області.
Задовільний (III)	29-42	Учні знають про небезпеки і знають, що вони повинні дотримуватися деякі основні принципи безпеки, але вони потребують подальшої освіти з цього питання. Вони не визнають своїх інцидентів і не знають, що робити в таких випадках
Низький (II)	15-28	Учні мають обмежене розуміння інформаційної безпеки та потребують значної підтримки та навчання для покращення своїх навичок.
Незадовільний (I)	0-14	Учні або не знають, або мають дуже обмежені знання і навички в галузі інформаційної безпеки і потребують серйозного навчання та підтримки.

Для проведення анкетування та тестування учнів буде використано онлайн-формат, і для цього будуть використовуватись платформи Google Forms та OnlineTestPad. Ці інструменти надають зручний та ефективний спосіб збору відповідей від учасників дослідження та підрахунок результатів в залежності від обраних варіантів. Використання Google Forms та OnlineTestPad дозволить легко створити анкети та тести, які можна буде надіслати учням для заповнення через Інтернет. Такий підхід спростить процес збору даних та дозволить швидко та зручно аналізувати результати дослідження.

2.2 Аналіз одержаних результатів дослідження стану сформованості навичок інформаційної безпеки в учнів 7 класів

Аналіз стану сформованості навичок інформаційної безпеки учнів відіграє важливу роль у визначенні ефективних заходів для навчання та підвищення обізнаності цієї аудиторії. Результати дослідження дають нам

змогу виявити сильні та слабкі сторони учнів у цій області, а також визначити групи, які можуть потребувати додаткової підтримки та навчання.

У цьому підрозділі ми розглянемо отримані результати дослідження та здійснимо аналіз рівня сформованості навичок інформаційної безпеки серед учнів 7-х класів. Такий аналіз дозволить нам визначити наявність різних рівнів обізнаності в цій галузі та визначити подальші кроки для покращення навчальних планів та підходів до безпеки в цифровому середовищі цих учнів.

У дослідженні брало участь 50 учнів 7-х класів закладу загальної середньої освіти. На загальному рівні, можна визначити, що більшість учасників дослідження демонструють рівень сформованості вище середнього в галузі інформаційної безпеки (рис. 2.7, 2.8). Вони проявляють обізнаність та здатність застосовувати важливі аспекти інформаційної безпеки в цифровому світі.

Проте варто відзначити, що в рамках дослідження було виявлено рідкі випадки, коли результати учнів відповідають рівню сформованості низькому або нижче середнього. Ці випадки свідчать про необхідність подальшої роботи над підвищенням інформаційної грамотності та безпеки серед цієї групи учнів.

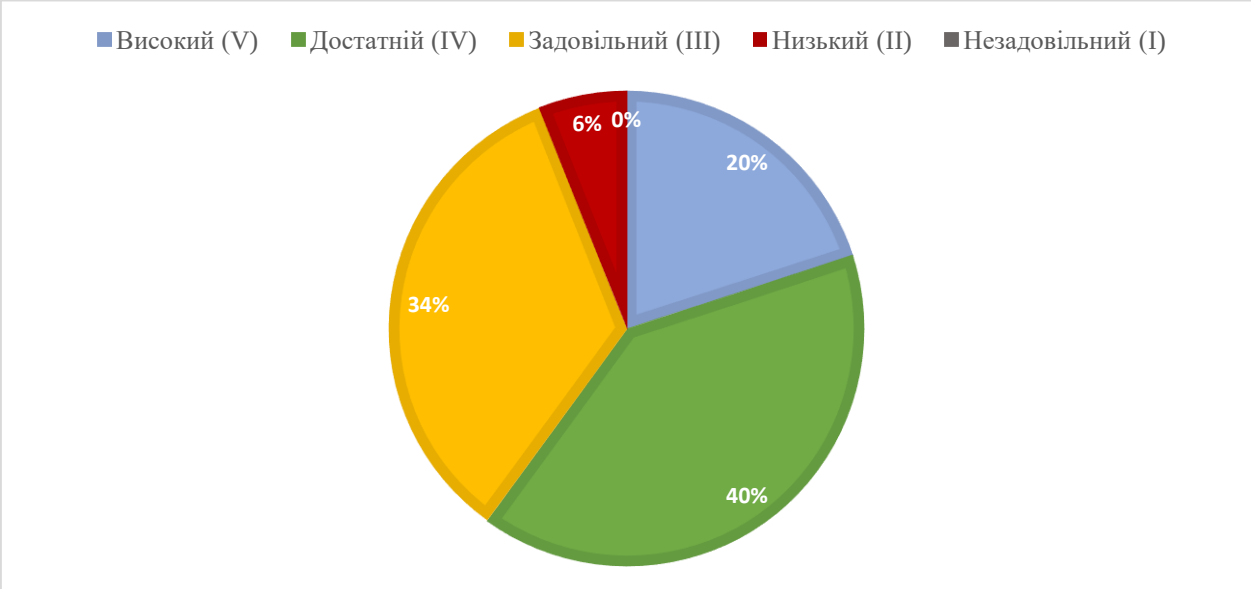


Рис. 2.7. Результат тестування для визначення середнього рівня обізнаності з інформаційної безпеки учнів 7-х класів

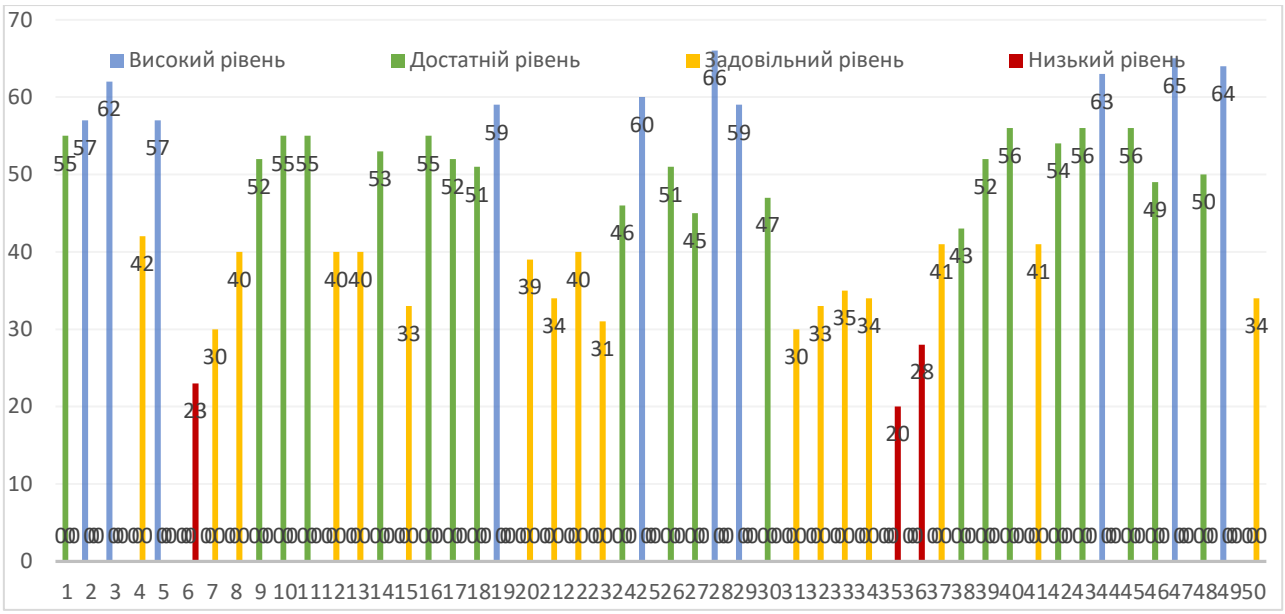


Рис. 2.8. Кількісна оцінка рівня обізнаності з інформаційної безпеки учнів 7-х класів

Проаналізуємо результати дослідження учнів з кожної з методик.

Аналіз результатів опитування щодо знань і практики створення та використання надійних паролів дає змогу отримати важливу інформацію про інформаційну грамотність учнів та їхні звички захищати ідентифікаційні дані в Інтернеті. Розглянемо тепер основні висновки, зроблені на основі отриманих даних.

1. Використання Інтернету. Слід зазначити, що 100% учнів щодня користуються Інтернетом. Це говорить про те, що доступ до цифрових технологій широко поширений серед учнів.

2. Знання паролів. За винятком одного учня, практично всі освітяни (98%) знають, що таке пароль і для чого він потрібен. Це свідчить про загальний рівень інформаційної грамотності учнів.

3. Використання пароля. Це дуже важлива категорія. Враховуючи той факт, що 46% учнів використовують один і той самий пароль для різних сервісів, слід пам'ятати, що така практика може бути небезпечною. Принаймні 54% відповіли «ні», що є позитивним знаком.

4. Складність пароля. 64% учнів створюють надійні та унікальні паролі для кожного сайту, які складаються з великих і малих літер, цифр і символів. Однак 10% використовують слабкі паролі, а 18% – один і той самий пароль для різних облікових записів. Необхідність створення надійних паролів очевидна.

5. Збереження паролів. 48% підбирають паролі, 26% записують їх, 16% використовують менеджер паролів і 10% зберігають їх на комп'ютері. Важливо, щоб учні розуміли, як правильно і безпечно зберігати паролі.

6. Додатковий захист. 64% використовують двофакторну автентифікацію, що свідчить про високий рівень захисту своїх облікових записів.

7. Зміна паролів. 44% змінюють пароль у разі підозри на злом, 20% – раз на рік, 6% – регулярно. 30% ніколи не змінюють свої паролі. Зміна паролів у разі підозри на злом дуже важлива, і більшість учнів знають про це.

8. Відновлення доступу. 66% учнів користуються послугою відновлення пароля на сайті, коли втрачають доступ до свого облікового запису через несанкціонований доступ або забувши пароль. Це говорить про те, що вони здатні вирішувати проблеми безпеки.

9. Обмін паролями. Тут 64% учнів не повідомляють нікому свої паролі, 44% – батькам і 10% – друзям.

10. Поінформованість про безпеку. Важливо зазначити, що лише 4% дітей знають про ситуації у своєму оточенні, коли вони стикалися з проблемами безпеки через слабкі паролі.

Загалом результати опитування показують, що багато учнів мають загальні уявлення про паролі та конфіденційність. Однак деякі з них використовують один і той самий пароль для кількох облікових записів, а інші – слабкі паролі. Заохочення учнів до створення надійних та унікальних паролів для кожного облікового запису та усвідомленого використання додаткових заходів безпеки, таких як двофакторна автентифікація, є важливим аспектом навчання інформаційної безпеки.

Розглянемо результати, отримані на основі даних тестування, яке дає змогу визначити, чи є навичка виявляти шкідливі програми показником рівня грамотності учнів у сфері інтернет-безпеки.

1. Розподіл балів. Розподіл балів показує різні рівні знань і вмінь учнів. 18 учнів отримали високі бали (від 8 до 9), що свідчить про високий рівень інформаційної грамотності в галузі виявлення шкідливих програм. Проте 7 учнів набрали лише від 1 до 4 балів, що може свідчити про низький рівень знань у цій галузі.

2. Поширені помилки:

- відповіді на запитання щодо ознак зараження шкідливим ПЗ – запитання містило більше ніж одну правильну відповідь, але лише 11 учнів змогли обрати обидва правильні варіанти (повільна робота комп'ютера та повідомлення про наявність викупу). Це дає можливість покращити розуміння ознак зараження комп'ютера;

- відповідь на запитання про взаємодію з невідомими абонентами – 30 учнів змогли правильно зазначити пункт «повідомити батькам або вчителю про те, що трапилося», але 15 учнів повісили слухавку, а 5 учнів повідомили всі свої дані. Ця ситуація підкреслює необхідність підвищення обізнаності учнів про безпеку даних і способи захисту особистої інформації.

2. Відсутність знань про двофакторну автентифікацію. Один зі учнів не був знайомий з концепцією двофакторної аутентифікації і тим, як вона сприяє забезпеченню безпеки облікового запису. Це важливий компонент комп'ютерної безпеки, який має бути включений до програми навчання.

3. Ігнорування попереджень про зараження комп'ютера. П'ять учнів проігнорували свої підозри про те, що їхній комп'ютер заражений шкідливою програмою. Це може свідчити про необхідність вдосконалення їхньої здатності розпізнавати проблеми та вживати заходів при їх виявленні.

Таким чином, аналіз результатів тестування показує, що учні мають різний рівень компетентності в галузі інформаційної безпеки в Інтернеті. Ці результати свідчать про необхідність подальшого вдосконалення навчання

комп'ютерній безпеці, особливо в галузі виявлення шкідливих програм і реагування на сумніви в безпеці.

Аналіз результатів анкети Лайкерта, присвяченої вивченню знань і практичних навичок учнів у сфері розпізнавання та запобігання шахрайству, фішингу та кібербулінгу в Інтернеті, дає змогу зробити такі основні висновки.

1. Розпізнавання шахрайства та фішингу:

- 58% учнів певною мірою згодні або повністю згодні з тим, що вони завжди розпізнають спроби фішингу та шахрайства;

- 28% учнів не впевнені, що можуть розпізнати фішинг;

- 30% учнів деякою мірою або категорично не згодні з цим твердженням.

2. Захист персональних даних:

- 60% учнів тією чи іншою мірою згодні з тим, що вони почуваються комфортно, захищаючи свої персональні дані в Інтернеті;

- 32% учнів не впевнені в тому, що вони можуть захистити свої дані;

- лише 12% учнів деякою мірою або категорично не згодні з цим твердженням.

3. Реагування на кібербулінг і шахрайство:

- 48% учнів тією чи іншою мірою згодні з тим, що вони завжди реагують на кібербулінг та шахрайство в Інтернеті, звертаючись до дорослих;

- 30% учнів не визначилися з тим, чи будуть вони реагувати на подібні інциденти;

- 20% учнів певною мірою або категорично не згодні з цим твердженням.

4. Перевірка посилань:

- 66% учнів тією чи іншою мірою згодні з тим, що вони завжди перевіряють посилання в електронних листах і на веб-сторінках, перш ніж натиснути на них.

- 20% учнів не впевнені в тому, чи стали б вони реагувати на такого роду інциденти;

- тільки 20% учнів певною мірою або категорично не згодні з цим твердженням.

5. Етикет спілкування в інтернеті:

- 78% учнів певною мірою або рішуче згодні з тим, що вони дотримуються етикету в Інтернеті та поважають інших людей у мережі;

- лише 14% учнів із цим не згодні.

6. Перевірка наявності «https://» на сайті:

- 74% учнів тією чи іншою мірою згодні з тим, що вони регулярно перевіряють відвідувані ними сайти «https://», щоб переконатися в їхній безпеці;

- 50% учнів тією чи іншою мірою не згодні з цим твердженням.

7. Реагування на небезпечні повідомлення :

- 58% учнів тією чи іншою мірою згодні з тим, що вони завжди ретельно перевіряють сайти, перш ніж надавати особисту інформацію або здійснювати платежі в Інтернеті. 36% учнів не реагують на небезпечні повідомлення;

- 36% учнів не висловлюють своєї думки з цього питання.

Загальний аналіз показує, що більшість учнів тією чи іншою мірою розуміють і дотримуються принципів Інтернет-безпеки, таких як розпізнавання фішингу, захист персональних даних і дотримання Інтернет-етикету. Однак деякі групи учнів можуть потребувати додаткового навчання та підвищення обізнаності в інтернеті, зокрема у питаннях перевірки ланок, безпеки зв'язків та розглядання сумнівних поштових повідомлень.

Аналіз результатів анкети Лайкерта відображає ставлення учнів до використання соціальних мереж, їхню відповідальність, обізнаність про безпеку та політику щодо використання соціальних мереж. Нижче подано основні висновки, зроблені на основі отриманих даних.

1. Відповідальність за використання соціальних мереж. 70% учнів відчувають відповідальність за використання соціальних мереж, що свідчить про їхнє серйозне ставлення до цього питання.

2. Безпека під час використання соціальних мереж. 66% учнів добре поінформовані про безпеку під час використання соціальних мереж.

3. Правила та політика використання соціальних мереж. 68% респондентів розуміють правила та політику використання соціальних мереж, включно з конфіденційністю та віковими обмеженнями.

4. Регулярність перевірки часу використання соціальних мереж. Майже половина учнів (44%) перевіряють час використання соціальних мереж часто або дуже часто, що може свідчити про важливість цієї теми в їхньому житті.

5. Ставлення до взаємодії з іншими користувачами. 62% учнів зазначили, що доброзичливо та шанобливо ставляться до інших користувачів соціальних мереж.

6. Розкриття особистої інформації. 70% з обережністю ставляться до розкриття особистої інформації в соціальних мережах, що свідчить про розуміння ними принципу конфіденційності.

7. Спілкування з батьками або викладачами. Лише 40% учнів регулярно обговорюють свою діяльність у соціальних мережах з батьками або викладачам

8. Джерела інформації про безпечне та відповідальне використання соціальних мереж. 62% учнів отримують інформацію про безпечне та відповідальне використання соціальних мереж з різних джерел.

9. Готовність навчатися та розвивати навички безпечного використання соціальних мереж. 66% учнів готові навчатися та розвивати навички безпечного використання соціальних мереж.

10. Значення соціальних мереж у житті учнів. 74% високо оцінюють можливості соціальних мереж і розуміють їхнє значення у своєму житті.

Загалом, переважна більшість учнів обізнані та відповідально ставляться до питань безпеки та відповідального використання соціальних мереж. Крім того, більшість їхніх батьків або викладачів залучені до роботи із соціальними мережами, що сприяє підвищенню рівня контролю та освіченості учнів у цій галузі. Однак є й ті, хто, можливо, потребує більшої уваги та просвіти в галузі онлайн-безпеки та відповідального використання соціальних мереж.

Аналіз результатів опитування за рейтинговою шкалою відображає ставлення та обізнаність учнів щодо різних аспектів безпеки в Інтернеті. Зазначимо, що за даним опитуванням учні самостійно оцінювали свої навички. Нижче представляємо основні висновки, які можна зробити на основі отриманих даних.

1. Обізнаність щодо основних загроз в Інтернеті. Більшість учнів (70%) мають високий рівень обізнаності про основні загрози в Інтернеті, що свідчить про їхню готовність розуміти ризики.

2. Навички створення та управління надійними паролями. 60% учнів мають середній або високий рівень навичок створення та управління надійними паролями.

3. Рівень використання антивірусного програмного забезпечення. 56% учнів використовують антивірусне програмне забезпечення.

4. Оновлення програмного забезпечення та операційної системи. 62% учнів регулярно оновлюють програмне забезпечення та операційні системи.

5. Знання про фішингові атаки. 70% учнів мають середній або високий рівень знань про фішингові атаки та способи їх виявлення.

6. Резервне копіювання важливих даних. Половина учнів створюють резервні копії важливих даних, щоб уникнути їх втрати.

7. Вміння розпізнавати небезпечні посилання та вкладення. Половина освітян (54%) мають середній або високий рівень вміння розпізнавати небезпечні посилання та вкладені файли.

8. Використання двофакторної автентифікації. 62% учнів використовують двофакторну автентифікацію для захисту своїх акаунтів.

9. Готовність ділитися випадковою інформацією в соціальних мережах. 68% з обережністю ставляться до того, щоб ділитися інформацією в соціальних мережах.

10. 64% учнів мають середній та високий рівень обізнаності про кібербулінг та способи захисту від нього.

Загалом, результати дослідження свідчать про те, що більшість учнів мають хороші навички та знання про безпеку в Інтернеті. Однак деякі з них можуть потребувати більшої уваги та навчання щодо деяких аспектів безпеки, таких як створення надійних паролів або розпізнавання небезпечних посилань.

Аналіз результатів опитування щодо ставлення учнів до надання особистої інформації в Інтернеті та заходів, яких вони вживають для захисту своєї приватності, дозволив нам зробити такі основні висновки.

1. Обережність при наданні особистої інформації в інтернеті усвідомлюють 52% учасників дослідження.

2. Половина учнів вважають, що їхні дані в Інтернеті є дуже важливими, тоді як решта 40% вважають, що вони є дещо важливими.

3. 78% учнів використовують різні заходи безпеки, такі як надійні паролі та антивірусне програмне забезпечення (70%). Більшість також визнає важливість двофакторної автентифікації (62%).

4. 70% респондентів створюють резервні копії важливих даних, що є доброю практикою для збереження інформації на випадок її втрати.

5. Більшість учнів (86%) усвідомлюють ризики та вживають заходів для обмеження доступу до своїх персональних даних у соціальних мережах.

6. 64% освітян обговорюють питання конфіденційності в Інтернеті з батьками або дорослими, що допомагає їм зрозуміти політику та практику.

7. 48% учнів під час реєстрації на веб-сайті або завантаження додатку надають альтернативні дані, щоб уникнути розголошення особистої інформації, вказуючи мінімально необхідну інформацію.

8. Деякі респонденти (32%) використовують режим браузера «інкогніто» браузера для перегляду чутливого контенту, щоб захистити конфіденційність, тоді як 18% не використовують цю функцію. Решта 50% не переглядають конфіденційний та чутливий контент.

9. Учні перевіряють надійність веб-сайтів та додатків, переглядаючи рейтинги та відгуки інших користувачів (46%), перевіряючи, чи з'єднання з

веб-сайтом має HTTPS (22%), та використовуючи додаткове програмне забезпечення для запобігання відстеженню (20%).

10. Більшість учнів (46%) не надають доступ до додатків та сайтів з прив'язкою до геолокації, а решта (46%) надають доступ лише до перевірених сайтів та додатків.

Загалом, результати опитування показують, що більшість учнів визнають важливість приватності в Інтернеті та роблять конкретні кроки для її захисту. Однак є ще багато можливостей для підвищення обізнаності та вжиття заходів для захисту приватності.

На останок зазначимо результати спостереження за поведінкою учнів у віртуальному середовищі.

1. Використання пошукових систем. Під час дослідження 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.

Висновки до розділу 2

Загальний висновок полягає в тому, що необхідно навчати школярів безпечного та відповідального використання Інтернету. Рекомендується проводити тренінги та нагадування про важливість перевірки джерел інформації, а також навчання тому, як захистити власні облікові записи та дані в онлайновому середовищі. Отримані результати також вказують на необхідність підвищення рівня інформованості учнів щодо безпечного та відповідального використання Інтернету. Доцільно навчати їх того, як розпізнавати та уникати шкідливих ресурсів, а також інформувати про наслідки завантаження чи збереження небезпечного контенту. Важливо також звернути увагу на ризики, пов'язані зі встановленням програмного забезпечення з ненадійних джерел, і наголосити на важливості забезпечення цифрової безпеки.

Для вивчення стану комп'ютерної безпеки учнів сьомих класів було використано кілька методів та інструментів. Для отримання повної інформації використовувалися анкети, тести, спостереження, рейтингові шкали та шкали Лайкерта. Використання Google Forms та OnlineTestPad для проведення опитувань спростило процес збирання та опрацювання даних.

Дослідження стану інформаційної безпеки серед учнів сьомих 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.

РОЗДІЛ 3. ПЕДАГОГІЧНІ УМОВИ ФОРМУВАННЯ НАВИЧОК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УЧНІВ 7 КЛАСІВ ЗАСОБАМИ ІНТЕРАКТИВНИХ ТЕХНОЛОГІЙ

3.1 Визначення педагогічних умов формування навичок інформаційної безпеки в учнів 7 класів засобами інтерактивних технологій

Науковці по-різному підходять до поняття «педагогічні умови», враховуючи різні аспекти, з яких вони його розглядають. Для педагогів, зокрема В. Кременя, педагогічні умови – це всі зовнішні чинники, які допомагають організувати навчальний процес. Наприклад, вони можуть включати питання організації, такі як плани уроків, організація навчальних матеріалів, що використовуються в класі, стилі викладання або те, як ці уроки проводяться, а також використання різних навчальних і технологічних ресурсів [30]. Педагогічні умови покликані сприяти навчанню, а також розвивати учня як особистість

Згідно з дослідженням С. Ладивір, вона розглядає це з психологічної точки зору, де педагогічні умови як середовище, що сприяє зростанню учнів, розглядаються з психолого-педагогічної точки зору. Важливість середовища, яке заохочує участь учнів, є життєво важливою для реалізації їх потенціалу [34]. Ці педагогічні фактори включають спільне планування колективної діяльності, створення мотивуючої атмосфери та вибір різних інструментів і методів для активного навчання.

Як і Я. Шугайло, соціологи та педагоги розглядають педагогічні умови як соціально-педагогічне середовище, що впливає на виховання та навчання учнів. Авторка констатує, що організаційні чинники впливають на соціальні відносини та взаємодії між учасниками навчально-виховного процесу [62]. Педагогічні умови полягають у створенні позитивного соціального клімату, в

якому відбувається взаємодія, надається підтримка та досягається взаєморозуміння між вчителями та учнями.

Варто зазначити, що різні автори подають поняття «педагогічні умови» різноманітно і широко. Вивчивши різні наукові джерела, було встановлено, що педагогічні умови – це цілеспрямовано створені обставини, які створюються для впливу на різні компоненти, що сприяють інноваційному підходу в освіті, та відіграють вирішальну роль у просуванні інновацій в освітньому процесі в загальноосвітньому навчальному закладі [64]. Перейдемо до розгляду конкретних педагогічних умов, які сприятимуть розвитку навичок інформаційної безпеки в учнів 7 класу.

Для того, щоб сприяти розвитку навичок інформаційної безпеки в учнів, важливо, щоб певні педагогічні умови були реалізовані на практиці. Це включає в себе створення сприятливого та інноваційного навчального середовища, підвищення мотивації школярів до вивчення інформаційної безпеки, а також сприяння партнерській взаємодії між викладачем та учнем. Розглянемо детальніше поставлені педагогічні умови.

Першою педагогічною умовою визначимо створення сприятливого та інноваційного навчального середовища.

В сучасному освітньому контексті відомо, що однією з найважливіших завдань вчителів та педагогів є створення сприятливого та інноваційного навчального середовища. Ця педагогічна умова спрямована на покращення якості навчання та розвитку учнів, враховуючи їхні індивідуальні потреби, сучасні технології та передові педагогічні підходи.

Сучасні дослідники активно досліджують поняття «навчальне середовище» та його вплив на процес навчання та розвитку учнів. Так, наприклад, один із видатних українських педагогів, В. Кремень, наголошує на важливості створення такого середовища, де кожен учень відчуває себе зайнятим, комфортно та здатним до саморозвитку [30].

Сприятливе навчальне середовище важливо розглядати як як комплексний аспект, що включає не лише фізичні параметри, а й

психосоціальні та емоційні складові. Про це згадується у дослідженнях Н. Давидюк [15], яка підкреслює важливість створення позитивного емоційного клімату в класі та взаємодії між учнями для успішного навчання. Це може передбачати використання різних підходів, таких як початок діалогу про середовище в класі між учнями та обговорення в класі питань безпеки під час доступу до мережі, сприяючи тим самим учнівській ініціативі та самовираженню.

Створення психологічно сприятливого середовища також може закликати вчителів заохочувати відкриті дебати та обмін ідеями щодо вирішення проблем, пов'язаних з кібербезпекою. У статті Л. Василенко [8] представлено кілька альтернативних можливостей. Вони повинні залучати учнів до таких видів діяльності, як групові проекти або командні дебати, які спрямовані на розвиток соціальних навичок, а також на усвідомлення ними важливості інформаційної безпеки в їхньому житті в Інтернеті.

Натомість, Н. Бітнер та Дж. Бітнер [65] у своїй роботі визначають, що інноваційне навчальне середовище визначається використанням передових технологій, педагогічних методів та підходів. Також автори вказують на важливість інтеграції сучасних технологій для забезпечення ефективного навчання. Інновації включають в себе використання віртуальних навчальних середовищ, інтерактивних технологій, проєктно-орієнтованого навчання та інших передових педагогічних підходів.

Отже, створення сприятливого та інноваційного навчального середовища є актуальним завданням для покращення умов навчання. А наукові дослідження вказують на важливість індивідуалізованого та інноваційного підходу до навчання, що сприяє розвитку учнів.

Наступною педагогічною умовою є підвищення мотивації учнів до вивчення інформаційної безпеки. У сучасному світі це стає життєво важливим питанням у досягненні успіхів у навчанні та особистісному розвитку. Перед вчителями стоїть завдання не просто подати інформацію, але й викликати захоплення та інтерес до досліджень. Визначимо, як педагогічна умова

зростання мотивації школяра впливає на здобуття знань з інформаційної безпеки і що можна зробити, щоб досягти цього наміру.

Мотивація є ключовим поняттям, що визначає бажання та готовність учнів до навчання та досягнення певних цілей. Це внутрішнє підприємливе прагнення, яке визначає напрямок та інтенсивність навчальної діяльності. Науковці у сфері педагогіки визначають різні аспекти мотивації, зокрема за теорією ієрархії потреб (А. Маслоу) [79] мотивація учнів може бути пов'язана з задоволенням основних потреб, таких як фізіологічні потреби, потреби в безпеці, соціальні потреби, почуття самооцінки та самореалізації. З погляду поведінкової психології (Б. Скіннер) [85], мотивація зумовлюється посиленням або покаранням, що допомагає формувати певні звички та навички. Теорія самовизначення Е. Деці [69] розглядає мотивацію як внутрішнє прагнення до розвитку свого потенціалу, визначення власних цілей та взаємодії з оточуючим світом. Але всі вони сходяться в одному: мотив є внутрішньою силою, що спонукає людину до діяльності.

На підставі здійсненого аналізу визначимо, що мотивація до вивчення інформаційної безпеки представляє собою внутрішнє стимулююче прагнення та інтерес учнів до освоєння концепцій, навичок і знань, пов'язаних з безпечним та відповідальним використанням інформаційних технологій. Ця мотивація визначається усвідомленням важливості інформаційної безпеки для особистого та професійного розвитку, забезпечення власної безпеки в цифровому середовищі та активного бажання засвоїти необхідні знання для ефективного використання інтернет-ресурсів та збереження конфіденційності особистої інформації.

Ми поділяємо точку зору, що мотивація формується, розвивається, змінюється, реорганізується та реалізується в процесі діяльності [64]. Беручи це до уваги, ми вважаємо, що наявність різноманітних мотивацій значно підвищить ефективність навчання, сприяючи досягненню навчальних цілей. Різноманітна мотивація сприяє створенню адаптивного середовища, де кожен учень може виявити свою внутрішню рушійну силу. Це не лише допомагає їм

засвоїти концепції інформаційної безпеки, але й дозволяє їм застосовувати набуті знання у своєму житті. Таким чином, різноманітна мотивація є ключем до розкриття потенціалу кожного учня та досягнення стандартів освіти в сучасному інформаційному суспільстві.

Мотивація школярів до вивчення інформаційної безпеки має вирішальне значення. Цього можна досягти, зацікавивши їх та підкресливши важливість цього предмету. Для досягнення цієї мети ми пропонуємо включати завдання та реальні життєві сценарії, які дозволяють застосовувати свої знання в реальних ситуаціях. С. Семчук у своєму дослідженні зазначила, що практичні завдання включають моделювання реальних сценаріїв кіберзагроз або вправи з етичного використання інформації, які дозволяють зрозуміти складнощі, пов'язані з пошуком рішень для проблем. Наприклад, використовуються відеоуроки та інтерактивні сценарії, які допомагають підвищити інтерес та покращити засвоєння матеріалу [50]. Такий підхід не тільки підвищить їхню мотивацію, а також зробіть процес навчання більш цікавим.

Важливо підкреслити, як навчання з інформаційної безпеки може позитивно вплинути на особисте та освітнє зростання учням, дозволяючи їм ставити цілі та визнавати важливість набуття цих знань. Створюючи середовище, в якому здобувачі можуть по-справжньому оцінити актуальність теми, ми сприяємо підвищенню мотивації до вивчення інформаційної безпеки. Нарешті, використання уроків, відео та онлайн-ігор може ефективно залучити учнів, одночасно представляючи актуальну тему в доступній формі.

Отже, підвищення мотивації учнів до вивчення інформаційної безпеки є необхідним і достатнім кроком для результативного й ефективного формування їх навичок у даній області і тому її будемо вважати педагогічною умовою.

Як третю педагогічну умову розглянемо сприяння партнерській взаємодії між викладачем та учнем.

Партнерські відносин між вчителем та учнем – це стосунки, які ґрунтуються на взаємоповазі, взаєморозумінні та спільній меті досягнення

знань та освітніх цілей [54]. Однак, незважаючи на важливість цього аспекту, існують певні проблеми, які можуть заважати налагодженню ефективних партнерських відносин [58].

1. Вчителі та учні часто можуть мати різні очікування від навчання. Наприклад, вчителі можуть прагнути до стандартів та оцінювання, тоді як учні можуть бажати більше акценту на індивідуалізацію та творчий підхід.

2. Недостатнє взаєморозуміння може виникнути через різниці вікових, культурних чи соціальних факторах. Це може створити бар'єри для ефективної комунікації та співпраці. Так, в контексті нашого дослідження, учні можуть не повністю усвідомлювати серйозність існуючих інтернет-загроз та не розуміти, як їм захистити свої дані.

3. Учні можуть відчувати брак можливостей для активної участі в процесі навчання та прийняття рішень, що може впливати на їхню мотивацію та інтерес до навчання.

4. Деякі вчителі можуть відчувати страх втрати авторитету, якщо дозволити учням більше впливати на навчальний процес, що може призвести до конфліктів у взаємодії.

Зауважимо, що формування навичок інформаційної безпеки в учнів вимагає ефективних та партнерських відносин між вчителем та учнем. Для вирішення проблем, які можуть виникнути в цьому процесі, доцільним буде вдосконалювати підходи та застосовувати новаторські стратегії такі як: відкритий діалог та слухання, залучення учнів до процесу планування навчання, застосування інноваційних методів навчання, організація позаурочних заходів та спільних проєктів, розвиток цифрової грамотності.

Багатогранна взаємодія між учнями та вчителями є ключовим фактором формування соціальної сторони педагогічних умов, яка відіграє вирішальну роль у формуванні партнерських відносин [51]. У конкретному контексті розвитку навичок інформаційної безпеки в учнів 7-х класів це передбачає створення сприятливого середовища для взаємодії та співпраці. Наприклад, учні можуть об'єднуватися в групи або клуби для обговорення актуальних тем

з кібербезпеки, обміну знаннями та вирішення спільних проблем. Такий підхід дозволяє вчителям та дітям спільно вивчати та обговорювати теми, пов'язані із сучасними технологіями та цифровим середовищем. Такі ініціативи сприяють розвитку почуття відповідальності та заохочують взаємопідтримку між учнями у віртуальному світі.

Також відмітимо, що за словами О. Волошиної, налаштування партнерських відносин враховує також і залучення батьків до спільних зусиль, спрямованих на сприяння навчанню та підготовці [10]. Прикладом цього може бути організація батьківських зборів або семінарів для обговорення проблем кібербезпеки та обміну корисними порадами і ресурсами. Така співпраця забезпечує послідовний підхід до безпеки в Інтернеті як вдома, так і в школі, сприяючи створенню сприятливого середовища для розвитку необхідних навичок та відповідальної поведінки в Інтернеті.

Отже, формування навичок інформаційної безпеки в учнів вимагає тісної співпраці між вчителем та учнем. Розуміння та вирішення проблем партнерських відносин допоможе створити ефективну освітню програму, яка дозволить молодому поколінню безпечно та відповідально користуватися інформаційними ресурсами.

Наступним звернемо увагу на використання інтерактивних технологій, оскільки вони є цінним ресурсом для залучення учнів та створення сприятливого навчального середовища.

Розглянувши умови та процес формування навичок інформаційної безпеки в учнів 7-х класів, стає очевидним, що успішний підхід вимагає впровадження сучасних інструментів, спрямованих на посилення участі та залучення учнів. У цьому відношенні інтерактивні технології відіграють важливу роль, не тільки роблячи навчальний процес цікавим, але й сприяючи більш ефективному засвоєнню навчального матеріалу.

Отже, коли йдеться про формування в учнів 7-го класу навичок інформаційної безпеки, визначені педагогічні умови приділяють значну увагу інтерактивним технологіям. Таке визнання важливості сучасних

технологічних досягнень має вирішальне значення для досягнення успішної освіти та виховання учнів. Ці умови мають на меті не лише заохотити учнів до участі в цифровому середовищі, але й задовольнити їхні індивідуальні інтереси та потреби, щоб створити продуктивний навчальний процес. Просуваючись далі, заглибимося в практичні заходи та поради щодо ефективного впровадження цих умов у клас.

3.2 Методичні рекомендації щодо реалізації педагогічних умов формування навичок інформаційної безпеки учнів 7 класів засобами інтерактивних технологій

У цьому підрозділі ми пропонуємо практичні поради щодо ефективного впровадження інтерактивних технологій у методику викладання з метою формування навичок інформаційної безпеки в учнів 7-го класу. Беручи до уваги унікальні особливості цього етапу підліткового віку та динаміку навчального середовища, рекомендовані нами стратегії спрямовані на підвищення рівня безпеки та обізнаності про цифрові ризики. Реалізація цих педагогічних умов формування в учнів 7 класу навичок інформаційної безпеки засобами інтерактивних технологій вимагає системного та ретельного підходу.

1. Створюйте спеціальні курси та плани:

- зрозумійте, як навчаються різні учні. Використовуйте стратегії, які найкраще підходять для навчання їх інформаційної безпеки;

- упорядковуйте теми, оновлюйте інформацію, повільно вводьте складні поняття та використовуйте їх у реальних ситуаціях;

- визначте критерії для оцінювання, тестів і перевірок, щоб з'ясувати, наскільки добре учні навчаються.

2. Змінюйте програми відповідно до потреб учнів:

- зробіть навчання особистим. Подумайте про те, як швидко навчається кожен учень, і створіть завдання для всіх рівнів навичок;

- пам'ятайте, що подобається учням. Використовуйте веселі приклади та сценарії, щоб зробити навчання приємним.

3. Створіть позитивний навчальний простір:

- створіть корисний клас. Зробіть його привітним і націленим на навчання;

- працюйте з батьками задля успіху учнів. Це допоможе у навчанні вдома і в школі.

4. Використовуйте цікаві методи навчання:

- використовуйте цікаві технічні засоби навчання, такі як комп'ютерні програми та інтерактивні завдання. Дітям це подобається, і вони краще вчаться;

- побудуйте відкритий канал зв'язку між вчителями та учнями. Це допомагає всім.

5. Допомагайте учням бути ініціативними:

- включіть заходи, які змушують учнів думати. Особливо в таких предметах, як інформаційна безпека;

- заохочуйте дітей проводити власні дослідження з безпеки. Це чудовий інструмент навчання.

6. Організуйте командну роботу та групове навчання:

- плануйте групові вправи та завдання. Це може покращити комунікацію та спільну роботу учнів;

- наводьте приклади з реального життя. Це може сприяти обговоренню різних рішень для інформаційної безпеки.

7. Проводьте інформаційні заходи та бесіди:

- запрошуйте фахівців з кібербезпеки для проведення занять та семінарів;

- проводьте бесіди для батьків про інформаційну безпеку. Поділіться порадами про те, як їхні діти можуть безпечно користуватися Інтернетом.

8. Розробіть спеціальні тренінги:

- створіть програми, пристосовані для вивчення певних аспектів інформаційної безпеки. Переконайтеся, що вони відповідають віковій групі;

- навчайте основам. Уроки повинні включати безпеку в Інтернеті, вірусологію та кібергігієну.

9. Використовуйте цікаві відеоуроки:

- використовуйте динамічні, інтерактивні відео для демонстрації прикладів кіберзагроз та їх запобігання;

- включіть у відеоуроки вправи на вирішення проблем, щоб розвивати навички реагування на кіберзагрози.

10. Розробіть практичні завдання:

- створюйте практичні завдання, які дозволять учням застосувати набуті знання в реальності;

- використовуйте симуляції та інтерактивні ігри для практичного навчання навичкам інформаційної безпеки.

11. Ініціюйте проведення вебінарів під керівництвом експертів:

- проводьте доступні лекції, на яких висококваліфіковані фахівці з кібербезпеки ділитимуться своїм досвідом та ключовими рекомендаціями;

- створіть середовище, в якому учні зможуть ставити запитання та отримувати ґрунтовні відповіді.

12. Підготуйте онлайн-вікторини та тести:

- створюйте тестові завдання, щоб оцінити рівень навчання та підвищити обізнаність про кіберзагрози;

- створюйте веселі онлайн-вікторини, щоб зацікавити учнів та підвищити їхню активність.

13. Розробка власних блогів та відеожурналів:

- дайте учням завдання створити блоги про безпеку в Інтернеті, щоб поділитися знаннями та думками;

- організуйте відеожурнали з корисними порадами щодо безпечного користування Інтернетом.

14. Адаптуйте методи:

- враховуйте унікальні риси кожного учня при плануванні та проведенні уроків;

- сприяйте самостійному навчанню, надаючи поради для самостійного вивчення предметів.

15. Створіть сприятливе навчальне середовище:

- учні повинні працювати в затишній атмосфері в класі і бути готовими брати участь у навчанні;

- слід налагодити співпрацю між батьками та педагогами, щоб надавати учням допомогу вдома і полегшити їм процес навчання.

Для ефективного та цікавого викладання кібербезпеки ми рекомендуємо використовувати інтерактивні технології, які не лише сприяють розумінню принципів безпеки в Інтернеті, але й роблять навчання цікавим та практичним.

Прикладами інтерактивних відеоуроків з інформаційної безпеки можуть бути платформи «Google: Be Internet Awesome» (рис. 3.1), «Дія: Освіта», «Netsmartz Workshop» які надають ігровий та взаємодійний підхід до навчання основам кібербезпеки для школярів. Використання інтерактивних відеоуроків на зазначених платформах стане не тільки педагогічно доцільним, але і ефективним засобом формування навичок інформаційної безпеки серед учнів загальноосвітніх закладів.

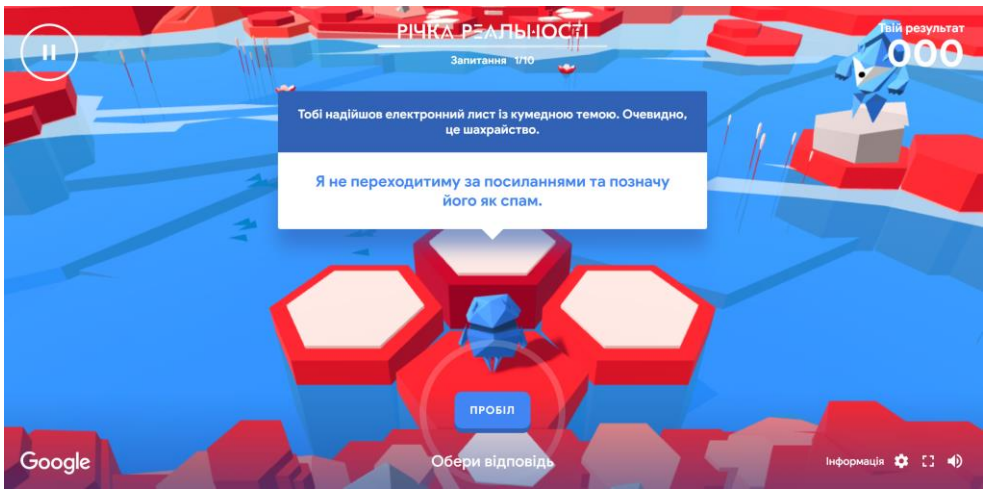


Рис. 3.1. Фрагмент інтерактивного відеоурока «Google: Be Internet Awesome» (скріншот з екрану)

Такі популярні платформи, як Kahoot!, Quizizz (рис. 3.2) та Socrative, надають викладачам чудові можливості для реалізації ефективного процесу навчання школярів інформаційної безпеки. Ці інтерактивні сервіси не лише надають зручні інструменти для створення тестів, а й пропонують зручний інтерфейс для їхнього адміністрування та оцінювання. Використання цих платформ у навчальному процесі дає змогу вчителям застосовувати інноваційні та захопливі методи навчання для формування в учнів базових навичок інформаційної безпеки. Ці інтерактивні інструменти створюють сприятливе середовище для активної участі учнів, роблять предмет цікавішим і покращують навички онлайн-безпеки.

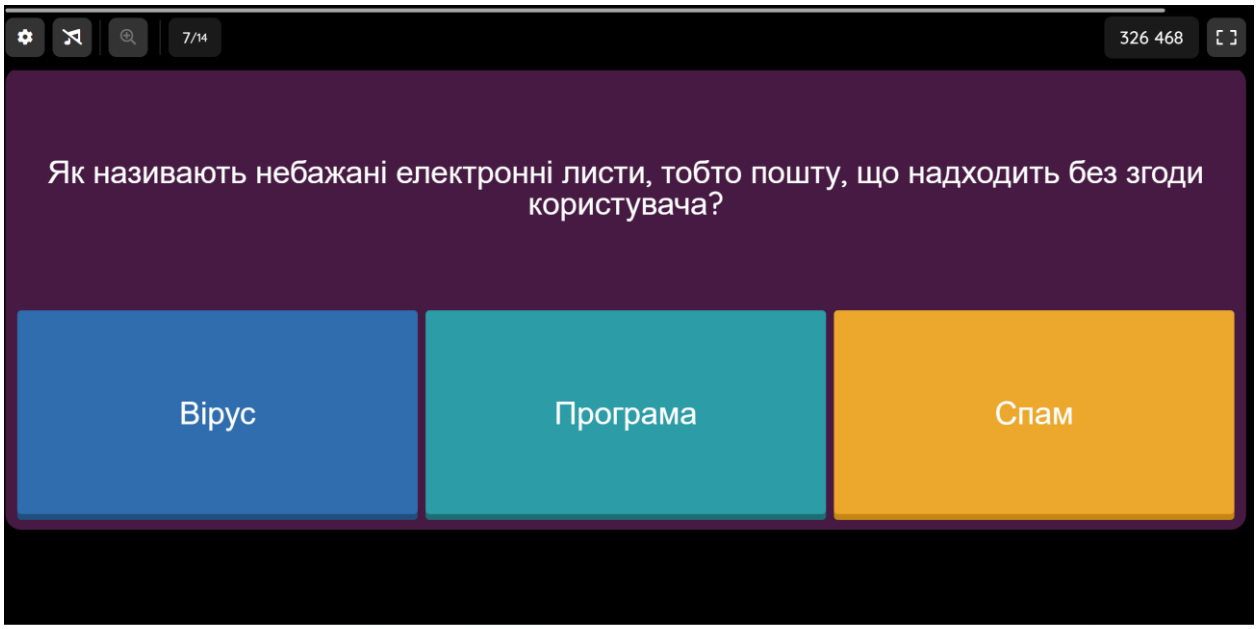


Рис. 3.2. Фрагмент онлайн-вікторини на платформі «Quizizz» (скріншот з екрану)

Пропонуємо сайти, які надають доступ до інтерактивних ігор та симуляцій з питань інформаційної безпеки: «Spoofy» (рис. 3.3) для боротьби з реальними кіберзагрозами, «CRDF GLOBAL» для отримання міцних знань з інтернет-безпеки та «Онлайн-безпека для підлітків» для симуляцій, спеціально розроблених для молоді (рис. 3.4). Ці інструменти навчання з

ефектом занурення – надійний спосіб зацікавити учнів і сприяти глибокому розумінню кіберзагроз.

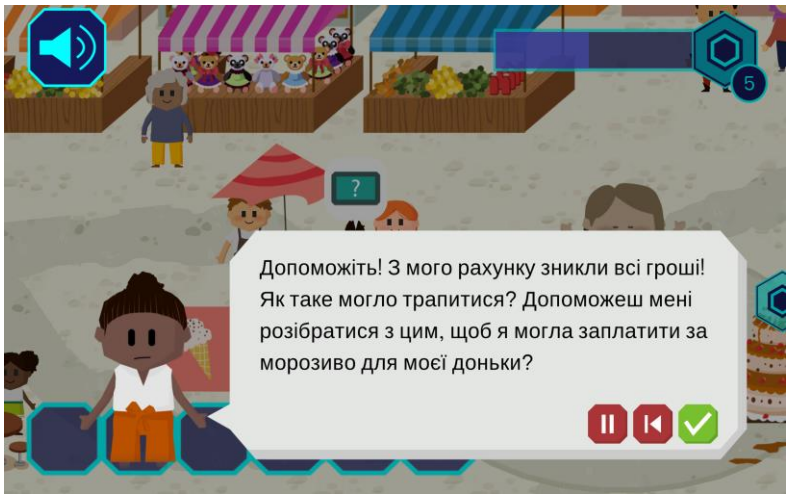


Рис. 3.3. Фрагмент інтерактивної гри про кібербезпеку «Spoofy» (скріншот з екрану)

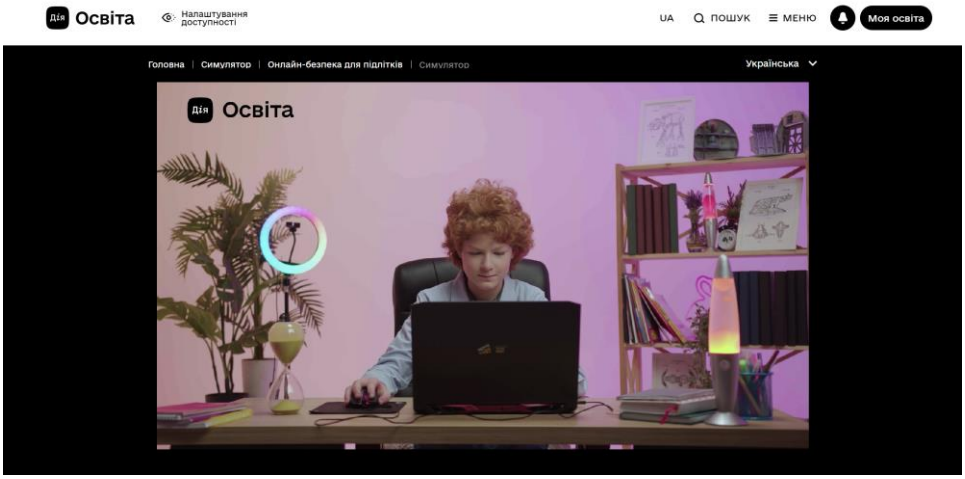


Рис. 3.4. Фрагмент симулятора онлайн-безпеки для підлітків на платформі «Дія: Освіта» (скріншот з екрану)

Приклади сайтів, де можна знайти та використати уроки з теми інформаційної безпеки через створення блогів, включають «Kidblog», «Edublogs» та «Blogger» (рис. 3.5). Ці динамічні платформи дають учням можливість висловлювати свої погляди та ідеї щодо безпеки в Інтернеті, а також брати участь у змістовних дискусіях з іншими користувачами.

Створюючи безпечну і збагачуючу віртуальну спільноту, ці сайти сприяють цінному і цікавому навчанню.

Рис. 3.5. Фрагмент блогу з кібербезпеки на платформі «Blogger» (скріншот з екрану)

Серед блогерів та експертів, які заглиблюються в тему підліткової інформаційної безпеки, варто відзначити блог «Дія: Цифрова освіта» (рис. 3.6), в якому беруть участь авторитетні фахівці з кібербезпеки та національно визнані медіа-діячі. Іншим цінним ресурсом є блог «Хакер, що біжить» експерта з кібербезпеки Володимира Стирана, а також онлайн-курс «Основи кібербезпеки для школярів», створений CRDF Global в Україні у співпраці з ГО «Смарт Освіта» та Technomatix. Ці ресурси демонструють високий рівень майстерності та вміння ефективно взаємодіяти з молодими людьми, розглядаючи відповідні аспекти кібербезпеки та пропонуючи практичні поради щодо безпечного користування Інтернетом.

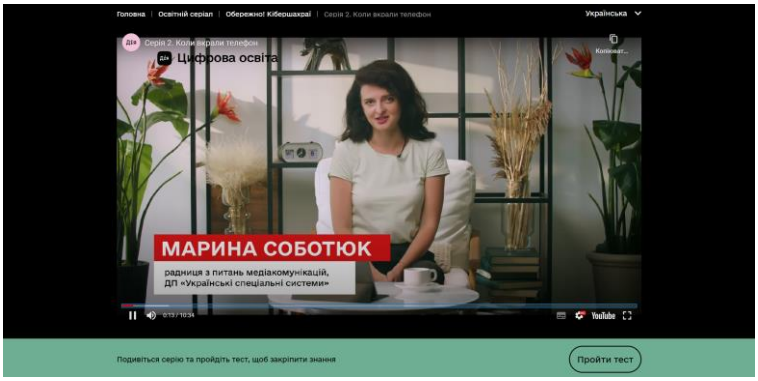


Рис. 3.6. Фрагмент блогу «Дія: Цифрова освіта» (скріншот з екрану)

Впроваджуючи ці методичні рекомендації, педагоги можуть ефективно формувати навички інформаційної безпеки в учнів 7 класу з використанням інтерактивних технологій. Важливо зазначити, що ключ до успіху полягає у створенні цікавого та динамічного навчального середовища. Ці рекомендації розроблені з урахуванням унікальних вікових та когнітивних здібностей учнів, заохочуючи їх до активної участі та сприяючи формуванню важливих навичок інформаційної безпеки. Рекомендоване використання інтерактивних технологій не лише передає знання, але й озброює учнів необхідними навичками для безпечної навігації в Інтернеті та на цифрових платформах.

Висновки до розділу 3

У цьому розділі ми ретельно систематизували та дослідили основні педагогічні умови формування навичок інформаційної безпеки в учнів 7-го класу. Перший підрозділ присвячений визначальній ролі педагогічних умов у формуванні в учнів розуміння інформаційної безпеки. Було виявлено, що інтерактивні технології відіграють вирішальну роль в ефективному формуванні цих навичок. Наведено різноманітні педагогічні умови, спрямовані на підвищення рівня розуміння учнями інформаційної безпеки. У другому частині викладено конкретні методичні пропозиції щодо інтеграції визначених педагогічних умов у навчальний процес з метою створення сприятливого середовища та озброєння здобувачів освіти необхідними знаннями.

Загалом, дуже важливо адаптувати педагогічні умови формування навичок інформаційної безпеки до вимог сьогодення та враховувати унікальний розвиток учнів 7 класу. В освітньому середовищі інтерактивні технології є важливими для ефективної реалізації цих педагогічних умов.

ЗАГАЛЬНІ ВИСНОВКИ

Кваліфікаційна робота висвітлює теоретичний аналіз проблеми формування навичок інформаційної безпеки в учнів 7-го класу за допомогою інтерактивних технологій та результати емпіричного дослідження стану зазначеної проблеми, що стало підставою для визначення педагогічних умов розв'язання проблеми дослідження, надання методичних рекомендацій щодо їх впровадження та формулювання таких висновків:

1. Під навичками інформаційної безпеки розуміється набір знань, навичок і поведінкових стратегій, що дають змогу безпечно й ефективно використовувати інформаційні технології. Вони включають в себе розуміння принципів безпечної поведінки в мережі, аналіз інформації, виявлення шахрайства, забезпечення захисту даних і розуміння наслідків ризикованих дій у кіберпросторі.

Визначено 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.

З'ясовано, що особливості формування навичок інформаційної безпеки в учнів 7-го класу виявляються у підвищеній активності в Інтернеті, підвищеній схильності до ризикованої поведінки, розвитку критичного мислення, впливу групової динаміки, розвитку розуміння конфіденційності та захисту даних.

2. Виявлені і розкриті можливості інтерактивних технологій навчання і виховання в ефективності формування навичок з інформаційної безпеки в учнів 7 класів: використання стимулюючого середовища, щоб навчити учнів розпізнавати та уникати потенційно небезпечних ситуацій в Інтернеті; залучення учнів до ігор та вирішення проблем, які стимулюють їхню активність та розвивають навички безпеки; візуалізація складних понять,

пояснення сценаріїв та демонстрація практичних прикладів; полегшення вимірювання прогресу та виявлення слабких місць, які потребують більшої уваги та навчання; створення реальних життєвих ситуацій для практичного навчання; надання учням можливості експериментувати.

Діагностика стану сформованості навичок інформаційної безпеки в учнів 7 класів здійснювалася за допомогою низки методик: анкетування про знання та практику створення та використання надійних паролів, тестування на визначення навички виявлення шкідливих програм, анкетування із запитаннями про знання та практику учнів щодо розпізнавання та уникнення онлайн-шахрайства, фішингу та кібербулінгу, анкетування за допомогою шкали Лайкерта щодо вмінь учня та його ставлення до використання соціальних мереж безпечно та відповідально, спостереження за поведінкою учнів у віртуальному середовищі, наприклад, за їхнім використанням пошукових систем, пошуком інформації в мережі або взаємодією з небезпечним вмістом, рейтингова шкала, що дозволить оцінити їхню позицію щодо кожного аспекту безпеки, анкетування, яка охоплює аспекти, як учні ставляться до надання персональних даних в Інтернеті, та які кроки вони вживають для збереження приватності, тестування для визначення середнього рівня навичок інформаційної безпеки учнів 7-х класів, а також для виявлення індивідуальних розбіжностей.

Базою дослідження став Одеський ліцей «Ланжеронівський» Одеської міської ради.

Одержані результати свідчать про те, що учні частково усвідомлюють ризики, пов'язані з розкриттям персональних даних, і вживають заходів для їхнього захисту; більшість із них знають про важливість засобів захисту особистої інформації (використання та створення паролів, двофакторної аутентифікації тощо); готові вживати заходи для захисту свого приватного життя і розуміють ризики, пов'язані з розкриттям персональних даних у соціальних мережах. Однак деякі аспекти потребують подальшого розвитку,

наприклад, здатність виявляти фішингові атаки та виявляти шкідливі посилання.

3. Визначені і обґрунтовані педагогічні умови формування навичок інформаційної безпеки в учнів 7 класів засобами інтерактивних технологій: створення сприятливого та інноваційного навчального середовища, підвищення мотивації школярів до вивчення інформаційної безпеки, а також сприяння партнерській взаємодії між викладачем та учнем

4. Розроблені методичні рекомендації щодо реалізації педагогічних умов формування навичок інформаційної безпеки в учнів 7 класів засобами інтерактивних технологій, які містять комплексні підходи та ефективні стратегії для вчителів, які дозволяють не лише ефективно передавати ключові поняття кібербезпеки, а й розвивати критичне мислення, практичні навички та самостійність учнів, і приклади сервісів інтерактивних технологій, які можуть бути успішно використані в навчальному процесі для підвищення ефективності формування навичок інформаційної безпеки.

Дослідження кваліфікаційної роботи не претендує на абсолютний результат, але поставлені завдання дослідження виконані, мету досягнуто.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авер’янова Н. М., Воропаєва Т. С. Інформаційна безпека України: соціально-філософські аспекти. *Молодий вчений,* 2020, №10 (86), С. 297-303. URL: https://doi.org/10.32839/2304-5809/2020-10-86-61 (дата звернення: 22.06.2023)

2. Бербец Т. М. Спостереження як ефективний метод педагогічного дослідження. *Вісник Українсько-туркменського культурно-освітнього центру: міждисциплінарний науковий збірник.* 2018. Вип.2, Ч. І. С. 20–26. URL: https://dspace.udpu.edu.ua/jspui/handle/6789/10413 (дата звернення: 04.10.2023)

3. Бондаренко В. І. Дистанційне навчання в Україні: стан, проблеми, перспективи. Київ : Ін-т інформ. та засобів навч. НАПН України, 2016. 164 с.

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

5. Бронетко В. О., Кудін А. П. Системи комп'ютерного тестування: огляд, аналіз, порівняння. *Збірник наукових праць Кам'янець-Подільського національного університету імені Івана Огієнка.* Серія педагогічна. 2009. №. 15. С. 16–18.

6. Бутинець, Т. А. Спостереження як основний метод наукового дослідження в контролі. *Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу.* 2016. 1(13), С. 163–174. URL: https://doi.org/10.26642/pbo-2009-1(13)-163-174 (дата звернення: 04.10.2023)

7. Вайдич Н. В. Педагогічне спостереження. *Наукові праці Міжрегіональної Академії управління персоналом. Філологія.* 2021. №2 (2). С.

5–9. URL: https://doi.org/10.32689/maup.philol.2021.2.1 (дата звернення: 04.10.2023)

8. Василенко Л. М. Психолого-педагогічні основи інтерактивної взаємодії вчителя і учнів на уроках математики. *Наукові записки [Кіровоградського державного педагогічного університету імені Володимира Винниченк*а]. *Серія: Педагогічні науки.* 2012. Вип. 109. С. 176–182. URL: http://nbuv.gov.ua/UJRN/Nz_p_2012_109_26 (дата звернення: 18.06.2023)

9. Волкова Н. П. Інтерактивні технології навчання у вищій школі: навчально-методичний посібник. Дніпро: Університет імені Альфреда Нобеля, 2018. 360 с. URL: https://ir.duan.edu.ua/handle/123456789/3218 (дата звернення: 22.06.2023)

10. Волошина, О. В. Педагогічні умови виховання толерантності у підлітків в позакласній роботі. *Modern Information Technologies and Innovation Methodologies of Education in Professional Training Methodology Theory Experience Problems.* 2021. (9), С. 116–122 URL: https://vspu.net/sit/index.php/sit/article/view/1172 (дата звернення: 22.10.2023)

11. Гайченко В. А., Коваль Г. М. Основи безпеки життєдіяльності людини: навч. посіб. 2-ге вид., стереотип. К.: МАУП, 2002. 232 с. URL: https://subject.com.ua/pdf/94.pdf (дата звернення: 18.06.2023)

12. Голубєва Н.В. Комп’ютерне тестування як одна з форм сучасного контролю знань. *Інформаційно-телекомунікаційні технології в державному управлінні: досвід, проблеми, перспективи* : зб. наукових праць. Львів : ЛДУБЖД, 2006. Вип. 1. С. 309–313. URL: http://repositsc.nuczu.edu.ua/handle/123456789/2138 (дата звернення: 04.10.2023)

13. Гончарова О.В. Рольова гра як метод формування мовленнєвих навичок студентів. *Інновації та традиції у мовній підготовці іноземних студентів* : тези доповідей міжнародного науково-практичного семінару. Х.: ХНУБА, 6 грудня 2019 р. С. 91–93.

14. Григорук П. М. Вимірювання і шкалювання даних. *Вісн. Хмельниц. нац. ун-ту. Екон. науки.* 2012. № 4, т. 2. С. 144–148.

15. Давидюк Н. Ю. Психолого-педагогічні умови розумового виховання дітей у працях в. О. Сухомлинського. *Нова педагогічна думка.* 2019. № 3, т. 3. С. 77–80. URL: https://doi.org/10.37026/2520-6427-2019-99-3-77-80 (дата звернення: 22.10.2023)

16. Дементієвська Н. П. Використання інтернет–ресурсів для навчального експерименту з курсу фізики середньої школи. *Інформаційні технології і засоби навчання. Електронне наукове фахове видання.* 2012. №. 29 т.3. URL: https://doi.org/10.33407/itlt.v29i3.692 (дата звернення: 22.06.2023)

17. Єрьоменко А. І. Вікові особливості формування навичок інформаційної безпеки підлітків. *Актуальні проблеми педагогічної науки в XXI столітті:* Матеріали III Регіональної наук.-практ. конф., 17 жовтня 2023 р. Одеса. 2023. С. 15–18.

18. Єрьоменко А. І. Інформаційна безпека підлітків в інтернет-мережі. *Педагогічна наука і освіта у сучасному вимірі: проблеми та перспективи розвитку:* Матеріали V Всеукраїнської наук.-практ. конф., 19 травня 2023 р. Одеса: видавець Букаєв Вадим Вікторович. 2023. С. 33–35.

19. Зарицька В. В. Вікові передумови розвитку емоційного інтелекту особистості (дошкільний і шкільний періоди). *Вісник Харківського національного педагогічного університету імені ГС Сковороди. Психологія.* 2011. №. 38. С. 35–53. URL: http://nbuv.gov.ua/UJRN/VKhnpu_psykhol_2011_38_6 (дата звернення: 18.06.2023)

19. Золотар, О. О. Класифікація інформаційної безпеки. *Інформація і право*. 2011. №2. С. 109–113. URL: http://nbuv.gov.ua/UJRN/Infpr_2011_2_19 (дата звернення: 18.06.2023)

21. Інноваційні технології навчання в умовах модернізації сучасної освіти : монографія / за наук. ред. д. пед. н., проф. Л. З. Ребухи. Тернопіль : ЗУНУ, 2022. 143 с.

22. Інтелектуальний розвиток дорослих у віртуальному освітньому просторі: монографія / М.Л. Смульсон, та ін. ; за ред. М. Л. Смульсон. К.: Педагогічна думка, 2015. 221 с.

23. Климнюк В. Є. Віртуальна реальність в освітньому процесі. *Збірник наукових праць Харківського національного університету Повітряних Сил.* 2018. №. 2. С. 207–212. URL: http://nbuv.gov.ua/UJRN/ZKhUPS_2018_2_30 (дата звернення: 22.06.2023)

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

25. Колісник-Гуменюк Ю. І. Інноваційні та інтерактивні технології навчання: наук. метод. Розробка. Львів: ЛННЦПО. 2018. 24 с. URL: https://enpuir.npu.edu.ua/bitstream/handle/123456789/24733/Metodychni%20Vkazivky%20Kursu%20Innovatsiini%20Ta%20Interaktyvni%20Tekhnolohii%20Navchannia.pdf?sequence=1 (дата звернення: 22.06.2023)

26. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України: дис. … д-ра юрид. наук : 12.00.07 / Одеса, 2004. 427 с.

27. Костирко Л. А. Комплексний аналіз інвестиційної привабливості підприємств в контексті фінансового забезпечення розвитку підприємств. *Фінансово-кредитна діяльність: проблеми теорії та практики.* 2018. Вип. 2. С. 198–207. URL: http://nbuv.gov.ua/UJRN/Fkd_2018_2_26 (дата звернення: 04.10.2023)

28. Коцур Н. І, Товкун Л. П., Варивода К. С. Основи безпеки життєдіяльності в загальноосвітніх навчальних закладах: навч. метод. посіб. Переяслав-Хмельницький(Київ.обл.): ФОП Домбровська Я.М., 2016. 518 с.

URL: http://ephsheir.phdpu.edu.ua/handle/8989898989/1795 (дата звернення: 18.06.2023)

29. Кравчук Г. Т., Шевчук Т. В. Симуляція як інтерактивний метод навчання майбутніх фахівців-економістів. *Физико-математическое образование.* 2019. №. 2 (20). С. 59–65. URL: http://nbuv.gov.ua/UJRN/fmo_2019_2_12 (дата звернення: 22.06.2023)

30. Кремень, В. Г. Концепція виховання дітей та молоді в цифровому просторі. / Кремень В. Г. та ін. *Вісник Національної академії педагогічних наук України.* 2022. №4(2), 30 с. URL: https://doi.org/10.37472/v.naes.2022.4206 (дата звернення: 22.10.2023)

31. Кулага І. В., Симуляції та «серйозні ігри»: досвід використання у навчальному процесі. *Університетська освіта.* 2011. №1. С. 82–88. URL: http://ivo.kneu.edu.ua/ua/education2_0/s_games_simul/ (дата звернення: 22.06.2023)

32. Кутішенко В. П. Вікова та педагогічна психологія (курс лекцій) : навч. посібник. Вид. 2-ге. Київ. 2010. 129 С. URL: https://elibrary.kubg.edu.ua/id/eprint/5696 (дата звернення: 18.06.2023)

33. Кухар Л. О., Сергієнко В. П. Конструювання тестів: навч. посіб. Луцьк, 2010. 182 с.

34. Ладивір С.О. Психолого-педагогічні умови розвитку інтелектуального потенціалу дитини. *Актуальні проблеми психології*: зб. наук. ст. 2006. Т. 4. С. 50–63.

35. Лещенко Г. В. Технології дистанційного навчання вищої школи. Харків: Основа, 2011. 304 с.

36. Литвинова С. Г. Методика використання технологій віртуального класу вчителем в організації індивідуального навчання учнів : дис. ... на здобуття наук. ступеня к-та пед. наук : 13.00.10. Київ, 2011. 219 с.

36. Лукіна Т.О. Технологія розробки анкет для моніторингових досліджень освітніх проблем. *Анотовані результати науководослідної роботи*

інституту педагогіки за 2008 рік. 2009. С. 119–121. URL: https://core.ac.uk/reader/32304920 (дата звернення: 04.10.2023)

38. Любчук В. В. Методичні аспекти формування вибірки у інтернет-дослідженнях. *Innovations technologies in science and practice*. 15–18 лютого. 2022 р. Haifa, Israel. Т. 6. С. 458–463. DOI – 10.46299/ISG.2022.I.VI. (дата звернення: 04.10.2023)

39. Методика і технології оцінювання діяльності загальноосвітнього навчального закладу: посібник. / Ляшенко О. І., Лукіна Т. О., Булах І. Є., Мруга М. Р. К. : Педагогічна думка, 2012. 160 с. URL: https://undip.org.ua/library/metodyka-i-tekhnolohii-otsiniuvannia-diialnosti-zahalnoosvitnoho-navchalnoho-zakladu-posibnyk/ (дата звернення: 04.10.2023)

40. Москаленко О. М. Авторський професійний кейс «цифрові технології у роботі вчителя математики» як дидактичний інструмент формування цифрової компетентності майбутніх учителів математики. *Освітні педагогічні науки: методологія, теорія, практика* : колективна монографія. / наук. ред. В. Фазан, В. Мокляк. Полтава : ПНПУ імені В. Г. Короленка, 2022. С. 408–426. http://elcat.pnpu.edu.ua/docs/Monografiya_2022.pdf#page=409 (дата звернення: 22.06.2023)

41. Овчарук, О.В. *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. 2020. Вип. 60. С. 90–98. URL: https://lib.iitta.gov.ua/727694/ (дата звернення: 18.06.2023)

42. Осадча К. П. Інформаційно-комунікаційні технології здійснення тьюторської діяльності у системі шкільної освіти. *Молодь і ринок.* 2016. № 8. С. 22–26. URL: http://nbuv.gov.ua/UJRN/Mir_2016_8_6 (дата звернення: 22.06.2023)

43. Основи стандартизації інформаційно-комунікаційних компетентностей в системі освіти України / Биков В. Ю. Атіка, Київ. 2010. 88 с.

44. Остапенко Л. П. Веб-квести в системі позакласної роботи з інформатики. *Наумовські читання* : матеріали XIX наук.-метод. конф. здобувачів вищої освіти та молодих учених, присвяч. року мат. освіти в Україні, Харків, 23-24 листоп. 2021. 2022. С. 204–206. URL: https://dspace.hnpu.edu.ua/handle/123456789/8106 (дата звернення: 22.06.2023)

45. Павелків Р. В. Вікова психологія. К.: Кондор. 2011. 468 с.

46. Парфілова С. Л., Заровна Ю. О. Освітній веб-квест як засіб формування читацької самостійності молодших школярів. *The II International Scientific and Practical Conference «Modern, relevant and popular research of world science»,* 04-07 жовтня, 2022, Токіо, Японія. С. 210–216. DOI: 10.46299/ISG.2022.2.2. (дата звернення: 22.06.2023)

47. Петрик В. М. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал.* 2009. № 5. С. 122–135.

48. Поляцко, К. Г. Методика оцінки оволодіння практичними навичками інтернами-хірургами на кафедрі хірургії післядипломної освіти. *Медична освіта.* 2014. №4. С. 66–68 URL: https://doi.org/10.11603/me.v0i4.2274 (дата звернення: 04.10.2023)

49. Пришляк О. Ю. Теорія і методика формування міжкультурної компетентності майбутніх фахівців соціономічних професій : дис. ... д-ра пед. наук : 13.00.04 / Тернопільський нац. пед. ун-т ім. В. Гнатюка. Тернопіль, 2021. 560 с. URL: http://dspace.tnpu.edu.ua/handle/123456789/21190 (дата звернення: 04.10.2023)

50. Семчук С. І. Використання інформаційних технологій у духовному становленні молодого покоління. *Збірник наукових праць Уманського державного педагогічного університету*. 2019. Вип. 1. С. 115–121. URL: https://doi.org/10.31499/2307-4914.1(23).2021.232748 (дата звернення: 22.10.2023)

51. Сипченко В.І. Гуманізація навчально-виховного процесу: *Збірник наукових праць. Випуск XII.* 2004. 354 с. URL: https://ddpu.edu.ua/images/naukvid/gnvp/gnvp_21.pdf#page=328 (дата звернення: 22.10.2023)

52. Сисоєва С. О. Інтерактивні технології навчання дорослих : навч.-метод. Посібник для викладачів системи формальної, неформальної та інформальної освіти дорослих. Київ, 2011. 320 с. URL: https://core.ac.uk/download/pdf/33688940.pdf (дата звернення: 22.06.2023)

53. Староста В. І., Товканець Г. В. Методологія та методи науково-педагогічних досліджень. Мукачево: МДУ, 2015. 64 с.

54. Стешиц І. В. Педагогічне партнерство як ключова компетентність вчителів-початківців нової української школи. *Наукові інновації та передові технології.* 2022. №. 8 (10). URL: https://doi.org/10.52058/2786-5274-2022-8(10)-145-155 (дата звернення: 22.10.2023)

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

56. Струтинська О. В. Особливості сучасного покоління учнів і студентів в умовах розвитку цифрового суспільства. *Електронне наукове фахове видання "ВІДКРИТЕ ОСВІТНЄ Е-СЕРЕДОВИЩЕ СУЧАСНОГО УНІВЕРСИТЕТУ".* 2020. №. 9. С. 145–160. URL: https://doi.org/10.28925/2414-0325.2020.9.12 (дата звернення: 18.06.2023)

57. Трач Ю. В. VR-технології як метод і засіб навчання. *Освітологічний дискурс.* 2017. №. 3-4. С. 309–322. URL: https://doi.org/10.28925/2312-5829.2017.3-4.3932 (дата звернення:)

58. Федірчик Т. Д. Педагогіка партнерства як чинник формування ефективної взаємодії учасників освітнього процесу в умовах Нової української школи. *Гірська школа Українських Карпат.* 2019. № 21. С. 50–54 URL: http://lib.pnu.edu.ua:8080/handle/123456789/8575 (дата звернення: 22.10.2023)

58. Цимбалюк С. О. Оцінювання персоналу : навч. посіб. Київ : КНЕУ, 2021. 311 с. URL: https://ir.kneu.edu.ua:443/handle/2010/35638 (дата звернення: 04.10.2023)

60. Чала О. М. Використання інноваційних підходів та інтерактивних технологій на уроках української мови та літератури. *Сучасний освітній простір – досвід, пошук, результат*: матеріали І Всеукраїнської науково-практичної інтернет-конференції, 29 серпня 2023 року. Суми. С. 38–40.

61. Чмиленко Ф. О. Посібник до вивчення дисципліни «Методологія та організація наукових досліджень. Дніпропетровськ : РВВ ДНУ, 2014. 48 с. URL: https://library.megu.edu.ua:9443/jspui/handle/123456789/2510 (дата звернення: 04.10.2023)

62. Шугайло Я. В. Соціально-педагогічні умови зменшення негативних наслідків впливу ЗМІ на соціалізацію підлітків. *Вісник Запорізького національного університету. Педагогічні науки.* 2010. № 1(12). С. 244–252. URL: https://web.znu.edu.ua/herald/issues/2010/2010-ped-1.pdf#page=244 (дата звернення: 22.10.2023)

63. Що таке Kahoot! і чому його варто спробувати для організації дистанційного навчання. *BUKI:* веб-сайт. URL: https://buki.com.ua/news/shchotake-kahoot-i-chomu-yoho-varto-sprobuvaty-dlya-orhanizatsiyi-dystantsiynohonavchannya/ (дата звернення: 22.06.2023)

64. Ягоднікова В. В. Теорія і практика формування інноваційної спрямованості виховного процесу загальноосвітньої школи : дис. на здобуття наук. ступеня д-ра пед. наук : 13.00.07 / Одеса, 2016. 526 с. URL: https://vspu.edu.ua/content/specialized_academic_council/doc/2016/Yahodnikova_V/dis.pdf (дата звернення: 22.10.2023)

65. Bitner N., Bitner J. Integrating Technology into the Classroom: Eight Keys to Success. *Journal of Technology and Teacher Education*, 2002. 10(1). P. 95–100. URL: https://www.learntechlib.org/primary/p/9304/ (дата звернення: 22.10.2023)

66. Buzan B. New Patterns of Global Security in the Twenty-First Century. *International Affairs (Royal Institute of International Affairs 1944-).* 1991. Vol. 67, No. 3. P. 431–451.

67. Changeux J.-P. The Challenge of Development: Theory and Practice in Human Resource Management. Routledge, 2017. URL: https://doi.org/10.4324/9781315131177 (дата звернення: 18.06.2023)

68. Cohen-Hatton, S. R., Honey, R. C. Goal-oriented training affects decision-making processes in virtual and simulated fire and rescue environments. *Journal of Experimental Psychology: Applied.* 2015. 21(4). P. 395–406. URL: https://doi.org/10.1037/xap0000061 (дата звернення: 22.06.2023)

69. Deci E. L., Koestner R., Ryan R. M. A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation. *Psychological bulletin*. 1999. T. 125. №. 6. 627 p.

70. Dempsey J. V. Interactive instruction and feedback. Educational Techology Publications, Inc., Englewood Cliffs, New Jersey, 1993. 384 p.

71. Ferguson N., Schneier B. Practical Cryptography. Wiley Publishing , Inc., Indianapolis, Indiana, 2003. 432 p.

72. Gagne R. M. The conditions of learning. Holt, Rinehart and Winston, 1970. 407 p.

73. Gee J. P. Learning and games. Chicago, IL : MacArthur Foundation Digital Media and Learning Initiative, 2008. P. 21–40. URL: https://www.issuelab.org/resources/861/861.pdf (дата звернення: 22.06.2023)

74. Howie S., Gilardi M. Virtual Observations: a software tool for contextual observation and assessment of user's actions in virtual reality. *Virtual Reality 25*. 2021. P. 447–460. URL: https://doi.org/10.1007/s10055-020-00463-5 (дата звернення: 22.06.2023)

75. Hwang G. J., Hung C. M., Chen N. S. Improving learning achievements, motivations and problem-solving skills through a peer assessment-based game development approach. *Education Tech Research Dev 62*. 2014. P. 129–

145 (2014). URL: https://doi.org/10.1007/s11423-013-9320-7 (дата звернення: 22.10.2023)

76. Kolb D. A. Experiential Learning: Experience as the Source of Learning and Development. New Jersey: FT Press, 2014. 390 p.

77. Lopes P. N., Salovey P. Toward a broader education: Social, emotional, and practical skills. *Building academic success on social and emotional learning: What does the research say*. New York: Teachers College Press, 2004. P. 76–93. URL: https://www.academia.edu/download/59807495/Toward_a_Broader_Education_Social_Emotio20190620-19554-uautzz.pdf (дата звернення: 18.06.2023)

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

79. Maslow A., Lewis K. J. Maslow's hierarchy of need. *Salenger Incorporated,* 1987. №17(13) T. 14. P. 987–990.

80. Mayer R. E. Multimedia learning. *Psychology of learning and motivation.* Academic Press, 2002. T. 41. P. 85–139. URL: https://doi.org/10.1016/S0079-7421(02)80005-6 (дата звернення: 22.06.2023)

81. McBrien J. L., Cheng R., Jones P. Virtual spaces: Employing a synchronous online classroom to facilitate student engagement in online learning. *International review of research in open and distributed learning.* 2009. T. 10. №. 3. URL: https://doi.org/10.19173/irrodl.v10i3.605 (дата звернення: 22.06.2023)

82. Revere L., Kovach J. V. Online technologies for engaged learning. A Meaningful Synthesis for Educators. *Quarterly Review of Distance Education.* 2011. T. 12. №. 2. URL https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5057da57b469a5133f7b5f375a9c2e7cb4ba3ea8 (дата звернення: 22.06.2023)

83. Rogers C. Freedom to Learn. Columbus, Ohio: Merill, 1969. 358 p.

84. Šilonová V. et al. Застосування цифрових технологій у дистанційному педагогічному оцінюванні здобувачів вищої освіти. *Information Technologies and Learning Tools.* 2021. Т. 82. №. 2. С. 243–265.

85. Skinner B. Science and Human Behavior. *Appleton-Century-Crofts,* New York, USA, 1990. 341 p.

86. Vlasii O. O., Dudka O. M., Stefanyshyn M. V. Інтерактивні технології як засіб підвищення ефективності навчання. *Mountain School of Ukrainian Carpaty.* 2020. №. 23. P. 128–132. URL: https://doi.org/10.15330/msuc.2020.23.128-132 (дата звернення: 18.06.2023)

87. Worobjowa T. V. Розвиток критичного мислення та креативності методом побудови асоціативних мап (майндмеппінг). *KELM (Knowledge, Education, Law, and Management).* 2013. Т. 2. №. 2. P. 50–63. URL: https://www.ceeol.com/search/article-detail?id=622272 (дата звернення: 18.06.2023)

ДОДАТКИ

Додаток А

Перелік питань опитування

Навички інформаційної безпеки учнів 7-х класів

Форма складається з кількох розділів, які стосуються різних аспектів безпеки, а саме:
Розділ 1. Знання та практика створення та використання надійних паролів
Розділ 2. Виявлення шкідливих програм
Розділ 3. Розпізнавання та уникнення онлайн-шахрайства, фішингу та кібербулінгу
Розділ 4. Використання соціальних мереж
Розділ 5. Позиція учнів щодо різних аспектів безпеки
Розділ 6. Збереження приватності особистої інформації

Розділ 1. Знання та практика створення та використання надійних паролів

1. Як часто Ви використовуєте Інтернет?*
- a) Щоденно
- b) Кілька разів на тиждень
- c) Рідко
- d) Ніколи

2. Ви знаєте, що таке пароль і для чого він потрібен?*
- a) Так
- b) Ні

3. Чи використовуєте ви один і той самий пароль для кількох різних сервісів (пошта, соціальні мережі, інтернет-магазини і т. д.)?*
- a) Так
- b) Ні

4. Як ви обираєте паролі для своїх облікових записів?*
- a) Вигадую міцні паролі, які складаються з комбінації великих і малих літер, цифр та символів, і вони є унікальними для кожного облікового запису.
- b) Використовую слабкі паролі, які легко запам'ятовую, оскільки це зручно для мене.
- c) Використовую однаковий пароль для багатьох облікових записів, щоб не забути їх.
- d) Використовую менеджери паролів, які генерують та зберігають складні паролі для мене

5. Як ви зберігаєте свої паролі? (Наприклад, папка на комп'ютері, записую на папері, використовуєте менеджери паролів тощо.)*
- a) Зберігаю в папці на комп'ютері
- b) Записую на папері
- c) Використовую менеджер паролів
- d) Запам'ятовую

6. Чи використовуєте ви двофакторну аутентифікацію (2FA) для захисту своїх облікових записів? (Наприклад, коди з SMS або додатки для генерації кодів.)*
- a) Так
- b) Ні

7. Чи змінюєте ви паролі регулярно? Як часто?*
- a) Так. Раз на рік
- b) Так. Що частіше, то краще
- c) Так. Коли є підозра, що хтось дізнався мій пароль
- d) Не змінюю

8. Якщо ви втратили доступ до свого облікового запису через незаконний доступ чи забули пароль, як ви відновлюєте доступ?*

a) Використовую сервіс відновлення паролю на сайті та змінюю пароль на новий
b) Створюю новий обліковий запис
c) Інше:

9. Чи ділитеся Ви своїми паролями з кимось?*

a) Ділюсь із батьками
b) Ділюсь із друзями
c) Не ділюсь паролями ні з ким

Розділ 2. Виявлення шкідливих програм

1. Що таке антивірусна програма і для чого вона призначена? *

a) Для створення вірусів
b) Для захисту комп'ютера від шкідливих програм
c) Для створення резервних копій файлів

2. Які можливі наслідки можуть виникнути, якщо ваш комп'ютер заразиться вірусами або шкідливими програмами? *

a) Видаляться всі файли на комп'ютері
b) Комп'ютер стане швидше
c) Втрата даних, збільшення ризику крадіжки особистої інформації

3. Які ознаки можуть свідчити про те, що комп'ютер може бути заражений шкідливим програмним забезпеченням? Виберіть всі відповіді, які вам відомі. *

a) Повільна робота комп'ютера
b) Зникнення антивірусного програмного забезпечення
c) Вискачуть повідомлення про викуп

4. Як можна захистити свій комп'ютер від шкідливих програм? Виберіть всі відповіді, які вам відомі. *

a) Регулярно оновлювати антивірусне програмне забезпечення
b) Відкривати всі електронні листи з невідомих джерел
c) Завжди завантажувати програми з офіційних джерел

5. Що таке "фішинг"? *

a) Вид риболовлі
b) Спроба шахрайства, коли атакуюча сторона намагається видалити вашу інформацію
c) Забій риби

6. Як ви визначите, що електронний лист, який ви отримали, є спробою фішингу?*

a) Я завжди відкриваю всі листи
b) Завжди перевіряю адресу відправника та текст повідомлення
c) Відкриваю вкладені файли без перевірки

7. Що робити, якщо ви підозрюєте, що ваш комп'ютер заражений шкідливою програмою? *

a) Ігнорувати це
b) Поставити антивірусну програму
c) Замінити комп'ютер

8. Які дії ви виконаєте, якщо вам зателефонував невідома людина і намагається отримати ваші персональні дані? (оберіть один варіант відповіді)*

a) Подати всі дані
b) Повідомити батькам або вчителям
c) Повісити слухавку

9. Як вибрати надійний пароль для облікового запису в інтернеті? *

a) Використовувати простий пароль, щоб легше його запам'ятати
b) Використовувати довгий пароль з буквами, цифрами та спеціальними символами

c) Використовувати один і той самий пароль для всіх облікових записів

10. Що таке двофакторна аутентифікація і як вона допомагає збільшити безпеку облікового запису? *

a) Це страховка для автомобіля

b) Це захист, коли потрібно ввести два паролі

c) Це процедура, під час якої для входу потрібно ввести не тільки пароль, а й інший код, який надсилається на ваш мобільний телефон або інший пристрій.

Розділ 3. Розпізнавання та уникнення онлайн-шахрайства, фішингу та кібербулінгу

1. Я завжди розпізнаю спроби фішингу та шахрайства в інтернеті.*

- ○ Повністю не погоджуюся
- ○ Трохи не погоджуюся
- ○ Не визначаються
- ○ Трохи погоджуюся
- ○ Повністю погоджуюся

2. Я відчуваю себе впевнено у захисті своєї особистої інформації в інтернеті.*

- ○ Повністю не погоджуюся
- ○ Трохи не погоджуюся
- ○ Не визначаються
- ○ Трохи погоджуюся
- ○ Повністю погоджуюся

3. Я завжди реагую на випадки кібербулінгу та шахрайства в мережі та шукаю допомогу в дорослих.*

- ○ Повністю не погоджуюся
- ○ Трохи не погоджуюся
- ○ Не визначаються
- ○ Трохи погоджуюся
- ○ Повністю погоджуюся

4. Я завжди перевіряю ланки в поштових повідомленнях та веб-сайтах, переконуючись, що вони безпечні перед тим, як натискати на них.*

- ○ Повністю не погоджуюся
- ○ Трохи не погоджуюся
- ○ Не визначаються
- ○ Трохи погоджуюся
- ○ Повністю погоджуюся

5. Я завжди підтримую добрий інтернет-етикет та поважаю інших у мережі.*

- ○ Повністю не погоджуюся
- ○ Трохи не погоджуюся
- ○ Не визначаються
- ○ Трохи погоджуюся
- ○ Повністю погоджуюся

6. Я регулярно перевіряю наявність "https://" у веб-сайтах, які відвідую, та переконуюся, що вони безпечні.*

- ○ Повністю не погоджуюся
- ○ Трохи не погоджуюся
- ○ Не визначаються
- ○ Трохи погоджуюся
- ○ Повністю погоджуюся

7. Я завжди ретельно розглядаю запити в друзі та повідомлення від незнайомих осіб в соціальних мережах та месенджерах.*

- ○ Повністю не погоджуюся
- ○ Трохи не погоджуюся
- ○ Не визначаються

- Трохи погоджуюся
- Повністю погоджуюся

8. Я завжди стежу за змінами в поведінці онлайн і намагаюся розпізнавати випадки кібербулінгу та намагаюся допомогти постраждалим.*

- Повністю не погоджуюся
- Трохи не погоджуюся
- Не визначаються
- Трохи погоджуюся
- Повністю погоджуюся

9. Я завжди ретельно досліджую веб-сайти, перш ніж надавати особисту інформацію або виконувати оплату в інтернеті.*

- Повністю не погоджуюся
- Трохи не погоджуюся
- Не визначаються
- Трохи погоджуюся
- Повністю погоджуюся

10. Я завжди ретельно перевіряю поштові повідомлення із сумнівними запитами або лінками, перш ніж натискати на них.*

- Повністю не погоджуюся
- Трохи не погоджуюся
- Не визначаються
- Трохи погоджуюся
- Повністю погоджуюся

Розділ 4. Використання соціальних мереж

1. Оцініть свою відповідальність щодо використання соціальних мереж на шкалі від 1 (зовсім не відповідальний) до 5 (дуже відповідальний).*

Не відповідальний
1
2
3
4
5
Дуже відповідальний

2. Наскільки ви впевнені у своїх навичках забезпечення безпеки під час використання соціальних мереж? Оцініть себе на шкалі від 1 (незнаючий) до 5 (дуже обізнаний).*

Незнаючий
1
2
3
4
5
Дуже обізнаний

3. Наскільки ви ознайомлені з правилами та політикою використання соціальних мереж, зокрема щодо конфіденційності, вікових обмежень та захисту від шахрайства? Використовуйте шкалу від 1 (незнаючий) до 5 (дуже обізнаний).*

Незнаючий
1
2
3
4
5

Дуже обізнаний

4. Як часто ви перевіряєте час, який витрачаєте на соціальних мережах? Оцініть це на шкалі від 1 (рідко) до 5 (дуже часто).*

Рідко
1
2
3
4
5
Дуже часто

5. Оцініть своє ставлення до взаємодії з іншими користувачами соціальних мереж. Використовуйте шкалу від 1 (конфліктний) до 5 (дружелюбний та поважаючий інших).*

Конфліктний
1
2
3
4
5
Дружелюбний та поважаючий інших

6. Як ви ставитеся до розкриття особистої інформації в соціальних мережах? Оцініть це на шкалі від 1 (дуже легковажно) до 5 (дуже обережно).*

Дуже легковажно
1
2
3
4
5
Дуже обережно

7. Як часто ви обговорюєте свою діяльність в соціальних мережах з батьками або вчителями? Використовуйте шкалу від 1 (зовсім не обговорюю) до 5 (часто обговорюю).*

Зовсім не обговорюю
1
2
3
4
5
Часто обговорюю

8. Звідки ви отримуєте інформацію про безпеку та відповідальне використання соціальних мереж? Використовуйте шкалу від 1 (не отримую інформацію) до 5 (отримую інформацію від різних джерел).*

Не отримую інформацію
1
2
3
4
5
Отримую інформацію від різних джерел

9. Наскільки ви готові навчатися і вдосконалювати свої навички в безпечному використанні соціальних мереж? Використовуйте шкалу від 1 (не готовий) до 5 (дуже готовий).*

Не готовий
1
2
3

4
5
Дуже готовий

10. Як багато ви цінуєте можливості соціальних мереж та розумієте їхню важливість у вашому житті? Використовуйте шкалу від 1 (не ціную) до 5 (дуже ціную).*

Не ціную
1
2
3
4
5
Дуже ціную

Розділ 5. Позиція учнів щодо різних аспектів безпеки

1. Оцініть свою свідомість про основні загрози в Інтернеті (від 1 до 5, де 1 – низька свідомість, 5 – висока свідомість).*

Низька свідомість
1
2
3
4
5
Висока свідомість

2. Як ви оцінюєте свої навички створення та керування сильними паролями (від 1 до 5, де 1 – слабкі навички, 5 – відмінні навички).*

Низькі навички
1
2
3
4
5
Слабкі навички

3. Оцініть свій рівень використання антивірусного програмного забезпечення на пристроях (від 1 до 5, де 1 – не використовую, 5 – завжди використовую).*

Не використовую
1
2
3
4
5
Завжди використовую

4. Як часто ви оновлюєте програми та операційну систему на своєму комп'ютері чи смартфоні (від 1 до 5, де 1 – рідко оновлюю, 5 – завжди оновлюю).*

Не оновлюю
1
2
3
4
5
Завжди оновлюю

5. Оцініть свій рівень обізнаності щодо фішингових атак та способів їх виявлення (від 1 до 5, де 1 – мало обізнаний, 5 – дуже обізнаний).*

Незнаючий
1
2

3
4
5
Дуже обізнаний

6. Як часто ви робите резервні копії важливих даних (від 1 до 5, де 1 – рідко, 5 – щоденно).*

Ніколи
1
2
3
4
5
Щоденно

7. Оцініть свою здатність розпізнавати небезпечні посилання та вкладені файли у електронних листах чи повідомленнях (від 1 до 5, де 1 – погано розпізнаю, 5 – добре розпізнаю).*

Не вмію розпізнавати
1
2
3
4
5
Завжди розпізнаю

8. Як часто ви використовуєте двофакторну аутентифікацію для захисту своїх облікових записів (від 1 до 5, де 1 – не використовую, 5 – завжди використовую).*

Не використовую
1
2
3
4
5
Завжди використовую

9. Оцініть свою готовність ділитися випадковою інформацією в соціальних мережах та месенджерах (від 1 до 5, де 1 – готовий ділитися, 5 – обережний у розповсюджені інформації).*

Ділюсь з усіма
1
2
3
4
5
Не ділюсь ні з ким

10. Як ви оцінюєте свій рівень обізнаності щодо кібербулінгу та засобів захисту від нього (від 1 до 5, де 1 – мало обізнаний, 5 – дуже обізнаний).*

Незнаючий
1
2
3
4
5
Дуже обізнаний

Розділ 6. Збереження приватності особистої інформації

1. Чи ставите ви усвідомлено до надання своїх особистих даних (ім'я, прізвище, адреса тощо) в Інтернеті?*

a) Так
b) Ні

2. Як ви оцінюєте важливість захисту ваших особистих даних в Інтернеті на шкалі від 1 (не важливо) до 5 (дуже важливо)?*

a) Мої особисті дані в Інтернеті не є важливими
b) Мої особисті дані в Інтернеті мають певну важливість
c) Мої особисті дані в Інтернеті є дуже важливими

3. Які заходи безпеки ви вживаєте для захисту своїх особистих даних в Інтернеті? (Можете обрати декілька варіантів)*

a) Використання сильних паролів
b) Використання антивірусного програмного забезпечення
c) Двофакторна аутентифікація
d) Не ділитися особистими даними з незнайомцями
e) Перевірка налаштувань конфіденційності на соціальних мережах

4. Чи робите ви резервні копії важливих даних (фотографії, документи тощо) для збереження інформації в разі її втрати?*

a) Так
b) Ні

5. Чи розумієте ви ризики, пов'язані з розкриттям особистих даних в соціальних мережах, і приймаєте заходи для їх обмеження?*

a) Так
b) Ні

6. Чи обговорюєте ви питання приватності в Інтернеті з батьками або дорослими?*

a) Так
b) Ні

7. Як ви реагуєте на запити про особисті дані в Інтернеті, наприклад, під час реєстрації на сайті чи завантаження додатку?*

a) Вказую точну інформацію
b) Вказую мінімальну необхідну інформацію
c) Знаходжу альтернативи для уникнення надання особистих даних

8. Чи використовуєте ви "приватний режим" (інкогніто) в браузері для перегляду чутливих або особистих матеріалів в Інтернеті*

a) Так
b) Ні
c) Не переглядаю такі матеріали

9. Як ви визначаєте довіру до веб-сайтів чи додатків, які збирають особисті дані?*

a) Перевіряю рейтинг та відгуки інших користувачів
b) Звертаю увагу на наявність HTTPS-з'єднання
c) Використовую додатковий програмний засіб для блокування відстежування
d) Інше:

10. Як ви відноситесь до надання доступу до своєї геолокації додаткам та сайтам?*

a) Ніколи не надаю доступ до своєї геологації
b) Надаю доступ до геолокації тільки довіреним сайтам та додаткам
c) Надаю доступ до геолокації всім сайтам та додаткам

Додаток Б

Перелік питань тестування

1 1 з 33

Частина 1. Парольний захист

Частина 1. Парольний захист

1. Як часто ви змінюєте свої паролі до облікових записів в Інтернеті?

- Раз на місяць або частіше.
- Раз на півроку
- Рідко або ніколи
- Не знаю, як це роботи

2 2 з 33

Частина 1. Парольний захист

Частина 1. Парольний захист

2. Як ви оцінюєте складність ваших паролів?

- Вони прості і легко запам'ятовуються
- Вони складніші, але можливо запам'ятати
- Вони складні та унікальні для кожного облікового запису

3 3 з 33

Частина 1. Парольний захист

Частина 1. Парольний захист

3. Яка дія є безпечною під час вибору паролю?

- Використовувати простий пароль, щоб його легко запам'ятати
- Використовувати один і той же пароль для всіх облікових записів
- Використовувати унікальний та складний пароль для кожного облікового запису

4 4 з 33

Частина 1. Парольний захист

Частина 1. Парольний захист

4. Чи використовуєте ви двоетапну аутентифікацію (наприклад, SMS-коди або додаткові паролі) для своїх облікових записів?

- Ні, ніколи
- Інколи, для деяких важливих облікових записів
- Так, для більшості облікових записів

5 5 з 33

Частина 2. Противірусний захист

Частина 2. Противірусний захист

1. Чи встановлений на вашому комп'ютері антивірусний програмний продукт?

- Ні, не встановлений
- Так, але рідко оновлюється
- Так, і регулярно оновлюється

6 6 з 33

Частина 2. Противірусний захист

Частина 2. Противірусний захист

2. Якщо ваш антивірус виявить потенційно небезпечний файл, як ви реагуєте?

- Відкриваю файл без перевірки
- Відправляю файл у карантин і звертаюся до допомоги батьків
- Видаляю файл і повідомляю про це антивірусному програмному продукту

7 7 з 33

Частина 2. Противірусний захист

Частина 2. Противірусний захист

3. Чому важливо регулярно оновлювати програмне забезпечення і пристрої (наприклад, операційну систему та антивірус)?

- Для того щоб зробити пристрої швидшими
- Для покращення зовнішнього вигляду.
- Для заповнення дірок у безпеці і захисту від нових загроз

8 8 з 33

Частина 3. Програмний захист

Частина 3. Програмний захист

1. Чи завжди оновлюєте ви програми на своєму комп'ютері або мобільних пристроях?

- Ні, ніколи
- Так, якщо є час і бажання
- Так, якомога швидше після виходу оновлень

9 9 з 33

Частина 3. Програмний захист

Частина 3. Програмний захист

2. Як ви відноситесь до використання програмного забезпечення з відкритим вихідним кодом?

- Не розумію, що це
- Використовую іноді, якщо підходить
- Використовую і підтримую відкритий вихідний код

10 10 з 33

Частина 3. Програмний захист

Частина 3. Програмний захист

3. Чи можна довіряти додаткам із невідомих джерел, які пропонують безкоштовні версії платних додатків?

- Так, завжди можна довіряти.
- Так, якщо вони запитують лише основні дозволи.
- Ні, це може бути ризиковано, інколи це можуть бути шкідливі додатки

11 11 з 33

Частина 3. Програмний захист

Частина 3. Програмний захист

4. Чому важливо завантажувати додатки лише з офіційних джерел (наприклад, App Store або Google Play Store)?

- Додатки з офіційних джерел завжди безкоштовні.
- Додатки з офіційних джерел часто перевіряються на наявність шкідливого коду.
- Інші джерела завжди надають нові версії додатків

12 12 з 33

Частина 4. Захист від фішингу

Частина 4. Захист від фішингу

1. Як ви реагуєте на надходження сумнівних листів або повідомлень, які запитують особисту інформацію?

- Надсилаю особисту інформацію без перевірки
- Запитую батьків або вчителів, чи це безпечно
- Ігнорую або видаляю такі листи без надання інформації

13 13 з 33

Частина 4. Захист від фішингу

Частина 4. Захист від фішингу

2. Які дії слід виконати, якщо ви отримали спамове повідомлення або електронний лист з підозрілим вмістом?

- Відкрити вміст і перевірити, що там написано
- Видалити повідомлення або електронний лист без відкривання
- Відповісти на повідомлення і попросити видалити вашу адресу зі списку розсилки

14 14 з 33

Частина 4. Захист від фішингу

Частина 4. Захист від фішингу

3. Якщо ви отримаєте дуже цікавий лист або пропозицію в Інтернеті, яка здається занадто хорошою, щоб бути правдою, то що ви зробите?

- Запитаю поради у дорослих або вчителів
- Зареєструюся на цьому сайті із своєю особистою інформацією
- Видалю лист або повідомлення без думок

15 15 з 33

Частина 5. Захист від кібербулінгу

Частина 5. Захист від кібербулінгу

1. Що таке кібербулінг?

- Використання Інтернету для пошуку інформації
- Агресивна, образлива або загрожлива поведінка в Інтернеті з наміром завдати шкоди іншим людям
- Спільна робота над інтернет-проектами

16 16 з 33

Частина 5. Захист від кібербулінгу

Частина 5. Захист від кібербулінгу

2. Як ви реагуєте на образливі або загрожувальні повідомлення в Інтернеті

- Відповідаю образливим чи загрожувальним повідомленням
- Повідомляю батьків, вчителів або адміністраторів сайту
- Ігнорую або блокую особу, яка надсилає образливі повідомлення

17 17 з 33

Частина 5. Захист від кібербулінгу

Частина 5. Захист від кібербулінгу

3. Якщо ви бачите, що когось ображають або загрожують в Інтернеті, як ви реагуєте?

- Повідомлю вчителя або батьків про це
- Проігнорую це і не втручаюся
- Долучусь і також почну ображати

18 18 з 33

Частина 6. Захист при роботі в Інтернеті та соціальних мережах

Частина 6. Захист при роботі в Інтернеті та соціальних мережах

1. Як часто ви перевіряєте налаштування приватності на своїх соціальних мережах?

- Регулярно і вношу зміни, якщо потрібно
- Час від часу
- Ніколи не роблю цього

19 19 з 33

Частина 6. Захист при роботі в Інтернеті та соціальних мережах

Частина 6. Захист при роботі в Інтернеті та соціальних мережах

2. Яка інформація НЕ повинна бути розміщена у публічних профілях соціальних мереж?

- Повне ім'я та дата народження
- Улюблені фільми і музика
- Адреса місця проживання

20 20 з 33

Частина 6. Захист при роботі в Інтернеті та соціальних мережах

Частина 6. Захист при роботі в Інтернеті та соціальних мережах

3. Чи ділитеся ви особистою інформацією (наприклад, номером телефону чи адресою) у відкритих чатах чи на соціальних мережах?

- Ніколи
- Тільки зі своїми друзями
- З будь-ким, хто попросить

21 21 з 33

Частина 6. Захист при роботі в Інтернеті та соціальних мережах

Частина 6. Захист при роботі в Інтернеті та соціальних мережах

4. Як ви визначаєте довіру до веб-сайтів, які збирають особисті дані?

- Перевіряю рейтинг та відгуки інших користувачів
- Не перевіряю нічого і відразу надаю інформацію
- Довіряю всім веб-сайтам.

22 22 з 33

Частина 7. Організаційний захист

Частина 7. Організаційний захист

1. Чи знаєте ви правила користування комп'ютерами та Інтернетом у вашій школі?

- Так і дотримуюся їх.
- Так, але ігнорую
- Ні, не знаю

23 23 з 33

Частина 7. Організаційний захист

Частина 7. Організаційний захист

2. Чи часто ви берете участь у тренінгах чи навчанні щодо інформаційної безпеки?

- Ніколи
- Декілька разів на рік
- Регулярно

24 24 з 33

Частина 7. Організаційний захист

Частина 7. Організаційний захист

3. Як ви відноситесь до власної відповідальності за свою інформаційну безпеку в Інтернеті?

- Інші повинні дбати про мою безпеку
- Думаю, що це моя відповідальність разом із підтримкою батьків та вчителів

Розумію, що я сам відповідальний і повинен дотримуватися правил інформаційної безпеки

25 25 з 33

Частина 7. Організаційний захист

Частина 7. Організаційний захист

4. Чи допомагаєте ви своїм друзям або родині захищати їхню інформаційну безпеку?

- Ні, це не моя справа
- Так, допомагаю їм встановлювати паролі і надавати поради з безпеки
- Вони ніколи не питають мене про це

26 26 з 33

Частина 8 . Використання мобільних пристроїв

Частина 8 . Використання мобільних пристроїв

1. Як ви захищаєте свій мобільний пристрій (смартфон, планшет) від несанкціонованого доступу?

- Встановлюю пароль або відбиток пальця із PIN-кодом
- Використовую простий пароль
- Не захищаю взагалі.

27 27 з 33

Частина 8 . Використання мобільних пристроїв

Частина 8 . Використання мобільних пристроїв

2. Чому важливо встановлювати пароль або використовувати біометричну аутентифікацію на мобільних пристроях?

- Щоб ускладнити іншим користувачам
- Щоб заблокувати доступ до особистої інформації у випадку втрати пристрою
- Щоб прискорити роботу пристрою

28 28 з 33

Частина 8 . Використання мобільних пристроїв

Частина 8 . Використання мобільних пристроїв

3. Якщо ваш мобільний пристрій вимагає оновлення операційної системи, коли це краще робити?

- Якщо у вас є час і бажання.
- Якщо це не заважає поточним діям, виконуйте оновлення якомога швидше

  Це не важливо, оновлення не впливають на безпеку

29 29 з 33

Частина 9. Захист особистої інформації

Частина 9. Захист особистої інформації

1. Як ви ставитеся до надання своїх особистих даних в Інтернеті (наприклад, ім'я, адреса, номер телефону)?

- Ніколи не надаю таку інформацію
- Надаю, якщо це потрібно для реєстрації на сайтах
- Надаю без думок

30 30 з 33

Частина 9. Захист особистої інформації

Частина 9. Захист особистої інформації

2. Як ви зберігаєте особисті документи або файли на вашому комп'ютері?

- Зашифровую їх або зберігаю на захищеному диску
- Просто зберігаю на комп'ютері
- Не зберігаю нічого особистого

31 31 з 33

Частина 9. Захист особистої інформації

Частина 9. Захист особистої інформації

3. Якщо незнайома особа запитує вас про особисту інформацію в Інтернеті, що ви робите?

- Надаю всю необхідну інформацію
- Не розголошую особисту інформацію і повідомляю батькам чи вчителю
- Надаю неправдиву інформацію для веселощів.

32 32 з 33

Частина 9. Захист особистої інформації

Частина 9. Захист особистої інформації

4. Чому важливо обмежувати кількість особистої інформації, яку ви розміщуєте в Інтернеті?

- Більше інформації – краще.
- Щоб запобігти можливому зловживанню інформацією і захистити свою приватність

Це не має значення, інтернет – це вільна площина

Додаток В

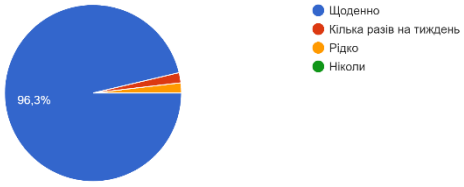
Результати опитування учнів 7-х класів

Запитання, на які часто відповідають неправильно

Запитання	Правильні відповіді
3. Які ознаки можуть свідчити про те, що комп'ютер може бути заражений шкідливим програмним забезпеченням? Виберіть всі відповіді, які вам відомі.	12/54
8. Які дії ви виконаєте, якщо вам зателефонував невідома людина і намагається отримати ваші персональні дані? (оберіть один варіант відповіді)	2/54

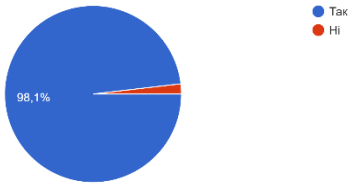
1. Як часто Ви використовуєте Інтернет?

54 відповіді



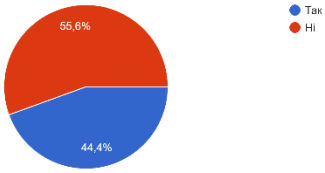
2. Ви знаєте, що таке пароль і для чого він потрібен?

54 відповіді



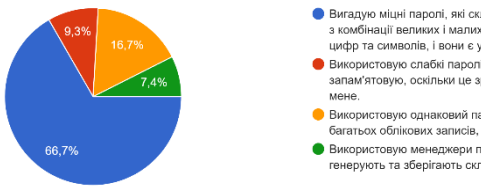
3. Чи використовуєте ви один і той самий пароль для кількох різних сервісів (пошта, соціальні мережі, інтернет-магазини і т. д.)?

54 відповіді



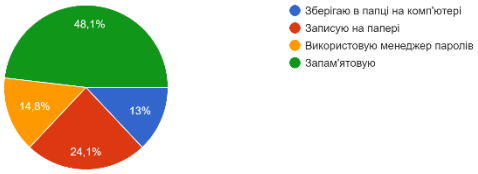
4. Як ви обираєте паролі для своїх облікових записів?

54 відповіді



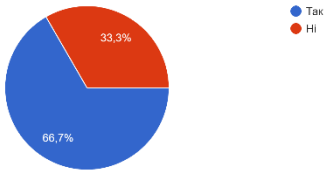
5. Як ви зберігаєте свої паролі? (Наприклад, папка на комп'ютері, записую на папері, використовуєте менеджери паролів тощо.)

54 відповіді



6. Чи використовуєте ви двофакторну аутентифікацію (2FA) для захисту своїх облікових записів? (Наприклад, коди з SMS або додатки для генерації кодів.)

54 відповіді



7. Чи змінюєте ви паролі регулярно? Як часто?

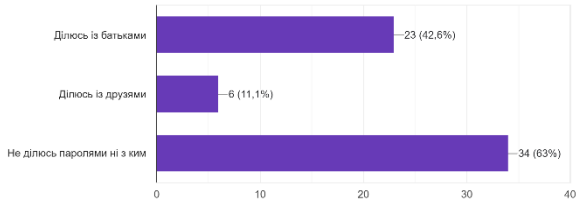
54 відповіді

8. Якщо ви втратили доступ до свого облікового запису через незаконний доступ чи забули пароль, як ви відновлюєте доступ?

54 відповіді

9. Чи ділитеся Ви своїми паролями з кимось?

54 відповіді

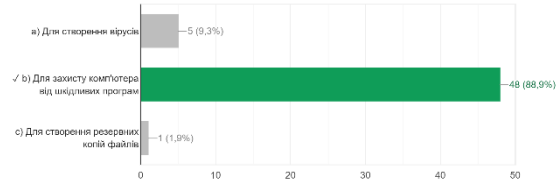


10. Якщо ви знаєте когось, хто стикався з проблемами безпеки через використання слабких паролів, будь ласка, поділіться цим досвідом.

54 відповіді

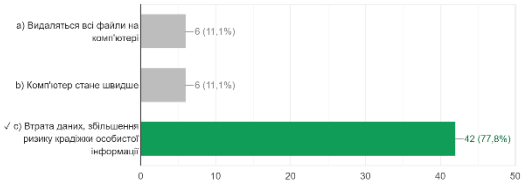
1. Що таке антивірусна програма і для чого вона призначена?

48 правильні відповіді з 54



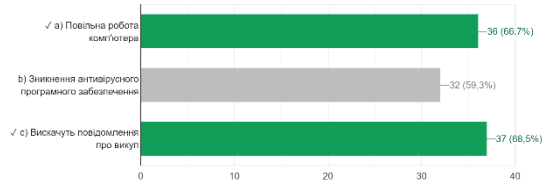
2. Які можливі наслідки можуть виникнути, якщо ваш комп'ютер заразиться вірусами або шкідливими програмами?

42 правильні відповіді з 54



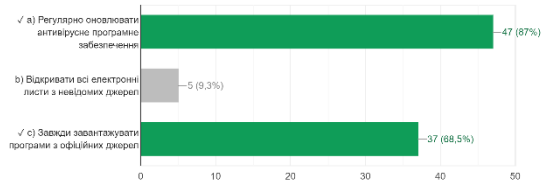
3. Які ознаки можуть свідчити про те, що комп'ютер може бути заражений шкідливим програмним забезпеченням? Виберіть всі відповіді, які вам відомі.

12 правильні відповіді з 54



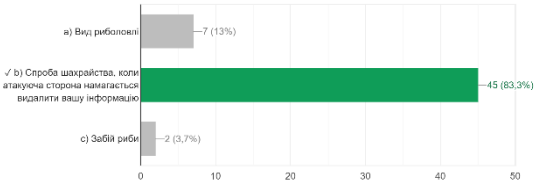
4. Як можна захистити свій комп'ютер від шкідливих програм? Виберіть всі відповіді, які вам відомі.

31 правильні відповіді з 54



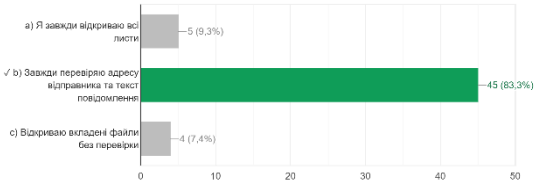
5. Що таке "фішинг"?

45 правильні відповіді з 54



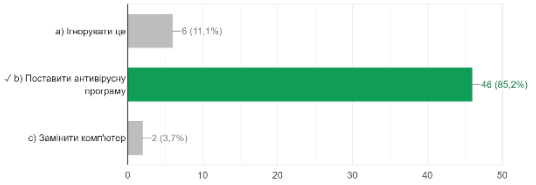
6. Як ви визначите, що електронний лист, який ви отримали, є спробою фішингу?

45 правильні відповіді з 54



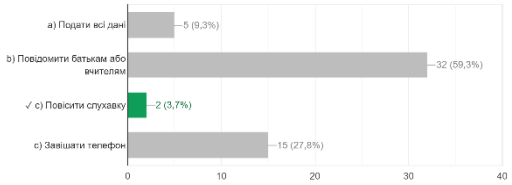
7. Що робити, якщо ви підозрюєте, що ваш комп'ютер заражений шкідливою програмою?

46 правильні відповіді з 54



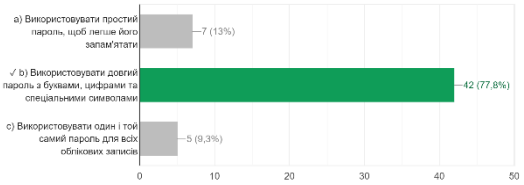
8. Які дії ви виконаєте, якщо вам зателефонував невідома людина і намагається отримати ваші персональні дані? (оберіть один варіант відповіді)

2 правильні відповіді з 54



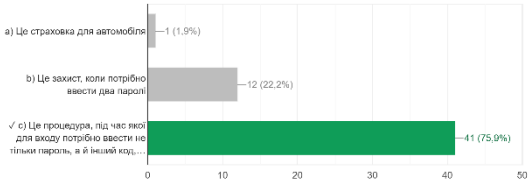
9. Як вибрати надійний пароль для облікового запису в інтернеті?

42 правильні відповіді з 54

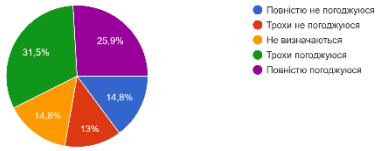


10. Що таке двофакторна аутентифікація і як вона допомагає збільшити безпеку облікового запису?

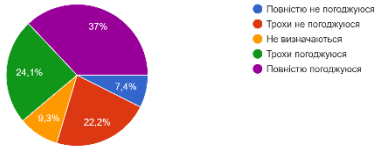
41 правильні відповіді з 54



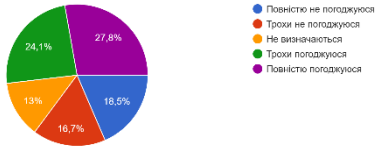
1. Я завжди розпізнаю спроби фішингу та шахрайства в інтернеті.
54 відповіді



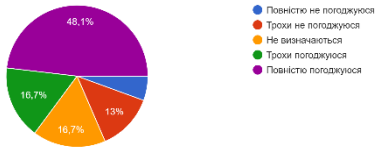
2. Я відчуваю себе впевнено у захисті своєї особистої інформації в інтернеті.
54 відповіді



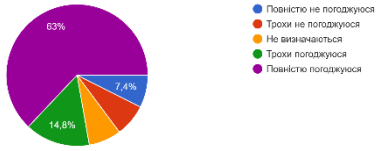
3. Я завжди реагую на випадки кібербулінгу та шахрайства в мережі та шукаю допомогу в дорослих.
54 відповіді



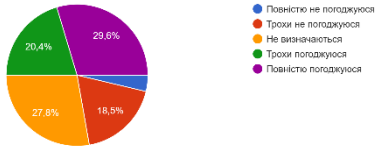
4. Я завжди перевіряю ланки в поштових повідомленнях та веб-сайтах, переконуючись, що вони безпечні перед тим, як натискати на них.
54 відповіді



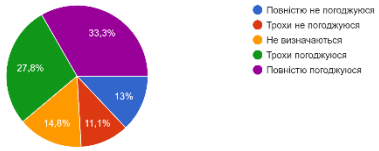
5. Я завжди підтримую добрий інтернет-етикет та поважаю інших у мережі.
54 відповіді



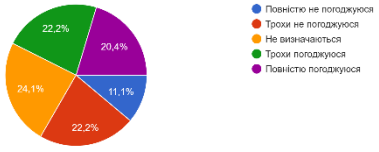
6. Я регулярно перевіряю наявність "https://" у веб-сайтах, які відвідую, та переконуюся, що вони безпечні.
54 відповіді



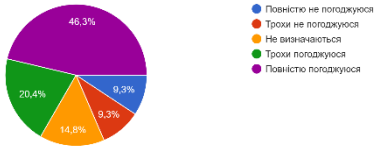
7. Я завжди ретельно розглядаю запити в друзі та повідомлення від незнайомих осіб в соціальних мережах та месенджерах.
54 відповіді



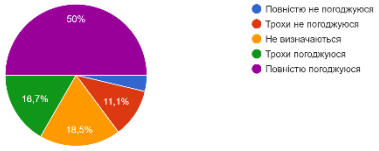
8. Я завжди стежу за змінами в поведінці онлайн і намагаюся розпізнавати випадки кібербулінгу та намагаюся допомогти постраждалим.
54 відповіді



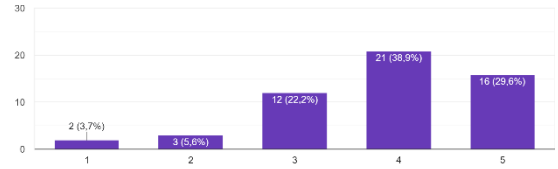
9. Я завжди ретельно досліджую веб-сайти, перш ніж надавати особисту інформацію або виконувати оплату в інтернеті.
54 відповіді



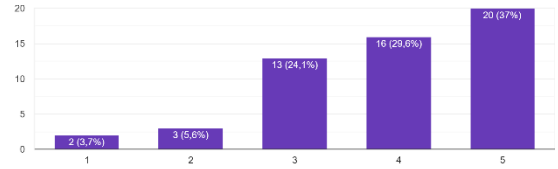
10. Я завжди ретельно перевіряю поштові повідомлення із сумнівними запитами або лінками, перш ніж натискати на них.
54 відповіді



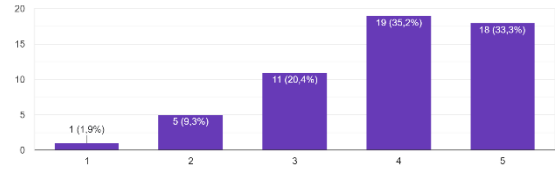
1. Оцініть свою відповідальність щодо використання соціальних мереж на шкалі від 1 (зовсім не відповідальний) до 5 (дуже відповідальний).
54 відповіді



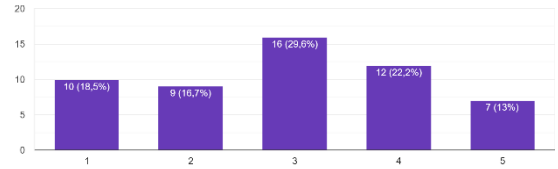
2. Наскільки ви впевнені у своїх навичках забезпечення безпеки під час використання соціальних мереж? Оцініть себе на шкалі від 1 (незнаючий) до 5 (дуже обізнаний).
54 відповіді



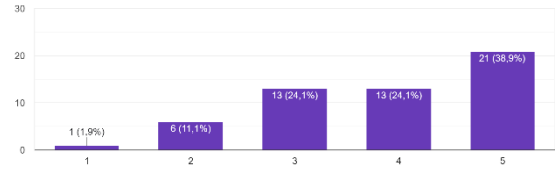
3. Наскільки ви ознайомлені з правилами та політикою використання соціальних мереж, зокрема щодо конфіденційності, вікових обмеже...калу від 1 (незнаючий) до 5 (дуже обізнаний).
54 відповіді



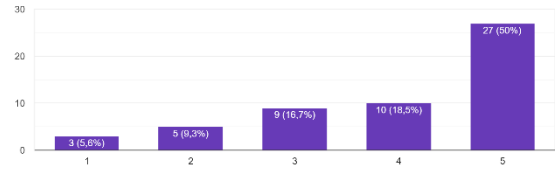
4. Як часто ви перевіряєте час, який витрачаєте на соціальних мережах? Оцініть це на шкалі від 1 (рідко) до 5 (дуже часто).
54 відповіді



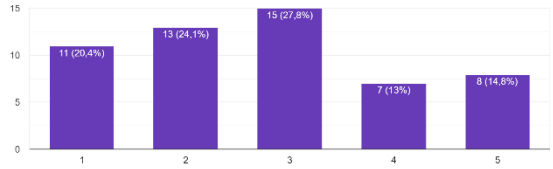
5. Оцініть своє ставлення до взаємодії з іншими користувачами соціальних мереж. Використовуйте шкалу від 1 (конфліктний) до 5 (дружелюбний та поважаючий інших).
54 відповіді



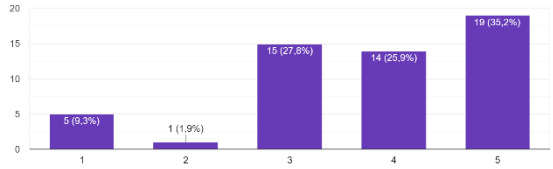
6. Як ви ставитеся до розкриття особистої інформації в соціальних мережах? Оцініть це на шкалі від 1 (дуже легковажно) до 5 (дуже обережно).
54 відповіді



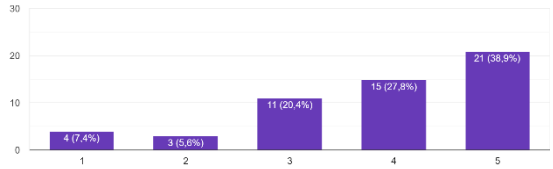
7. Як часто ви обговорюєте свою діяльність в соціальних мережах з батьками або вчителями? Використовуйте шкалу від 1 (зовсім не обговорюю) до 5 (часто обговорюю).
54 відповіді



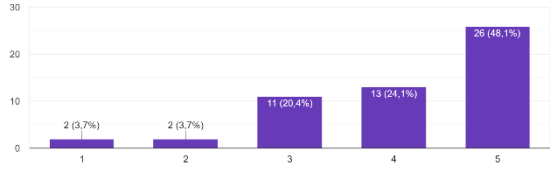
8. Звідки ви отримуєте інформацію про безпеку та відповідальне використання соціальних мереж? Використовуйте шкалу від 1 (не отриму...до 5 (отримую інформацію від різних джерел).
54 відповіді



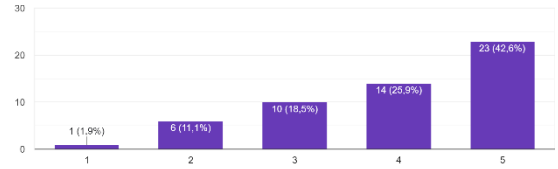
9. Наскільки ви готові навчатися і вдосконалювати свої навички в безпечному використанні соціальних мереж? Використовуйте шкалу від 1 (не готовий) до 5 (дуже готовий).
54 відповіді



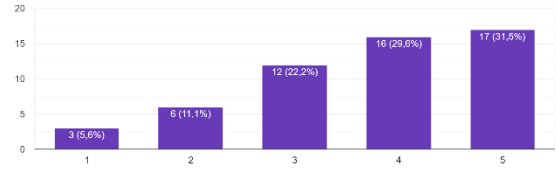
10. Як багато ви цінуєте можливості соціальних мереж та розумієте їхню важливість у вашому житті? Використовуйте шкалу від 1 (не ціную) до 5 (дуже ціную).
54 відповіді



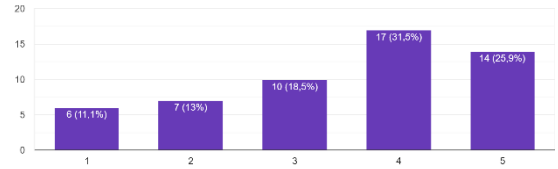
1. Оцініть свою свідомість про основні загрози в Інтернеті (від 1 до 5, де 1 - низька свідомість, 5 - висока свідомість).
54 відповіді



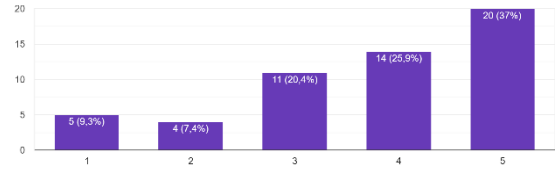
2. Як ви оцінюєте свої навички створення та керування сильними паролями (від 1 до 5, де 1 - слабкі навички, 5 - відмінні навички).
54 відповіді



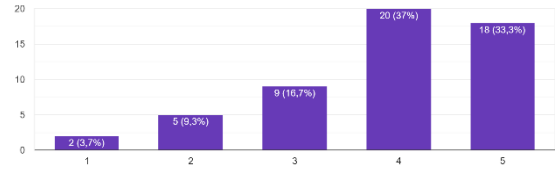
3. Оцініть свій рівень використання антивірусного програмного забезпечення на пристроях (від 1 до 5, де 1 - не використовую, 5 - завжди використовую).
54 відповіді



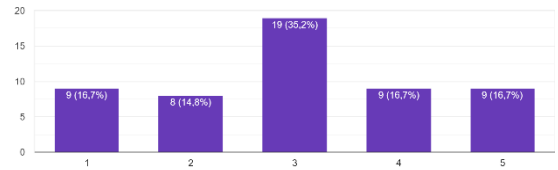
4. Як часто ви оновлюєте програми та операційну систему на своєму комп'ютері чи смартфоні (від 1 до 5, де 1 - рідко оновлюю, 5 - завжди оновлюю).
54 відповіді



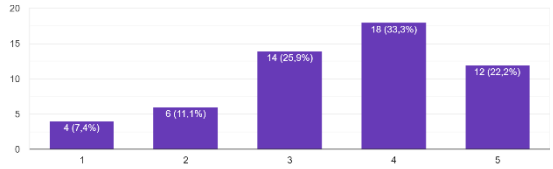
5. Оцініть свій рівень обізнаності щодо фішингових атак та способів їх виявлення (від 1 до 5, де 1 - мало обізнаний, 5 - дуже обізнаний).
54 відповіді



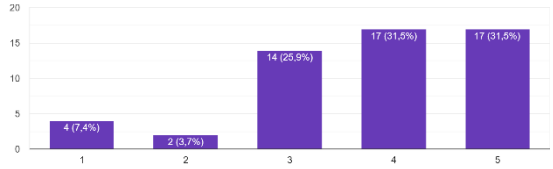
6. Як часто ви робите резервні копії важливих даних (від 1 до 5, де 1 - рідко, 5 - щоденно).
54 відповіді



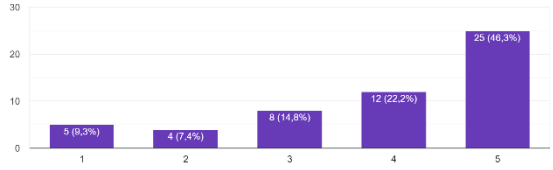
7. Оцініть свою здатність розпізнавати небезпечні посилання та вкладені файли у електронних листах чи повідомленнях (від 1 до 5, де 1 - погано розпізнаю, 5 - добре розпізнаю).
54 відповіді



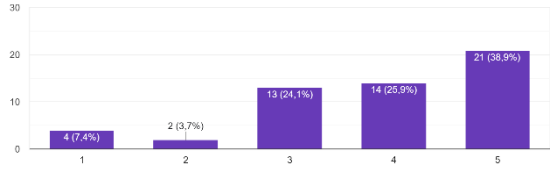
8. Як часто ви використовуєте двофакторну аутентифікацію для захисту своїх облікових записів (від 1 до 5, де 1 - не використовую, 5 - завжди використовую).
54 відповіді



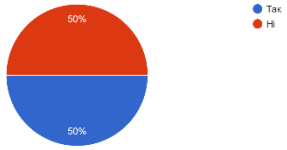
9. Оцініть свою готовність ділитися випадковою інформацією в соціальних мережах та месенджерах (від 1 до 5, де 1 - готовий ділитися, 5 - обережний у діленні інформації).
54 відповіді



10. Як ви оцінюєте свій рівень обізнаності щодо кібербулінгу та засобів захисту від нього (від 1 до 5, де 1 - мало обізнаний, 5 - дуже обізнаний).
54 відповіді

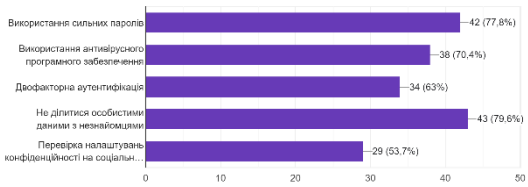


1. Чи ставите ви усвідомлено до надання своїх особистих даних (ім'я, прізвище, адреса тощо) в Інтернеті?
54 відповіді

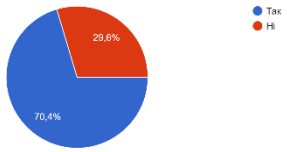


2. Як ви оцінюєте важливість захисту ваших особистих даних в Інтернеті на шкалі від 1 (не важливо) до 5 (дуже важливо)?
54 відповіді

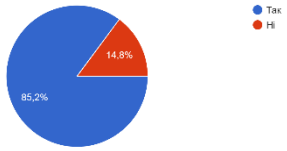
3. Які заходи безпеки ви вживаєте для захисту своїх особистих даних в Інтернеті? (Можете обрати декілька варіантів)
54 відповіді



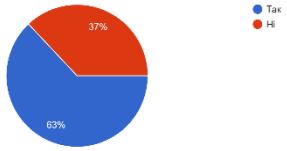
4. Чи робите ви резервні копії важливих даних (фотографії, документи тощо) для збереження інформації в разі її втрати?
54 відповіді



5. Чи розумієте ви ризики, пов'язані з розкриттям особистих даних в соціальних мережах, і приймаєте заходи для їх обмеження?
54 відповіді

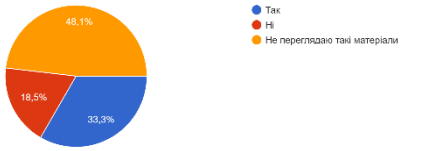


6. Чи обговорюєте ви питання приватності в Інтернеті з батьками або дорослими?
54 відповіді



7. Як ви реагуєте на запити про особисті дані в Інтернеті, наприклад, під час реєстрації на сайті чи завантаження додатку?
54 відповіді

8. Чи використовуєте ви "приватний режим" (інкогніто) в браузері для перегляду чутливих або особистих матеріалів в Інтернеті?
54 відповіді



9. Як ви визначаєте довіру до веб-сайтів чи додатків, які збирають особисті дані?
54 відповіді

10. Як ви відноситесь до надання доступу до своєї геолокації додаткам та сайтам?
54 відповіді