МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХЕРСОНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ПЕДАГОГІЧНИЙ ФАКУЛЬТЕТ
КАФЕДРА ПЕДАГОГІКИ ТА ПСИХОЛОГІЇ ДОШКІЛЬНОЇ ТА ПОЧАТКОВОЇ ОСВІТИ

ПЕДАГОГІЧНИЙ ІНСТРУМЕНТАРІЙ РОБОТИ ВЧИТЕЛЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО–БЕЗПЕЧНОГО СЕРЕДОВИЩА

Кваліфікаційна робота (проєкт)

на здобуття другого (магістерського) рівня вищої освіти

Виконала: студентка 2 курсу 211М групи

Спеціальності 013 Початкова освіта
Освітньо-професійної (наукової)
програми Початкова освіта

Шастіна Анастасія Юріївна

Керівник д.пед.н., професорка Петухова Л. Є.
Рецензентка начальниця відділу загальної середньої освіти управління освіти Херсонської міської ради Омельчук С. В.

Херсон – 2021

ЗМІСТ

ВСТУП

Актуальність дослідження. У сучасному світі із активним технологічним прогресом інформаційно–комунікаційні технології займають важливе місце вже навіть у житті молодшого школяра. Не могла залишитись осторонь і шкільна система. Вчителі та учні ефективно використовують ІКТ на уроках та під час підготовки домашніх завдань. Для того аби навчальний процес був максимально продуктивним, а учні знаходились у безпеці від негативного впливу медіа–продуктів вчитель має забезпечити таке навчальне середовище, яке буде захищене від різного роду інформаційних загроз, тобто створити інформаційно–безпечне середовище. Будь–яку проблему краще попередити, ніж потім вирішувати, тому актуальним є використання вчителем педагогічного інструментарію який забезпечуватиме учням цілком безпечний простір під час використання ними ІКТ.

Над питанням забезпечення інформаційно–безпечного середовища працювали і продовжують працювати науковці, педагоги та методисти, а саме: Малих Т.А., Кочарян А.Б., Гущина Н.І, Підгорна Т.В., Ковальчук В. Н., Черних О.О. та інші.

Мета дослідження полягає у розробленні та експериментальній перевірці педагогічного інструментарію вчителя для забезпечення інформаційно–безпечного середовища молодших школярів.

У відповідності до мети дослідження були поставлені такі **завдання:**

1. Розкрити ключові дефініції дослідження;

2. Проаналізувати вплив медіатизації на процес навчання учнів початкової школи;

3. Дослідити загрози в інтернеті як психолого–педагогічну проблему;

4. Провести компаративний аналіз інтернет–безпеки молодших школярів України і за кордоном, та діагностику організації інформаційної безпеки в школах Херсонщини;

5. Проаналізувати педагогічний інструментарій по забезпеченню інформаційно–безпечного середовища молодших школярі та розробити модель;

6. Розробити методичні рекомендації щодо підвищення рівня інформаційної безпеки молодших школярів.

Об'єкт дослідження – освітній процес у початковій школі з використанням ІКТ.

Предмет дослідження – педагогічний інструментарій вчителя для забезпечення інформаційно–безпечного середовища.

Для реалізації мети та завдань дослідження було використано комплекс наукових **методів**: теоретичні методи – вивчення і теоретичний аналіз психолого–педагогічної та методичної літератури з теми кваліфікаційної роботи; вивчення матеріалів та публікацій з поставленої проблеми. Практичні методи – анкетування, бесіда. Методи емпіричного дослідження – спостереження, вивчення і узагальнення передового педагогічного досвіду.

Наукова новизна одержаних результатів полягає в уточненні змісту понять дослідження: інформаційно–безпечне середовище; спроектований інструментарій забезпечення інформаційно–безпечного середовища.

Практичне значення одержаних результатів полягає у розробленні методичних рекомендацій по забезпеченню інформаційно–

безпечного середовища для молодших школярів. Окремо для вчителів ми розробили дві презентації, одна – для учнів, інша – для їх батьків. Розроблені нами презентаційні матеріали покликані допомогти вчителю забезпечити інформаційно–безпечне середовище для дитини.

Апробація. За результатами дослідження опубліковано дві статті: «Проблема інформаційної безпеки дітей молодшого шкільного віку» в збірці студентських наукових статей ХДУ 2021 року та «Роль вчителя початкової школи у забезпеченні інформаційно–безпечного середовища для учнів» в збірці наукових статей Національного педагогічного університету ім. М.П. Драгоманова.

Структура роботи. Кваліфікаційна робота складається зі вступу, двох розділів, висновків, списку використаних джерел та додатків.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО–БЕЗПЕЧНОГО СЕРЕДОВИЩА

1.1 Ключові дефініції дослідження

Для початку визначимо, що ж таке інформаційна безпека. В. Фурашев дає наступне визначення: «інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди через:

– негативний інформаційний вплив за допомогою, насамперед, несанкціонованого створення, розповсюдження, використання свідомо спрямованої із визначеною метою неповної, невчасної, невірогідної та упередженої інформації;

– негативні наслідки застосування інформаційних технологій;

– несанкціоноване порушення режиму доступу до інформації з подальшим її розповсюдженням та використанням» [39, с.54].

На думку В. Ісаєва: «Інформаційна безпека – це стан захищеності інтересів особистості, суспільства, держави в інформаційній сфері. Інформаційна сфера являє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, які здійснюють збір, поширення і використання інформації, а також системи регулювання виникаючих при цьому суспільних відносин» [14].

Н. Ковалева розділяє інформаційну безпеку на інформаційно–ідеологічну та інформаційно–технічну. Під інформаційно–технічною безпекою автор розуміє «захищеність приватних відомостей особи від

випадкових або навмисних впливів природного або штучного характеру, і як наслідок цього – нанесення збитків особі» [16, с. 110], а під інформаційно–ідеологічною безпекою – «захищеність особи від навмисного або ненавмисного інформаційного впливу, що в результаті призводить до порушення прав і свобод у галузі створення, використання та розповсюдження відомостей, користування інформаційною інфраструктурою і ресурсами, суперечить моральним та етичним нормам, що призводить до деструктивного впливу на особистість людини та має неусвідомлений характер впровадження у суспільну свідомість антисоціальних установок» [16, с. 110].

В. Бурячок у найзагальнішому розумінні визначає інформаційну безпеку як: «такий стан захищеності інформаційного простору, за якого неможливо завдати збитку властивостям об'єкта безпеки, що стосуються інформації та інформаційної інфраструктури…» [4, с. 12].

Перейдемо до більш конкретних визначень, а саме «інформаційна безпека людини» та «інформаційна безпека школяра».

Як зазначає Г. Сащук: «інформаційна безпека людини – це стан захищеності людини, різноманітних соціальних груп та об'єднань людей від впливів, за наявності яких проти волі та бажання людей можуть змінюватися їхні психічні стани і психологічні характеристики, модифікуватися їхня поведінка й обмежуватися свобода вибору» [34].

Т. Підгорна дає наступне визначення: «інформаційна безпека школярів – це стан захищеності основних інтересів учнів від загроз, викликаних інформаційним впливом на психіку та соціокультурний розвиток різними соціальними суб'єктами й інформаційним середовищем суспільства, у тому числі освітнім» [30, с.72].

Т. Малих інформаційну безпеку молодшого школяра визначає як стан захищеності його життєво важливих інтересів, що визначається його умінням виявляти та ідентифікувати загрози інформаційного впливу та умінням компенсувати негативні ефекти інформаційного впливу [25].

Також для нашого дослідження важливим є дефініція “інформаційно–психологічної безпеки людини». В. Толубко розрізняє рівні розуміння поняття “інформаційно–психологічної безпеки людини». За визначенням автора: «Інформаційно–психологічна безпека людини (у вузькому розумінні) – це стан захищеності психіки людини від негативного впливу, який здійснюється через вплив деструктивних інформаційних матеріалів на свідомість і (або) підсвідомість людини, що приводить до неадекватного сприйняття нею дійсності. Інформаційно–психологічна безпека людини (в широкому розумінні) – це:

– належний рівень теоретичної та практичної підготовки особистості, за якого досягається захищеність і реалізація її життєво важливих інтересів і гармонійний розвиток незалежно від наявності інформаційних загроз;

– здатність держави створити можливості для гармонійного розвитку й задоволення потреб людей в інформаційних матеріалах, незалежно від наявності інформаційних загроз;

– гарантування, розвиток і використання інформаційного середовища в інтересах суспільства і кожної людини;

– захищеність від різного роду інформаційних небезпек» [4, с. 56].

Проаналізувавши різні визначення інформаційної безпеки людини та врахувавши індивідуальні та вікові особливості молодших школярів, під їх інформаційною безпекою будемо розуміти стан захищеності основних інтересів дітей від загроз, які є або можуть бути викликані інформаційним впливом на психіку та соціальний, культурний розвиток різними суб’єктами та інформаційним середовищем суспільства, освітнім у тому числі. У даному контексті під основними інтересами дітей молодшого шкільного віку будемо розуміти реалізацію конституційних прав на отримання якісної освіти, яка у тому числі спрямовується на формування їх інформаційної культури, та гарантує забезпечення інформаційно–безпечного середовища.

Шлях забезпечення інформаційної безпеки школярів – це створення безпечного інформаційного простору як у школі, так і вдома учнів. В

організації безпечного особистісного інформаційного простору Ю. Богатирьова визначає такі групи заходів інформаційної безпеки школярів як:

– правові;

– технічні та програмні;

– виховні;

– організаційні;

– моральні й етичні;

– захист психіки та здоров'я дитини [3].

Розглянемо їх детальніше:

Правове забезпечення – це закони, нормативні акти, правила, процедури та відповідні заходи по створенню інформаційно–безпечного середовища учнів на законодавчій і правовій основі для реалізації політики держави у сфері захисту дітей від інформаційно небезпечних матеріалів, що завдають шкоди їх здоров'ю та психіці.

Законодавством України у сфері інформаційної безпеки дітей регламентується:

– захист від впливу негативного контенту в ЗМІ;

– заборона показу матеріалів негативного змісту в час доступний для дітей;

– відповідне до вікової класифікації маркування інформаційних матеріалів;

– відсутність негативного впливу рекламної продукції на свідомість дітей;

– вилучення і блокування інформаційних матеріалів злочинного змісту через мережу Інтернет;

– допустимість обмеження доступу дітей до інформаційних ресурсів негативного характеру в мережі Інтернет;

– взаємодія правоохоронних органів із провайдерами [30].

Технічне і програмне забезпечення – застосування апаратних та програмних забезпечень для профілактики нанесення матеріальної та моральної шкоди дитині, шляхом втручання у роботу мережних фільтрів, програм Батьківського контролю та інших технічних засобів захисту даних.

Виховні заходи щодо забезпечення інформаційної безпеки – формування у дітей розуміння наслідків власних дій в інформаційному просторі та відповідальності за них. Виховання культури безпечної поведінки дитини в Інтернеті.

Організаційний захист – це регулювання інформаційної діяльності дітей, контроль за використанням мережевих сервісів, що робить неможливим нанесення шкоди особистому інформаційному середовищу дитини.

Моральний та етичний аспект – дотримання дітьми правил поводження в мережі Інтернет, норм поведінки в суспільстві.

Захист психіки та здоров’я дитини – це різноманітні заходи щодо підтримання фізичного благополуччя дітей та їх хорошого психічного здоров’я. Профілактика комп’ютерної та інтернет–залежності, допомога педагога та психолога з питань зменшення негативних інформаційних впливів на життєдіяльність школярів.

Далі перейдемо до визначення поняття «педагогічний інструментарій». Важливо відмітити, що в термінології педагогічного інструментарію у вітчизняній педагогіці немає однозначності. В результаті одне й те ж поняття в різних навчальних джерелах називається по–різному.

Ми розуміємо педагогічний інструментарій як сукупність форм, методів, прийомів і засобів педагогічної взаємодії суб'єктів освіти та виховання. Вони, являють собою специфічні (педагогічні) інструменти, за допомогою яких здійснюється формування необхідних особистісних якостей дитини.

Рис. 1.1. Педагогічний інструментарій викладача

Наступними важливим поняттями для нашого дослідження є інформаційно–комунікаційні технології та медіатизація. За визначенням А. Б. Кочарян: «інформаційно–комунікаційні технології або ІКТ — це технології, пов’язані зі створенням, збереженням, передачею, обробкою та управлінням інформацією. Цей широко вживаний термін включає в себе всі технології, що використовуються для спілкування та роботи з інформаційними ресурсами» [22, с.5]. Медіатизацію В. П. Коломієць розглядає як процес проникнення ІКТ в повсякденне життя людей.

Отже, ключовими для нашого дослідження є наступні дефініції:

– інформаційна безпека молодшого школяра – це стан захищеності учнів молодшої школи від загроз, які можуть бути викликані інформаційним впливом і негативно діяти на психіку та соціальний, культурний розвиток дитини.

– педагогічний інструментарій – це сукупність форм, методів, прийомів і засобів педагогічної взаємодії суб'єктів освіти та виховання. Вони, являють собою специфічні (педагогічні) інструменти, за допомогою яких здійснюється формування необхідних особистісних якостей дитини.

– інформаційно–комунікаційні технології – це технології, пов’язані зі створенням, збереженням, передачею, обробкою та управлінням інформацією. Цей термін включає в себе всі технології, що

використовуються для спілкування та роботи з інформаційними ресурсами [22, с.5].

Ці терміни будуть покладенні в основу нашого дослідження.

1.2 Вплив медіатизації на процес навчання учнів початкової школи

Вивчаючи проблеми з теми нашої роботи, ми проаналізували і вплив медіатизації на процес навчання учнів початкової школи. Діти можуть використовувати інтернет з різними цілями: для того аби поспілкуватися з друзями, послухати музику, переглянути відео–фрагменти, пограти в ігри, виконати завдання вчителя, знайти та ознайомитись з інформацією яка цікавить і т. д. Для того аби задовольнити свої бажання та потреби учні використовують безліч послуг Інтернету, найпопулярніші із них такі як: web–браузери, web–сайти, пошукові системи, електронна пошта, відео–конференції та різноманітні соціальні мережі. Зупинимось на них детальніше:

Розпочнемо із самого масштабного, а саме із Web–браузера. Це програмне забезпечення для комп'ютера або інших електронних пристроїв, яке працює за умови під'єднання до мережі Інтернет. Дозволяє отримати доступ до текстової, фото–, відео– та інших видів інформації, завантаженої на інший комп'ютер. Педагог має навчити дітей обирати для роботи безпечний браузер, на який обов'язково будуть встановлені антивірусні програми.

Наступними розглянемо Web–сайти, що являють собою набір Web–сторінок, об'єднаних спільною темою, адресою, оформленням та логічною структурою. Для того аби відвідати Web–сайт необхідно знати його адресу. Доступ до більшості із сайтів є безкоштовним. Але деякі можуть вимагати зареєструватися: тобто надати ім'я, адресу електронної пошти, вік, стать тощо. У даному питанні також треба бути застережливим і пояснити дітям,

що реєструватися та залишати особисту інформацію можна лише на перевірених сайтах із дозволу батьків або вчителя. Найперше що має зробити вчитель – це дати перелік сайтів, які містять точну, перевірену, наукову інформацію.

Для навчання та задоволення власного інтересу діти активно використовують пошукові системи. Їх метою є забезпечення навігації серед мільйонів сайтів. Тобто за допомогою них учні і знаходять потрібну інформацію. Прикладами пошукових систем є: https://www.google.com та http://www.bing.com. Педагог має навчити своїх учнів правильно користуватися пошуковими системами, фільтрувати інформацію та обирати ту, яка є достовірною.

Останнім часом набули особливої популярності відео–конференції. Це миттєвий обмін аудіо– та відео–матеріалами через Інтернет в режимі реального часу. Відео–конференції набули популярності у всьому світі через необхідність організації дистанційного навчання пов'язаного із епідемією COVID–19.

Також в умовах віддаленого навчання вчителі та учні частіше почали використовувати електронну пошту, яка є версією звичайної пошти, але з використанням технічних пристроїв. Являє собою спосіб обміну повідомленнями між користувачами та надає можливість ділитися будь–якими матеріалами (текст, фото–, відео–, аудіо–файли тощо). Кожен користувач має індивідуальну адресу, яка ідентифікує її власника. Вчителеві зручно надсилати необхідні матеріали та повідомлення відразу всім своїм учням, а потім отримувати відповіді та виконанні завдання на ту ж електронну пошту.

Останніми у нашому списку, але далеко не останніми по важливості хочемо відмітити соціальні мережі. Вони дають можливість користувачам створити власну сторінку (анкету), розміщувати на ній фото, аудіо– та відеоматеріали, надсилати повідомлення друзям та спостерігати за

оновленнями на їх сторінках. Соціальні мережі є дуже популярними серед молоді, бо вони дозволяють вільно спілкуватися та самореалізовуватися [22].

Усе перераховане нами вище створює віртуальний простір, який дає можливість молодшим школярам реалізувати низку своїх базових потреб. Основні серед них: спілкування з однолітками, навчання, ігри та розваги, саморозвиток та самореалізація особистості.

Традиційна класно–урочна система започаткована Яном Амосом Коменським, була зорієнтована на передачу знань від учителя до учня. У сучасному ж освітньому просторі з появою ІКТ навчально–виховний процес переходить від навчання, в основі якого лежить передача інформації з вуст вчителя або прочитана у підручнику, до навчання дітей через сприймання та засвоєння нового за допомогою електронних ресурсів, Інтернету, навколишнього середовища і т. д. Вчитель, керуючи навчальним процесом може на будь–якому уроці використати дані технології. Організовуючи дослідницьку діяльність дітей, педагог орієнтує їх індивідуальну роботу на пошук необхідної інформації, вчить самостійно оцінювати її, розрізняти правдиву та фейкову інформацію, оцінювати надійність інформаційних джерел тощо.

Важливою зміною сучасного навчання стало і те, що учні навчаються самостійно створювати різноманітні електронні продукти: малюнки, інтелект карти, мультимедійні презентації і т. д. З появою великої кількості технічних засобів за допомогою яких учень може самостійно знаходити інформацію яка йому необхідна, зникає сенс у перевантажені пам’яті дитини великим об’ємом інформації. Зате виникає необхідність навчити школяра знаходити правдиву інформацію та ефективно використовувати її у своїй практичній діяльності, застосовувати набуті знання у реальному житті.

Ще однією важливою особливістю є те, що навчання дітей з використанням ІКТ дозволяє вчителеві організовувати його в індивідуальному темпі необхідному для кожного учня, створюючи при цьому ситуацію успіху та підвищуючи інтерес та мотивацію до навчання.

Отже, перевагами навчання з використанням ІКТ є:

– індивідуалізація навчання;

– більше можливостей у вчителя для організації самостійної роботи учнів;

– за один і той самий проміжок часу можна виконати більший обсяг завдань на уроці, порівняно з традиційною формою навчання;

– різноманітні форми роботи з використанням ІКТ збільшують інтерес учнів до теми, що вивчається та підвищують мотивацію до вивчення предмета в цілому;

– збільшення обсягу нових знань завдяки використанню мережі Інтернет.

Проведена нами робота над вивченням питання впливу медіатизації на процес навчання учнів початкової школи дозволила зробити висновок, що використання різноманітних інформаційних ресурсів, таких як: web–браузери, web–сайти, пошукові системи, електронна пошта, відео–конференції та різноманітні соціальні мережі позитивно впливають на процес навчання учнів початкової школи за умови грамотного їх використання вчителем. Поєднуючи традиційні методи навчання та сучасні інформаційні технології педагог має можливість зробити процес навчання гнучким та індивідуальним.

1.3 Загрози в інтернеті як психолого–педагогічна проблема

Інтернет – корисний та потужний ресурс, який має багато переваг, значно полегшує життя людині. При цьому даючи велику кількість можливостей своїм користувачам, він може становити і реальну загрозу. Ми, дорослі, краще вміємо аналізувати інформацію яку отримуємо, а ось діти молодшого шкільного віку тільки навчаються цьому. Вони є психологічно вразливими відносно тієї інформації на яку можуть натрапити в інтернеті.

Тому наше завдання як педагогів та помічників допомогти нашим учням розібратися, що може становити для них небезпеку та вміти її уникати.

З метою більш детального вивчення теми, був пройдений курс «Безпека дитини в інтернеті: від загроз до можливостей» і отриманий сертифікат на дві академічні години (Додаток А).

Автор курсу О. Черних зазначає, що загроза в інтернеті не дорівнює шкоді. Загроза може завдати її, а може і не завдати [40].

За віковою періодизацією дитячий вік від шести до одинадцяти років вважається молодшим шкільним віком. Даний період має свої певні психологічні особливості. Вступ дитини до школи, різка зміна оточення відображаються на психіці учня. Важливо зазначити і те, що у дитини змінюється провідна діяльність з ігрової на навчальну. Тепер вона у ролі школяра і вимагають від неї більше ніж зазвичай. Продовжують активно формуватись норми культурної поведінки та моралі, вміння самодисциплінуватися та прогнозувати наслідки своїх вчинків. Зважаючи на широке використання у навчальному процесі ІКТ важливим є засвоєння молодшим школярем норм поведінки в інтернеті. Так як психіка дитини є ще дуже вразливою і випадкова інформація з інтернету, що не розрахована на вік молодшого школяра може завдати великої шкоди, варто контролювати її дії у мережі.

Детально дослідивши та проаналізувавши дану проблему ми зупинимось на конкретних інтернет загрозах з якими можуть зіштовхнутися учні початкової школи:

Найперше це різного роду віруси. Вони являють собою програму, яка спеціально створена зловмисниками з метою завдати шкоди тому до кого потрапить цей вірус. Комп’ютерні віруси здатні до само розмноження та заподіяння шкоди починаючи від появи різних небажаних користувачем звукових та візуальних ефектів, що заважають використовувати комп’ютер, закінчуючи повною втратою інформації, яка містилась на певному носії. На сьогодні існує понад п’ятдесят тисяч різних комп’ютерних вірусів.

Найпоширеніші шляхи їх передачі через заражену флеш–карту та через систему електронної пошти. Основні ознаки за якими можна запідозрити зараження комп'ютера вірусом такі: різке зменшення оперативної пам'яті, сповільнена робота та завантаження, різні зміни у файлах, звукові та візуальні ефекти.

Ще однією інтернет–загрозою для дітей є онлайн–звабления. Злочинці створюють сторінки в соціальних мережах, які наповнені контентом, що є цікавим дітям. Пишуть їм у приватні повідомлення та намагаються потоваришувати та завоювати довіру. З часом таке спілкування переходить межі нормального, злочинці намагаються втягти дитину в ситуацію сексуального насилля. Пишуть непристойні речі, просять надіслати особисті фото тощо. Часто таке спілкування закінчується погрозами, вимаганням коштів та шантажем розповісти про все батькам дитини і розповсюдити її фото. Молодший школяр ще не здатен достатньо критично оцінити те, що з ним відбувається та боїться повідомити про все батькам. Звичайно така ситуація здатна негативно вплинути на ще не остаточно сформовану психіку дитини. Саме тому важливо встановлювати довірливі стосунки з дітьми та пояснювати чому небезпечно спілкуватись із незнайомцями.

Наступною інтернет–загрозою для молодших школярів вважаємо небажаний контент. Це шкідливі та нелегальні для зазначеного вікового періоду матеріали, які містяться у вільному доступі. По–перше, це контент для дорослих, а саме порно контент. Інтернет надає можливість вільного доступу до такого контенту будь–кому. Існує висока вірогідність того, що дитина натрапить на нього в інтернеті навіть якщо спеціально не шукатиме цього. По–друге, це різного роду матеріали які пропагують шкідливі звички, жорстоку поведінку і т. д. Молодшому школяреві, який натрапить на матеріали які містять жорстокі сцени насилля над людьми або тваринами можуть завдати психологічної травми та перешкоджати формуванню нормальних моральних цінностей. По–третє, це інформація яка може підштовхнути до скоєння злочину. Така інформація також є у вільному

доступі, достатньо лише ввести ключову фразу або слово, і на екрані вже відповідь, наприклад на питання як виготовити вибухівку, або де купити наркотики. Тому батькам важливо контролювати дії своїх дітей в інтернеті, та встановлювати спеціальні програми, які блокуватимуть доступ до певних сайтів або матеріалів.

Не можемо не згадати і за кібер–хуліганство. Це вид інформаційної атаки на дитину через інтернет. Загроза у тому, що учень не може сховатися від такого хуліганства вдома. Навіть на очах батьків, які часто не помічають що з дитиною щось коїться, вона може стати жертвою кібер–хуліганів. Основним видом кібер–хуліганства є кібер–булінг. Це цькування дитини через соціальні мережі, електрону пошту, чати в іграх і т. д. Батьків та вчителів повинно насторожити те, що дитина стала тривожною, боїться відкривати смс–повідомлення, виявляє небажання відвідувати школу або користуватись комп'ютером.

Ще одним видом інтернет загрози вважаємо шпигунське програмне забезпечення. Воно може потрапити на технічний пристрій через лист з електронної пошти, достатньо лише перейти через посилання у ньому. Такі програми здатні зібрати інформацію що міститься на цьому технічному пристрої. Це можуть бути різні паролі, номера телефонів, адреса, особиста інформація тощо.

Також для молодших школярів становлять загрозу соціальні мережі, які сьогодні є досить популярними вже навіть серед учнів молодшої школи. І більшість із соціальних мереж заохочують надавати якомога більше особистої інформації про себе при створенні сторінки і заповнені анкети. Це прізвище та ім'я, дата народження, адреса, номери телефонів, інформація про родину, інтереси тощо. Зловмисникам стає нескладно обрати потенційну жертву в мережі. До того ж користувачі добровільно надають конфіденційну інформацію про себе. Часто діти виставляють особисті фото, які також можуть бути використані шахраями. Педагогам важливо проводити профілактичні бесіди з учнями в школі на тему безпечного користування

інтернетом. Такі бесіди повинні періодично повторюватися та закріплюватися.

Наступною інтернет–загрозою ми вважаємо недостовірну інформацію. Вже давно відомо, що далеко не вся інформація з мережі є правдивою. І якщо це інформація, яка стосується наприклад здоров'я виявилась недостовірною то скориставшись нею можна заподіяти шкоди здоров'ю. Особливо учням молодшої школи важливо це розуміти, адже у них ще недостатньо розвинуті навички аналізу та узагальнення, відсутнє вміння критично мислити на необхідному рівні. Важливо пояснити дитині, що дійсно необхідну інформацію варто дізнаватись у спеціалістів, для цього треба звернутись до батьків або вчителя.

Детально дослідивши та проаналізувавши інтернет загрози як психолого–педагогічну проблему ми можемо виділити такі основні інтернет загрози для молодших школярів, як: віруси, небажаний контент, недостовірна інформація, інтернет–зваблення, кібер–хуліганство, шпигунське програмне забезпечення та соціальні мережі. Все це становить загрозу, так як психіка дитини молодшого шкільного віку ще не достатньо сформована для того, аби вміти самостійно аналізувати інформацію яка є в інтернеті. Молодші школярі легко можуть натрапити на інформацію, яка негативно вплине на їх психіку та перешкоджатиме формуванню правильних життєвих цінностей та норм моралі.

1.4 Компаративістика рівня інтернет–безпеки молодших школярів України та за кордоном

Для більш детального вивчення проблеми ми провели компаративістику рівня інтернет–безпеки молодших школярів України та за кордоном, і хочемо виділити основне із проведеного нами аналізу.

За результатами дослідження Eurobarometer, яке проводилось у 2008 році у 27 країнах членах Європейського Союзу, 75% дітей від 6 до 17 років

були активними користувачами мережі інтернет. До того ж половина таких користувачів є дітьми батьків, які не використовують інтернет зовсім. Лише з половиною дітей, які користуються інтернетом батьки говорили про безпечну поведінку у ньому. Найчастіше це було попередження про важливість не розголошення дітьми особистої інформації – у 92% випадків. На другому місці 83% випадків – заборона спілкування з незнайомими людьми в інтернеті. 59% батьків використовували спеціальне програмне забезпечення, яке контролює сайти відвідані дитиною, а батьки які не робили цього пояснюють це тим, що довіряють своїй дитині, або ж просто не вміють користуватися такими програмами.

Інше дослідження, яке проводилось в рамках проекту EU Kids Online в Лондонському економічному інституті у 2009 році показало дещо інші результати. 77% батьків у Великій Британії використовують програмне забезпечення для контролю за діями дитини в інтернеті. 87% проводять бесіди зі своїми чадами щодо безпечного поводження в інтернеті. Але одночасно з тим, британських батьків не надто непокоїть той факт, що діти переглядають дорослий контент в інтернеті [22, с. 9].

У 2014 році компанія «Ofcome» провела дослідження у Великій Британії щодо використання дітьми цифрових медіа. Воно показало позитивні зрушення стосовно критичного ставлення дітей до змісту інформації в інтернеті. Порівняно з дослідженням попереднього року все більше школярів (26 %) розуміють, що далеко не вся інформація в інтернеті є правдивою та безпечною і може використовуватись при підготовці домашніх завдань. Три четверті батьків довіряють своїм дітям в безпечному користуванні інтернетом та вважають себе достатньо обізнаними та спроможними допомогти своїм дітям у разі виникнення ризиків чи проблем.

Південна Корея розвиває інноваційні освітні технології з 1997 року і є країною яка готується до нової цифрової еволюції. Такий розвиток звичайно не може не вплинути на освітній процес. Хочемо зазначити, що у Програмі міжнародного оцінювання учнів PISA Digital Reading Assessment за 2009 рік

саме Корея посіла перше місце поряд з Фінляндією та Гонконгом. Школярі продемонстрували кращі здібності до розв'язування проблем за допомогою Інтернету, залишивши США далеко позаду, на чотирнадцятому місці.

Корея активно використовує електронні підручники, планшети та ноутбуки під час навчання дітей у школах. Все програмне забезпечення є інформаційно–безпечним для учнів, адже було розроблено виключно для навчальних цілей. Дослідження показали, що навчання за допомогою таких технічних пристроїв сприяє підвищенню в учнів мотивації до навчання і як результат покращує їх знання та вміння. Загалом рівень інтернет–безпеки у Кореї є досить високим.

В. Гулай повідомляє: «для забезпечення повноцінної та ефективної системи кібербезпеки уряд Ізраїлю ініціює і підтримує програми навчання спеціальних кадрів, а також інформаційні програми для населення країни, наприклад, навчання школярів навичкам цифрового захисту. Крім того, в країні підтримується кілька освітніх програм для молоді віком 16– 18 років. Вважаємо, що освітня програма у сфері кібербезпеки є позитивним фактором, який дає змогу поширити серед населення відомості з інформаційної безпеки. У рамках масштабної боротьби з хакерами Ізраїль спільно з США реалізує проекти шкільної та дошкільної освітньої підготовки у сфері кібербезпеки» [8].

Тепер перейдемо до рівня інтернет–безпеки молодших школярів України. Для початку представимо результати опитування батьків, які оцінили рівень володіння базовими цифровими навичками своєї дитини за шкалою від 1 (не володіє зовсім) до 6 (високий рівень володіння).

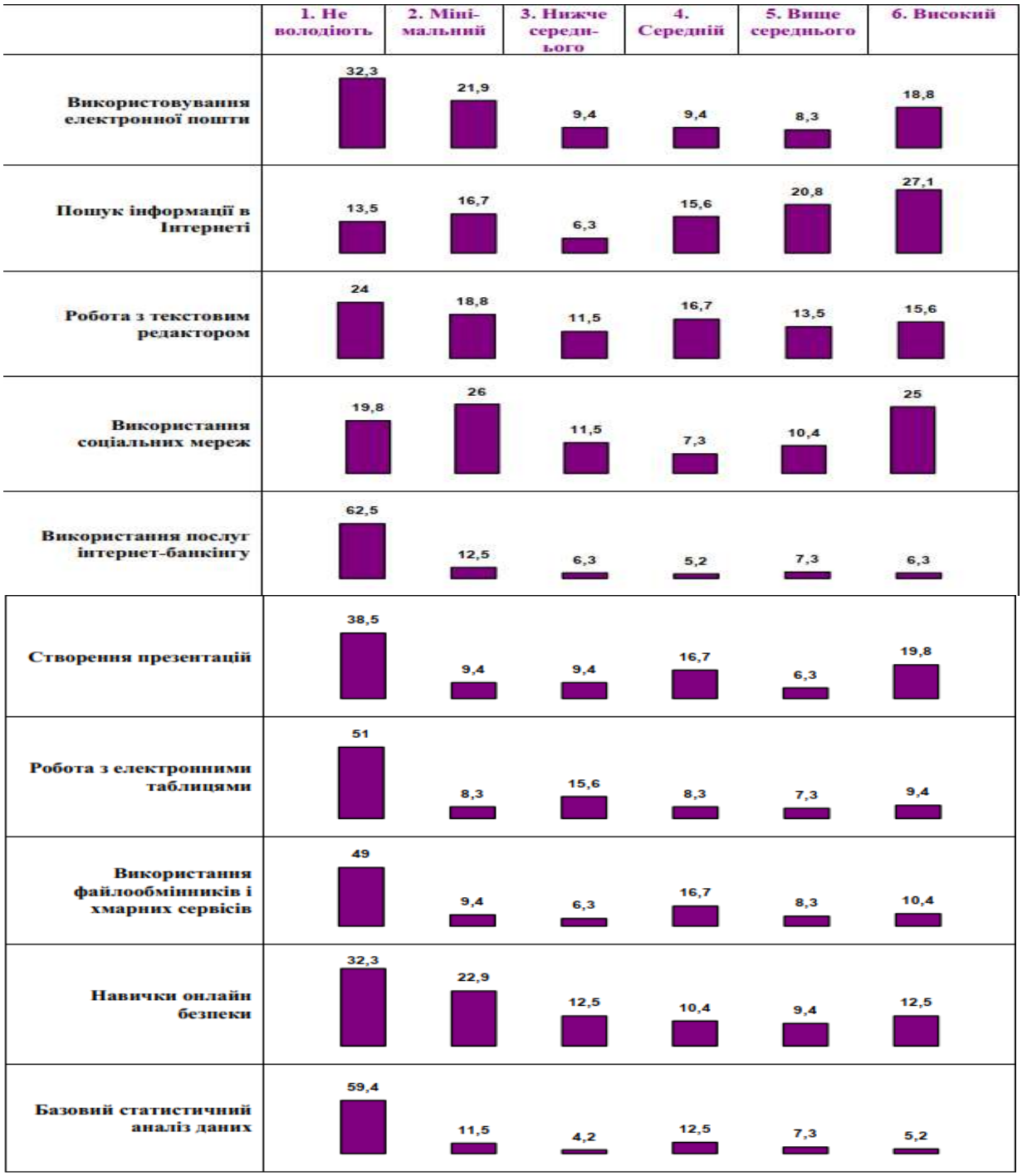


Рис. 1.2 Рівень володіння дітьми основними цифровими навичками

На думку батьків, діти краще володіють такими цифровими навичками, як: використання соціальних мереж (25,0% – «високий», 10,4% – «вище середнього»), пошук інформації в інтернеті (27,1% – «високий», 20,8% – «вище середнього»). Тоді як найгірше, на думку батьків, діти володіють навичками використання послуг інтернет–банкінгу (62,5% – не володіють, 18,8% – «низький» та «нижче середнього»), роботи з електронними таблицями (32,3% – не володіють, 23,9% – «низький» та «нижче

середнього»), використання файлообмінників і хмарних сервісів (49,0% – не володіють, 15,7% – «низький» та «нижче середнього»), базовий статистичний аналіз даних (59,4% – не володіють, 15,7% – «низький» та «нижче середнього»), навички безпеки (32,3% – не володіють, 35,4% – «низький» та «нижче середнього») [1].

Це українське дослідження провели у 2021 році напередодні Міжнародного дня захисту дітей. Державний інститут сімейної та молодіжної політики провів онлайн опитування батьків щодо використання ними телефонів/смартфонів та рівня володіння навичками безпеки при користуванні інтернет ресурсами (додаток Б).

Важливим для нас результатом цього дослідження є те, що більше половини батьків (62,2%) зізналися, що в їхньому житті траплялися випадки, коли дитина просила їх відкласти смартфон аби провести час разом**.** З них 10,7% опитаних батьків стикається з такою ситуацією досить часто.

Але на думку батьків, діти нерідко самі занурені в смартфони і не спілкуються з ними. 86,9% опитаних батьків зазначили, що просять своїх дітей

відкласти смартфон аби провести час разом**.** З них понад третини (35,4%) робить це досить часто.

Те, що діти «приклеєні» до пристроїв викликає занепокоєння серед батьків, про це зазначило понад половини опитаних (51,4%). Третину з них (33%) ця проблема дуже турбує. Разом з тим така ж сама частка батьків (33,0%) немає однозначної думки з цього приводу (варіант відповіді «як турбує, так і ні»), ще майже 6,0% опитаних батьків – взагалі не переймаються цією проблемою.

Те, що діти дуже багато часу безконтрольно проводять за гаджетами змушує батьків до відповідних дій (застосування засобів безпеки) аби, насамперед, убезпечити власних дітей від негативних явищ, на які можна наразитися в мережі інтернет.

Понад третини опитаних батьків встановлює програми батьківського контролю або застосовує певні обмеження на користування гаджетами та мережею інтернет (відповідно 35,0% і 34,0%).

Проте майже 10% опитаних батьків нічого не роблять аби запобігти всім

тим негативним явищам і небезпекам, на які наражаються діти при користуванні смартфоном та мережею інтернет. Тоді, як переважна більшість батьків (73,8%) вдається до особистих розмов з дитиною про небезпеку користування смартфоном та інтернет. Така ситуація свідчить про досить низький рівень володіння батьками навичками інтернет–безпеки [1].

А ми перейдемо до аналізу наступного українського дослідження. У 2009 році «Київстар» ініціював Всеукраїнське соціологічне дослідження «Знання і ставлення українців до питання безпеки дітей в інтернеті», яке провів Інститут соціології НАН України, яке показало, на які інтернет–загрози реагують діти[2, с.10–13]:

– «понад 28% опитуваних дітей готові надіслати свої фотокартки незнайомцям у Мережі;

– 17% без коливань діляться інформацією про себе і свою родину – адресу, професію, графік роботи батьків, наявність цінних речей у домі тощо. Навіщо незнайомцям така інформація, діти, як правило, не замислюються;

– 22% дітей періодично потрапляють на сайти для дорослих;

– 28% дітей, побачивши в інтернеті рекламу алкоголя або куріння, хоча б один раз спробували їх купити, а 11%− намагалися купувати наркотики;

– близько 14% опитуваних час від часу відправляють платні SMS за бонуси в онлайн іграх і лише деякі звертають увагу на вартість послуги» [2, с.10–13].

Результати дослідження свідчать про досить низький рівень інтернет–безпеки українських дітей. Хоча 87% батьків відповіли що саме вони повинні контролювати дії своєї дитини в інтернеті. А дійсно контролюють лише 18%.

Це говорить про низький рівень володіння батьками навичками користування програмами батьківського контролю.

Проведена нами компаративістика дала можливість зробити висновок, що Україні є куди рости та розвиватись. Прикладом для нашої країни може бути досвід Кореї та Ізраїлю. Але ми беззаперечно рухаємось у правильному напрямку, досліджуючи проблему інформаційної безпеки учнів ми стаємо ближчими до досягнення високих результатів. Загалом, інтернет мережа не має національних кордонів. Для створення безпечного інформаційного середовища для дітей в інтернеті необхідно об'єднувати зусилля урядів та суспільства всіх країн на міжнародному рівні. Через це міжнародні організації і розробили документи які спрямованні на захист дітей від порушення їх прав через використання ІКТ. Основним міжнародним документом зобов'язального характеру в цій сфері є положення Конвенції ООН про права дитини.

РОЗДІЛ 2
ОРГАНІЗАЦІЙНО–ПЕДАГОГІЧНІ УМОВИ ФОРМУВАННЯ ІНФОРМАЦІЙНО–БЕЗПЕЧНОГО СЕРЕДОВИЩА ДЛЯ МОЛОДШИХ ШКОЛЯРІВ

2.1 Діагностика стану організації інформаційної безпеки в школах Херсонщини

Ми вивчили та дослідили стан організації інформаційної безпеки в Херсонській спеціалізованій школі І–ІІІ ступенів № 30. Хочемо зазначити головне, що ми відмітили:

З 2 по 4 клас інформатика як навчальний предмет введений у програму. Але починаючи вже з першого класу учні вивчають інформатику в межах гурткової роботи. На перших заняттях дітей знайомлять з правилами поводження у комп'ютерному класі та з самим комп'ютером. Дають початкові уявлення та знання про інтернет та правила поводження у ньому. На базовому рівні розповідають про можливості та загрози інтернету. Далі в межах програми вивчаються наступні теми пов'язані з інтернет–безпекою учнів [38]:

– 2 клас – «Безпечний інтернет. Правдива та неправдива інформація у ньому», «Правила поводження з гаджетами у цифровому світі», «Програми та пристрої для спілкування в інтернеті, у безпечних онлайнових та офлайнових середовищах», «Етика спілкування в мережі, особливості цифрового спілкування. Як уникнути цькування в цифровому спілкуванні» [38].

– 3–4 класи – «Критерії оцінювання надійності інтернет–сайтів», «Вікові обмеження та свідомий вибір програм для роботи», «Освітні веб–ресурси та правила роботи з ними», « Етика спілкування в мережах та її дотримання», «Спільне та відмінне між реальним та віртуальним спілкуванням», «Цифрова репутація та цифровий слід. Відповідальна поведінка онлайн» [38]. «Конфіденційність даних, приватність інформації. Сильні і слабкі паролі», «Джерела отримання допомоги в прикрих і тривожних ситуаціях», «Культура в мережі. Правила комунікації з різними групами людей. Відповідальність за порушення правил взаємодії» [38].

Також важливо зазначити, що школа дотримується позиції регулярного нагадування дітям на уроках про основні правила безпеки в інтернеті, опосередковано згадувати про них якомога частіше.

Хочемо відмітити, що Херсонська спеціалізована школа I–III ступенів №30 є досить добре технічно оснащеною. Має чотири комп'ютерних класи (від 11 до 16 комп'ютерів у кожному, також для вчителя наявні принтери, сканери тощо). Недоліком все ж вважаємо розташування столів. Вони розміщенні так, що вчитель зі свого робочого місця не може бачити та контролювати учнівські екрани. Але цей недолік компенсується використанням вчителем програмного забезпечення для контролю за діями дітей. Школа використовує програму NetOp School. Вона дозволяє вчителеві дистанційно управляти комп'ютерами учнів, запускати демонстрацію свого екрану, швидко збирати та перевіряти виконанні завдання, обмежувати доступ дітей до певних сайтів.

Всі класи початкової школи забезпеченні необхідним технічним обладнанням, це і телевізори, і проектори та ноутбуки, і інтерактивні дошки. Вчителі активно використовують їх під час навчального процесу.

Важливою формою роботи школи по забезпеченню інформаційно–безпечного середовища для учнів молодшої школи є проведення кожного року дня безпечного інтернету. Останній такий захід відбувся 9 лютого 2021 року. Теми надає Safer Internet Day.

Ще однією не менш ефективною формою робити є проведення регулярних профілактичних бесід із батьками учнів на тему безпеки їх дітей в інтернеті, на яких вчитель обов'язково надає корисні рекомендації для батьків. Відбуваються вони планово на батьківських зборах, та за необхідності можуть проводитись частіше і носити індивідуальний характер.

Хочемо зазначити досить важливий момент, який негативно впливає на інформаційну безпеку учнів. Державою не передбачено фінансування коштів школам для закупівлі ними ліцензійного комп'ютерного забезпечення. У зв'язку з цим вчителі інформатики вимушені встановлювати на шкільні

комп’ютери піратські копії програмного забезпечення, які не виконують всіх необхідних функцій у повній мірі. Використання таких програм не гарантує безпеку користувачам, не захищає повною мірою від вірусів та небажаної реклами і контенту. У зв’язку із цим педагоги змушені більше часу та уваги приділяти контролю за діями дитини під час роботи навіть із потенційно безпечними програмами, наприклад «Сходинки до інформатики». Дана проблема існує майже у всіх школах Херсонщини.

У рамках нашого дослідження нами був проведений педагогічний експеримент у вигляді анкетування вчителів початкових класів та батьків молодших школярів з питань безпеки дітей в інтернеті. У нашому анкетуванні приймали участь 20 вчителів та 60 батьків Херсонської спеціалізованої школи І–ІІІ ступенів №52 та Херсонської спеціалізованої школи І–ІІІ ступенів №27. Питання анкет подаються в додатках (Додаток В).

Проаналізувавши відповіді двадцяти опитаних вчителів 1–4 класів, зі стажем роботи від одного до двадцяти семи років ми зробили наступні висновки:

Вчителі орієнтуються та добре розуміють поняття «інформаційна безпека учня». Педагоги, які приймали участь в анкетуванні повністю погоджуються з необхідністю цілеспрямованого формування вчителем в учнів навичок безпечного поводження в інтернеті та цілком усвідомлюють своє значення у забезпеченні інформаційно–безпечного середовища для учнів початкових класів.

Деякі наступні відповіді подаємо у вигляді діаграм.

На питання «Чи використовуєте Ви на уроках створенні власноруч медіапродукти? (презентації, відео, аудіозаписи тощо)?» 90% опитаних вчителів відповіли, що використовують на кожному уроці, та 10% – коли є технічна можливість.

Рис. 2.1.

На питання «Які мотиви спонукають Вас до використання ІКТ на уроках?» найчастіше вчителі обирали одразу декілька варіантів відповідей. Загалом варіанти «інтерес до інновацій» та «використання ІКТ робить навчальний процес більш ефективним» обрали по 30% опитаних, а варіанти «вимога керівництва школи» та «полегшує проведення уроків» по 20% опитаних вчителів.

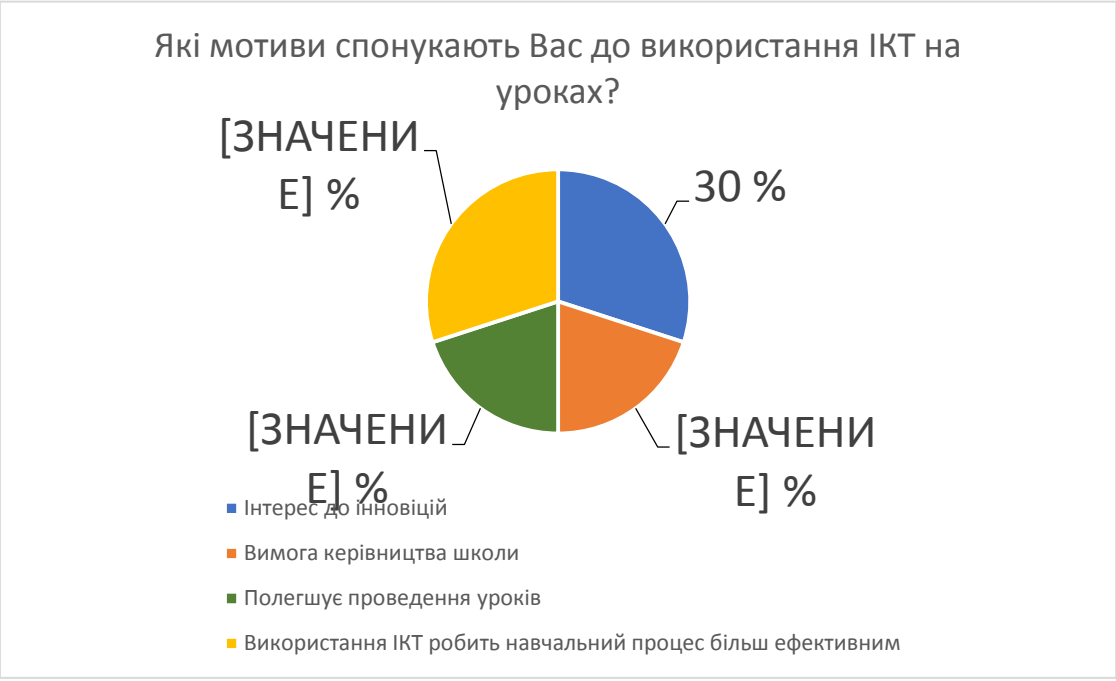


Рис. 2.2

На наступне питання анкети «Які труднощі у Вас виникають під час використання ІКТ?» ми отримали такі відповіді: «70% – недостатньо часу, 20% – відсутність необхідного технічного забезпечення у класі, 10% – моя недостатня обізнаність у цій сфері. Як ми бачимо проблемою для більшості вчителів є брак часу. Педагоги відзначають, що вимушені брати багато роботи додому, адже не встигають якісно підготуватись до уроків під час робочого часу в школі. Рішенням цієї проблеми ми бачимо наданням допомоги вчителеві у вигляді забезпеченням його матеріалами та готовими конспектами уроків, що супроводжуються презентаційним матеріалом.

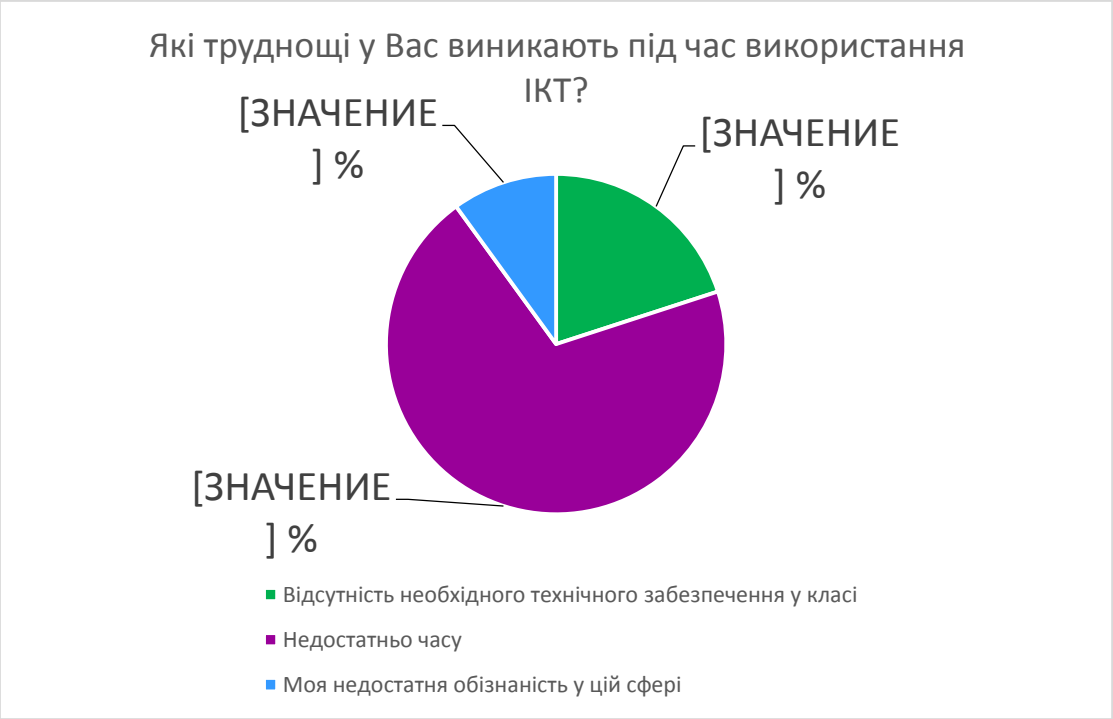


Рис. 2.3

На питання: «Який педагогічний інструментарій Ви використовуєте для забезпечення інформаційно–безпечного середовища учнів?» ми отримали наступні відповіді:

- складання пам’яток та правил;
- демонстрація презентацій та відеоматеріалів;
- бесіди;
- використання програм контролю на комп’ютерах у класі інформатики.

Загалом проаналізувавши всі отримані відповіді вчителів ми бачимо, що вони є досить обізнаними та зацікавленими у питанні забезпечення інформаційної безпеки своїх учнів. Регулярно проводяться бесіди, створюються плакати, складаються пам’ятки та правила безпечного поводження в інтернеті, на шкільних комп’ютерах використовуються програми контролю.

Наступними ми представимо результати анкетування шістдесяти батьків учнів початкових класів:

Із опитаних нами батьків 93% є активними користувачами інтернет–ресурсів та майже всі діти опитаних батьків мають власні технічні пристрої. У більшості випадків навіть декілька одразу.

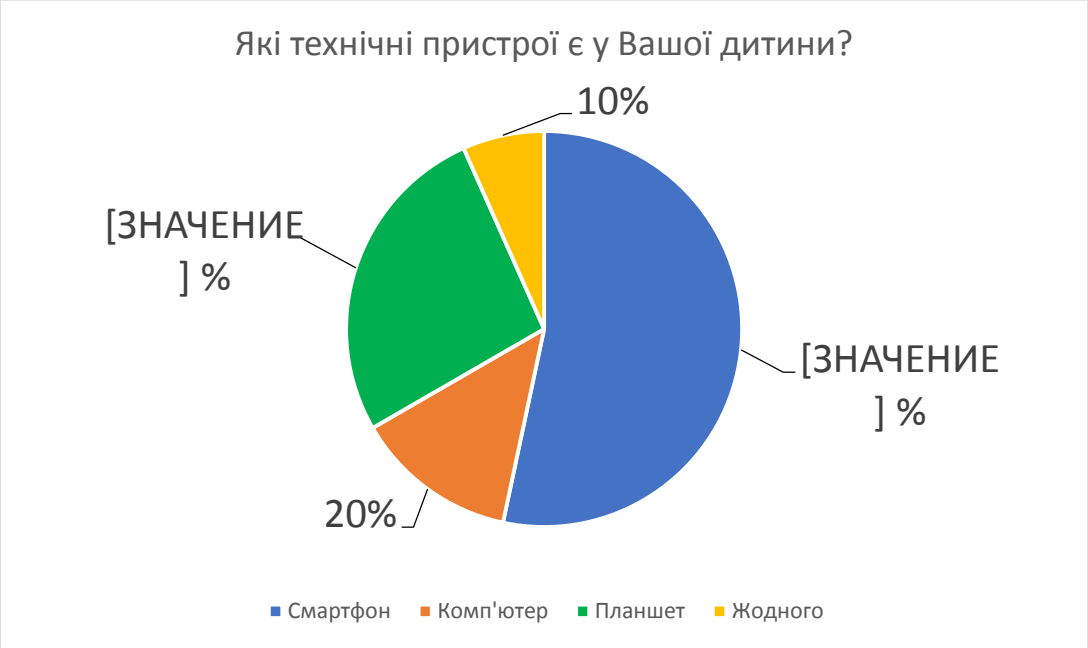


Рис. 2.4

Вибірка показала, що більше всього часу молодші школярі проводять у Viber, TikTok та Instagram – 20% щоденно, 45% – декілька разів на тиждень. Трохи менше діти користуються Facebook та Telegram. При чому добре прослідковується як збільшується час, що проводять діти в соціальних мережах з віком. У першому класі школярі проводять значно менше часу у соціальних мережах, аніж у четвертому. Збільшення часу проведеного молодшим школярем у соціальних мережах напряму пов’язаний із

зменшенням контролю за цим із боку батьків. Із віком діти починають використовувати власні технічні пристрої для пошуку навчальної інформації, батьки менше контролюють дії дитини в інтернеті і як результат школярі починають більше займатись тим, що приносить їм задоволення. Мережа TikTok зараз знаходиться на піку популярності і більшість користувачів – саме діти. При цьому дорослі, які бачили контент даної мережі, проти його перегляду дітьми, адже більшість роликів призначені для дорослої аудиторії та містять сцени насилля, агресію, пропаганду тютюну та алкоголю, небезпечні для життя та здоров'я сцени, нецензурну лексику і таке інше.

Рис. 2.5

На питання «Хто вирішує скільки часу дитина проведе з використанням технічних пристроїв та що саме вона там робитиме?» 65% батьків відповіли, що вони разом з дітьми домовляються, 25% батьків вирішують самостійно, 10% батьків дозволяють дитині вирішувати самостійно.

Рис. 2.6

85% дітей, чиї батьки приймали участь в анкетуванні переглядають телевізор щоденно, 10% – декілька разів на тиждень, 5% – декілька разів на місяць. 80% дітей переглядає мультфільми. 10% – фільми та серіали, по 5% – новини та науково–популярні передачі.

Рис. 2.7

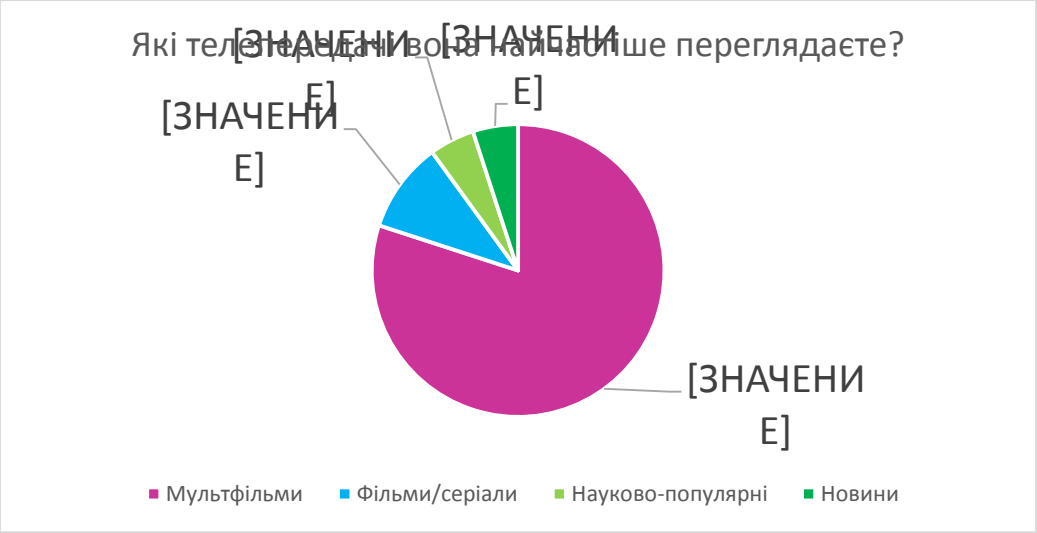


Рис. 2.8

100% батьків відповіли, що вони звертають увагу на достовірність інформації яку отримують через медіа джерела. Також переважна більшість правильно розуміє поняття «критичне оцінювання інформації».

Цікавим для нас було питання «Які основні мотиви контактів з інтернетом у Вашої дитини?». Результати, які ми отримали повністю збіглися з нашими передбаченнями, але на жаль, не бажаними результатами. 70% батьків відповіли, що їхні діти в інтернеті розважаються та відпочивають, 20% – шукають інформацію для учбових цілей, 10% – прагнуть отримати нову інформацію. Ми, як педагоги звичайно прагнемо до того, щоб молодші школярі використовували інтернет для навчання, пошуку цікавої та головне корисної інформації для себе.

Рис. 2.9

Зважаючи на те, що учні початкових класів ще не здатні до повноцінного критичного мислення та аналізу інформації, для нас були важливі та цікаві відповіді на наступне запитання «Яким чином Ви контролюєте дії своєї дитини в інтернеті?». Не можемо сказати, що відповіді нас цілком задовольнили, адже 60% опитаних батьків лише запитують у дитини про її дії в інтернеті, 15% взагалі не контролюють дії дитини в інтернеті, 10% переглядають історію браузера та лише 15% використовують програми батьківського контролю.

При цьому більшість (65% опитаних батьків) вважають, що займатися просвітою дітей щодо безпечної поведінки в інтернеті мають саме вони. 35% батьків відповіли що вчителі та батьки мають співпрацювати із даного питання.

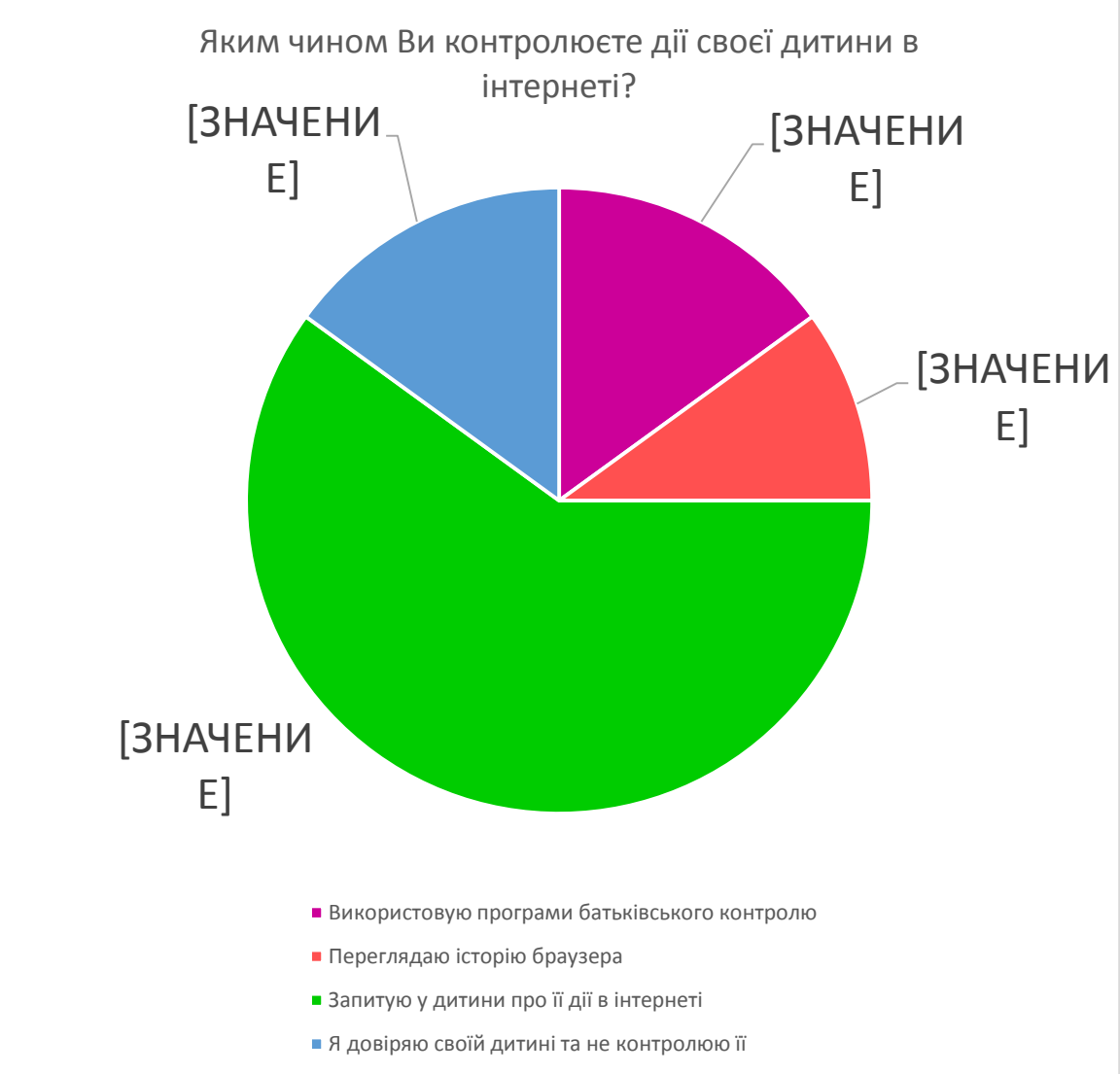


Рис. 2.10

Більше половини батьків (60%) не читають разом з дитиною газет та журналів. Інші читають книжки, енциклопедії, комікси про супергероїв та подібні журнали розважального характеру, «Розумашки», «Саша і Маша», «Їжак».

Проведене нами анкетування та аналіз отриманих відповідей вчителів та батьків учнів початкових класів дозволили зробити наступні висновки:

- Як вчителі так і батьки розуміють важливість створення інформаційно–безпечного середовища для дитини.
- Існує проблема його повноцінного забезпечення для дитини через недостатню обізнаність дорослих.
- Лише 15% батьків використовують програми батьківського контролю. Переважна більшість лише запитують у дитини про її дії в інтернеті.
- Вчителі не мають достатньо часу для підготовки до уроків з використанням ІКТ. Також ті вчителі, які мають стаж роботи більше двадцяти років звикли вчити дітей без використання технічних пристроїв. Існує проблема недостатньої обізнаності вчителів у цій сфері.
- Батьки учнів першого класу більше обмежують своїх дітей від соціальних мереж порівняно з батьками учнів четвертих класів. Чітко прослідковується збільшення часу, що проводить дитина у віртуальному світі.

2.2 Вивчення педагогічного інструментарію по забезпеченню інформаційно–безпечного середовища молодших школярів та розробка структурно-функціональної моделі

Як ми вже зазначали, у сучасному світі освіта та технології тісно пов’язані. Тому вчителі мають відповідати сучасним запитам суспільства та використовувати у своїй роботі різні технологічні інструменти, які будуть

підвищувати інтерес та мотивацію учнів до навчання. Проте головною вимогою при виборі такого інструментарію для педагога має бути безпека його використання.

Косович О. К. пропонує досить широкий перелік інструментів освітніх технологій для вчителів [20]. Ми хочемо виділити основні із них.

Перша група включає соціальні аспекти навчання. Наведені нижче інструменти використовують можливості соціальних медіа для допомоги школярам у процесі навчання, а педагогам для взаємодії: Edmodo – це освітній сайт, соціальна мережа схожа на Facebook, на якій спілкуються вчителі та учні щодо навчального матеріалу. EduBlogs платформа на якій можна вести свій власний блог, групами або ж усім класом. Добре використовувати при груповій роботі учнів. Skype можна використовувати для нарад вчителів, проведення батьківських зборів в умовах дистанційного навчання. За допомогою ресурсу Wikispaces вчитель має можливість надсилати учням онлайн матеріали уроків, додаткову інформацію, презентаційні матеріали, допоміжний матеріал для домашньої роботи Pinterest – вчитель може прикріпити практично будь–яке зображення, яке вважає необхідним. Можна використовувати як власну папку–сховище планів уроків, наочного матеріалу і таке інше.

Друга група освітніх інструментів зорієнтована безпосередньо на навчання і допоможе зробити урок більш цікавим та ефективним: MangaHigh та FunBrain містять безліч освітніх ресурсів з навчання математики в ігровій формі. Educreations – це онлайн–інструмент, використовуючи який вчитель може створити власне відео та навчити цьому учнів. Згодом діти зможуть навіть самостійно створювати відео до відповідних навчальних тем. З використанням Animoto можна легко виготовити відео–урок або ж розробити мультимедійне забезпечення до уроку, і швидко надіслати ці матеріали дітям. Система Socrative являє собою набір дидактичних ігор та вправ для дітей, які вчитель може відстежувати та оцінювати. Перевагою є те, що вона доступна до використання на будь–якому пристрої.

Третя група технічних інструментів дозволяє об’єднати тематично важливі уроки і допомогти у створенні учнівських проектів: Planboard– цей онлайн–інструмент створений спеціально для вчителів, він допомагає оцінити і упевнитися, наскільки добре організовані уроки і наскільки правильно проходить шкільний день. Timetoast являє собою онлайн помічника у розробленні проєкту. За його допомогою учні можуть спланувати свою роботу буквально по хвилинам. Capzles допомагає зберігати ріні фото–, відео–, та мультимедіа матеріали в одному місці, для того аби в подальшому було зручно використати їх для створення проєкту. Ще одним сервісом який допомагає вчителеві у створенні презентаційного забезпечення до уроку є онлайн ресурс Prezi. Все більшої популярності у сфері освіти набирають QR–коди. Для того аби створити і використовувати QR–код необхідним є ще один інструмент – Delivr, зараз він є майже на всіх сучасних смартфонах. Дітям особливо подобається навчатися з використанням QR–кодів. Хочемо відмітити і YouTube, адже він є надзивайно популярним у всьому світі, проте деякі школи не користуються ним, хоча на YouTube є багато пізнавальних навчальних відео матеріалів. Під час навчального процесу можна використовуватиосвітні канали, яких існує безліч, наприклад TED–Ed.

Наступні інструменти допоможуть не втрачати зв'язок, а також організовувати, мультимедійні уроки. Наприклад такий інструмент як Popplet помічник у створенні інтелектуальних карт. За допомогою цього ресурсу можна легко створити інтелектуальні карти та обмінятися ними. Google Earth відкриває безліч можливостей для вивчення досліджую світ. Сидячи в класі можна побувати на декількох онлайн екскурсіях за один урокю З допомогою LiveBinders можна підключитися та працювати з інтерактивною дошкою. Записати аудіо для учнів можна за допомогою такого інструменту як AudioBoo. [20].

Ми розробили власну модель по забезпеченню інформаційно–безпечного середовища. Пропонуємо досягати мети дотримуючись

принципів системності, науковості, зв’язку з життям, індивідуального підходу та доступності. При цьому використовувати в освітньому процесі компетентісний, особисто–орієнтований та трисуб’єктний підходи. З активним включенням бесід, демонстраційних матеріалів, моделюванням ситуацій та використанням дискусій. Використання проєктної роботи даватиме гарні результати у засвоєнні інформації учнями, адже є продуктом їх власної діяльності. Те ж саме можна сказати і про лепбук виготовлений учнями самостійно або в групах.

Окремо ми виділяємо такі організаційно–педагогічні умови:

- Створення позитивної мотивації до використання мережевого етикету. Важливо аби учень усвідомив власну потребу у своїй безпеці в інформаційно–комунікаційному просторі;
- Наявність технічного забезпечення та безпечних мережевих сервісів у навчальному процесі передбачає гарне технічне оснащення школи сучасним обладнанням та ліцензійованим програмним забезпеченням;
- Урахування життєвого та навчального досвіду дітей молодшого шкільного віку. Мається на увазі те, що вся інформація яка подається учням має бути розрахована на їхній вік.

При успішному виконанні всіх цих умов будуть забезпеченні на високому рівні такі критерії та показники: Мотиваційний – передбачає усвідомлення учнем потреби в своїй інформаційній безпеці. Когнітивний – сформованість цілісної системи сучасної картини світу. Діяльнісний – забезпечує вміння критично мислити, приймати правильні та виважені рішення. І звичайно рефлексивний, а саме здатність об’єктивно оцінити свої дії в інтернеті та їх наслідки.

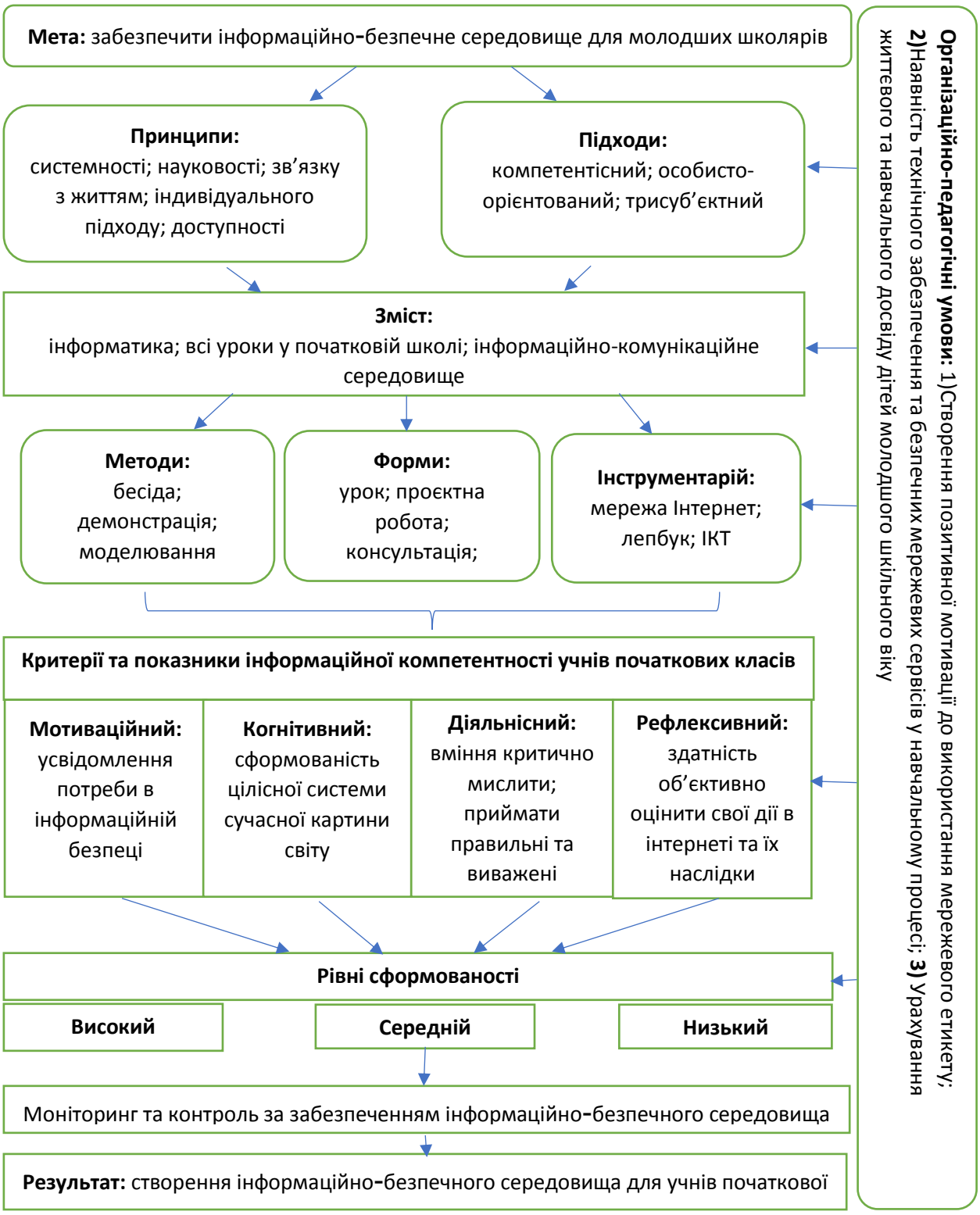


Рис. 2.1 Структурно–функціональна модель забезпечення інформаційно–безпечного середовища для учнів початкових класів

При дотриманні всіх структурно–функціональних елементів моделі буде створене інформаційно–безпечне середовище для учнів початкової школи.

2.3 Методичні рекомендації щодо підвищення рівня інформаційної безпеки молодших школярів

Провівши педагогічний експеримент у рамках нашого дослідження ми виділили головні недоліки у роботі вчителів та батьків і розробили методичні рекомендації для їх усунення.

Ми радимо вчителям комплексно використовувати програмне забезпечення для захисту шкільних комп'ютерів від вірусів, фільтрування контенту мережі Інтернет. Це можуть бути такі програми як наприклад, NetOp School, AdBlock.

Регулярне поновлення списків «білих» та «чорних» сайтів на шкільних комп'ютерах також підвищить рівень інформаційної безпеки для школярів. Хоча здавалося на уроці дії дитини знаходяться під керівництвом вчителя, все одно учні встигають відвідувати заборонені сайти, тому використання такого програмного забезпечення вважаємо необхідним.

Проведення регулярних бесід з дітьми на тему безпечного поводження в інтернеті та навчання їх мережевому етикету буде ефективним методом профілактики зіткнення учнів з інтернет загрозами. Із цією ж метою радимо створення разом з учнями правил користування інтернетом, виготовлення з ними стенду в клас. Постійне нагадування дітям про них різними способами (презентації, відеоматеріали, бесіди).

Доцільно проводити виховні години присвячені темі безпечного інтернету. Вчити учнів визначати правдивість інформації знайденої в інтернеті, вміти її фільтрувати та критично оцінювати.

Важливо також і вміти зацікавлювати учнів альтернативними видами діяльності, без використання мережі інтернет. Наприклад знайти необхідну інформацію в енциклопедії (добре буде мати невеличку бібліотеку в класі).

Необхідно проводити просвіту не лише дітей з даного питання, а і їх батьків. Наприклад, приділити деякий час питанню безпечного інтернету на батьківських зборах. Познайомити батьків із способами захисту дітей від інтернет загроз, пояснити необхідність використання програм батьківського контролю та навчити їх використовувати.

Батькам у першу чергу рекомендуємо використовувати програми батьківського контролю на смартфоні, планшеті та комп'ютері дитини. Встановлювати на всіх технічних пристроях програми захисту від вірусів та фільтрування контенту мережі Інтернет.

Дуже часто діти стикаються із проблемами в інтернеті і мовчать про них, чим тільки погіршують свій стан. Для того аби уникнути таких ситуацій варто встановити довірчі відносини між батьками та дитиною. Саме вони допоможуть уникнути негативних наслідків якщо дитина зіштовхнеться із кібербулінгом, шахрайством, звабленням в інтернеті і т. д.

Батькам необхідно розуміти важливість співпраця із вчителями та підтримувати ті правила, які створенні у класі. При цьому вчити свою дитину аналізувати інформацію та критично оцінювати її. На власному прикладі показувати, що не можна сліпо вірити всьому, що вона бачить в інтернеті чи по телевізору.

На основі результатів експерименту нами були розроблені методичні рекомендації для вчителів та батьків учнів початкових класів. Важливо зазначити, що тільки сумісне дотримання рекомендацій вчителями та батьками, їх співпраця дасть позитивний результат по створенню інформаційно–безпечного середовища для учнів. Також на допомогу вчителеві нами був розроблений презентаційний матеріал для батьків, який покликаний просвітити їх з питання інтернет безпеки дітей та презентаційний матеріал для учнів, у якому містяться правила поводження в інтернеті та поради як захистити себе у віртуальному світі.

ВИСНОВКИ

На основі поставлених завдань було зроблено наступні висновки:

1. Ключовими для нашого дослідження є наступні дефініції:

– інформаційна безпека молодшого школяра – це стан захищеності учнів молодшої школи від загроз, які можуть бути викликані інформаційним впливом і негативно діяти на психіку та соціальний, культурний розвиток дитини.

– педагогічний інструментарій – це сукупність форм, методів, прийомів і засобів педагогічної взаємодії суб'єктів освіти та виховання. Вони, являють собою специфічні (педагогічні) інструменти, за допомогою яких здійснюється формування необхідних особистісних якостей дитини.

– інформаційно–комунікаційні технології – це технології, пов’язані зі створенням, збереженням, передачею, обробкою та управлінням інформацією. Цей термін включає в себе всі технології, що використовуються для спілкування та роботи з інформаційними ресурсами.

Ці терміни будуть покладенні в основу нашого дослідження.

2. Проведена нами робота над вивченням питання впливу медіатизації на процес навчання учнів початкової школи дозволила зробити висновок, що використання різноманітних інформаційних ресурсів, таких як: web–браузери, web–сайти, пошукові системи, електронна пошта, відео–конференції та різноманітні соціальні мережі позитивно впливають на процес навчання учнів початкової школи за умови грамотного їх використання вчителем. Поєднуючи традиційні методи навчання та сучасні інформаційні технології педагог має можливість зробити процес навчання гнучким та індивідуальним.

3. Детально дослідивши та проаналізувавши інтернет загрози як психолого–педагогічну проблему ми можемо виділити такі основні інтернет

загрози для молодших школярів, як: віруси, небажаний контент, недостовірна інформація, інтернет–звaблення, кібер–хуліганство, шпигунське програмне забезпечення та соціальні мережі. Все це становить загрозу, так як психіка дитини молодшого шкільного віку ще не достатньо сформована для того, аби вміти самостійно аналізувати інформацію яка є в інтернеті. Молодші школярі легко можуть натрапити на інформацію, яка негативно вплине на їх психіку та перешкоджатиме формуванню правильних життєвих цінностей та норм моралі.

4. Проведена нами компаративістика дала можливість зробити висновок, що Україні є куди рости та розвиватись. Прикладом для нашої країни може бути досвід Кореї та Ізраїлю. Але ми беззаперечно рухаємось у правильному напрямку, досліджуючи проблему інформаційної безпеки учнів ми стаємо ближчими до досягнення високих результатів. Загалом, інтернет мережа не має національних кордонів. Для створення безпечного інформаційного середовища для дітей в інтернеті необхідно об’єднувати зусилля урядів та суспільства всіх країн на міжнародному рівні. Через це міжнародні організації і розробили документи які спрямованні на захист дітей від порушення їх прав через використання ІКТ. Основним міжнародним документом зобов’язального характеру в цій сфері є положення Конвенції ООН про права дитини.

Нами було проведено анкетування вчителів початкових класів та батьків молодших школярів з питань безпеки дітей в інтернеті. Проаналізувавши відповіді ми зробили наступні висновки:

- Як вчителі так і батьки розуміють важливість створення інформаційно–безпечного середовища для дитини.
- Існує проблема його повноцінного забезпечення для дитини через недостатню обізнаність дорослих.
- Лише 15% батьків використовують програми батьківського контролю. Переважна більшість лише запитують у дитини про її дії в інтернеті.

- Вчителі не мають достатньо часу для підготовки до уроків з використанням ІКТ. Також ті вчителі, які мають стаж роботи більше двадцяти років звикли вчити дітей без використання технічних пристроїв. Існує проблема недостатньої обізнаності вчителів у цій сфері.
- Батьки учнів першого класу більше обмежують своїх дітей від соціальних мереж порівняно з батьками учнів четвертих класів. Чітко прослідковується збільшення часу, що проводить дитина у віртуальному світі.

5. Дослідивши педагогічний інструментарій вчителя по забезпеченню інформаційно–безпечного середовища ми умовно розділили його на чотири групи. Перша група включає соціальні аспекти навчання; друга зорієнтована безпосередньо на навчання і допомагає зробити урок більш ефективним; третя допомагає у створенні проектів та об'єднанні тематично важливих уроків; четверта група педагогічних інструментів допоможе залишатися на зв'язку та організовувати, будувати мультимедійні уроки.

Ми розробили власну модель по забезпеченню інформаційно–безпечного середовища. Пропонуємо досягати мети дотримуючись принципів системності, науковості, зв'язку з життям, індивідуального підходу та доступності. При цьому використовувати в освітньому процесі компетентісний, особисто–орієнтований та трисуб'єктний підходи. З активним включенням бесід, демонстраційних матеріалів, моделюванням ситуацій та використанням дискусій. Використання проєктної роботи даватиме гарні результати у засвоєнні інформації учнями, адже є продуктом їх власної діяльності. Те ж саме можна сказати і про лепбук виготовлений учнями самостійно або в групах.

Окремо ми виділяємо такі організаційно–педагогічні умови:

- Створення позитивної мотивації до використання мережевого етикету. Важливо аби учень усвідомив власну потребу у своїй безпеці в інформаційно–комунікаційному просторі;

- Наявність технічного забезпечення та безпечних мережевих сервісів у навчальному процесі передбачає гарне технічне оснащення школи сучасним обладнанням та ліцензійованим програмним забезпеченням;
- Урахування життєвого та навчального досвіду дітей молодшого шкільного віку. Мається на увазі те, що вся інформація яка подається учням має бути розрахована на їхній вік.

При успішному виконанні всіх цих умов будуть забезпеченні на високому рівні такі критерії та показники: Мотиваційний – передбачає усвідомлення учнем потреби в своїй інформаційній безпеці. Когнітивний – сформованість цілісної системи сучасної картини світу. Діяльнісний – забезпечує вміння критично мислити, приймати правильні та виважені рішення. І звичайно рефлексивний, а саме здатність об’єктивно оцінити свої дії в інтернеті та їх наслідки.

6. На основі результатів експерименту нами були розроблені методичні рекомендації для вчителів та батьків учнів початкових класів. Важливо зазначити, що тільки сумісне дотримання рекомендацій вчителями та батьками, їх співпраця дасть позитивний результат по створенню інформаційно–безпечного середовища для учнів. Також на допомогу вчителеві нами був розроблений презентаційний матеріал для батьків, який покликаний просвітити їх з питання інтернет безпеки дітей та презентаційний матеріал для учнів, у якому містяться правила поводження в інтернеті та поради як захистити себе у віртуальному світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Артюх О. Р., Тілікіна Н. В. Аналітичний звіт за результатами опитування батьків щодо використання ними телефонів/смартфонів та володіння навичками інтернет–безпеки. *Державний інститут сімейної та молодіжної політики.* 2021. URL: https://dismp.gov.ua/onlajn–opituvannya–batkiv–shhodo–vikoristannya–telefoniv–smartfoniv/
2. Безпечне користування сучасними інфорамційно–комунікативними технологіями: методичні рекомендації. К. : Україна, 2010. 72 с. URL: https://www.saferinternetday.org/en–GB/home
3. Богатырева Ю. И. Создание инфобезопасной среды образовательного учреждения. *Известия Тульского государственного университета*. Гуманитарные науки. 2013. Выпуск № 3–2. С. 14–25.
4. Бурячок В. Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за ред. В. Б. Толубка. К. : ДУТ, 2015. 288 с.
5. Вітюк О. Комплексе застосування інформаційно–комунікаційних технологій у навчально–виховному процесі. *Директор школи*. 2014. №10. С. 41–45.
6. Галаган І. Використання інформаційно–комунікаційних технологій у початкових класах. *Початкова школа*. 2013. №2. С.33–34.
7. Ґудзик І. Інформаційна грамотність як важлива ознака компетентності учня. *Шлях освіти*. 2005. №4. С. 34–38.
8. Гулай В. В. Завідувач кафедри міжнародної інформації Василь Гулай про створення кібервійськ в Україні та досвід Ізраїлю. 2021. URL: https://lpnu.ua/news/zaviduvach-kafedry-mizhnarodnoi-informatsii-vasyl-gulai-pro-stvorennia-kiberviisk-i-dosvid

9. Дітковська Л. А. Для кого Інтернет може бути небезпечний. *Інформаційні технології і засоби навчання*. 2007. № 3. URL: www.ime.edu–ua.net/em3/content/07dladbm.htm
10. Жарков Я. Небезпеки особистості в інформаційному просторі. *Юридичний журнал*. 2007. № 2. URL: http://www.justinian.com.ua/article.php?id=2554
11. Захист дітей у цифровому середовищі: рекомендації для батьків та освітян. *Міжнародний союз електрозв'язку*. 2020. URL: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/1/za–initsiativi–mintsifri–pidgotuvali–rekomendatsii–shchodo–zakhistu–ditey–u–tsifrovomu–seredovishchi/COP–Guidelines–for–Parents–Educators–UAfin.pdf.
12. Золотар О.О. Інформаційна безпека людини :теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.
13. Інформаційна безпека держави у контексті протидії інформаційним війнам : навч. посіб. / за ред. В. Б. Толубка. К. : НАОУ, 2004. 177 с
14. Ісаєва В. О. Культура информационной безопасности. *Сборник четвертой открытой научно–практической конференции «безопасность человека в информационном пространстве»*. 2016. URL: https://www.tomintech.ru/lyceum/media/uploads/Sbornik%20Koferenz%20InfBezopasn2016.pdf.
15. Кобко Є. В. Інформаційна безпека в системі національної безпеки: сучасність і перспективи. *National law journal: teory and practice.* 2019. URL: http://www.jurnaluljuridic.in.ua/archive/2019/2/part_2/11.pdf.
16. Ковалева, Н. Н. Информационное право России : учеб. пособ. : Издательско–торговая корпорация "Дашков и Ко", 2007. 148 с
17. Ковальчук В. Н. Забезпечення інформаційної безпеки старшокласників у комп'ютерно–орієнтованому навчальному середовищі : дис. канд. пед. наук: 13.00.10. Житомир, 2011. 291 с

18. Ковальчук В. Н. Проблеми інформаційної безпеки дітей різних вікових категорій. *Комп'ютер у школі та сім'ї*. 2010. №8. С. 58–62.
19. Кондратенко Л. Особливості сприймання сучасними учнями початкової школи навчальної інформації. *Початкова школа*. 2018. №9. С. 14–17.
20. Косович О. К. Сучасні освітні інструменти для вчителів. 2018. URL: https://osvita.cv.ua/suchasni–osvitni–instrumenty–dlya–vchyteliv/
21. Коткова В. В. Дидактичний комплекс формування інформатичних компетентностей майбутніх учителів початкових класів. *Інформатика*. 2012. №3. С. 51–57. URL: http://ekhsuir.kspu.edu/bitstream/handle/123456789/3932/%d0%a1%d1%82%d0%b0%d1%82%d1%82%d1%8f_%d0%9a%d0%be%d1%82%d0%ba%d0%be%d0%b2%d0%be%d1%97_%d0%92.%d0%92..PDF?sequence=1&isAllowed=y
22. Кочарян А. Б., Гущина Н.І. Виховання культури користувача Інтернету. Безпека у всесвітній мережі: навчально-методичний посібник. Київ, 2011. С. 5
23. Литовченко І. В., Максименко С. Д., Болтівець С. І. Діти в Інтернеті: як навчити безпеці в віртуальному світі. К. : Вид. ТОВ Видавничий будинок "Аванпост–Прим". 2010. 48 с.
24. Малишевська І., Малишевський О. Виявлення змін процесу розвитку особистості учня під впливом інформатизації освіти. *Інфоматика*. 2009. №1. С. 85–92.
25. Малых Т. А. Педагогические условия развития информационной безопасности младшего школьника : автореф. дисс. канд. пед. наук. Иркутск, 2008. 27 с.
26. Мельничук І. О. Етапи формування інформаційної культури учнів. *Управління школою*. 2006. №25. С. 27–30.
27. Оспенникова Е. В. Информационно–образовательная среда современного школьника. *Школа технологии*. 2002. №4. С. 25–36.

28. Петухова Л. Є. Інформатичні компетентності майбутнього вчителя початкових класів (В моделі трисуб'єктної дидактики) : навч. метод. посіб. для студентів ВНЗ. Херсон: Вид–во ХДУ, 2010. 524 с.
29. Петухова Л. Є. Теоретичні основи підготовки вчителів початкових класів в умовах інформаційно–комунікаційного педагогічного середовища: Монографія. Херсон: Айлант, 2007. 200 с.
30. Підгорна Т. В., Берест І. Деякі аспекти організації інформаційної безпеки учнів. *Педагогіка і психологія професійної освіти*. 2014. №6. С. 70–78.
31. Полат Е. С. Проблемы информационной безопасности в образовательных сетях рунет. *Лаборатория дистанционного обучения*. URL: http://distant.ioso.ru/library/publication/infobez.htm
32. Про вищу освіту : Закон України від 01.07.2014 р. № 1556–VII. Дата оновлення: 28.09.2017. URL: http://zakon2.rada.gov.ua/laws/show/1556–18 (дата звернення: 15.11.2017).
33. Саттарова Н. И. Информационная безопасность школьников в образовательном учреждении : дисс. канд. пед. наук : 13.00.01. С.–Петерб. акад. последипл. пед. образования. С.–Пб., 2003. 215 с.
34. Сащук Г. М. Інформаційна безпека в системі забезпечення національної безпеки. URL: http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php.
35. Створення інформаційно–освітнього середовища сучасного закладу освіти України: матеріали Всеукраїнської науково–практичної конференції / За ред. Г. А. Коломоєць, О. М. Мельник, С. М. Грицай, А. В. Вознюк (м. Київ, 15 березня 2019 року). Суми: НВВ КЗ СОІППО, 2019. 124 с.
36. Створення інформаційно–освітнього середовища сучасного закладу освіти України: матеріали Всеукраїнської науково–практичної конференції. За ред. Г. А. Коломоєць, О. М. Мельник, С. М. Грицай, А.

В. Вознюк. (м. Київ, 15 березня 2019 року). Суми: НВВ КЗ СОІППО, 2019. 124 с.

37. Ступак Л. Розвиток інформаційної компетентності в початковій школі. *Сучасна школа України.* 2015. №9. С. 24–29.
38. Типові освітні програми для закл. загальної середньої освіти: 1–2 та 3–4 класи. К.: Видавництво «Світоч», 2019. 336 с.
39. Фурашев В. М. Сутність та визначення понять “інформаційна безпека” і “безпека інформації”. *“Правова інформатика”*. 2012. № 2(34). С. 51 – 59.
40. Черних О.О. Безпека дитини в інтернеті: від загроз до можливостей. URL: https://umity.in.ua/course/?id=112079
41. Черних О.О. Ч49 Онлайк: навчально–методичний посібник., К.: BAITE, 2020. 108 с. URL: https://www.osce.org/files/f/documents/0/f/483533.pdf
42. Шастіна А. Ю. Роль вчителя початкової школи у забезпеченні інформаційно–безпечного середовища для учнів. *Науковий простір студента: пошуки і знахідки (ч. 2): матеріали VII Всеукраїнської науково–практичної студентської інтернет–конференції* (24 березня 2021 року): збірник тез. Київ: НПУ імені Драгоманова, 2021. С. 357–361. URL: https://drive.google.com/file/d/1adhiAKRj6nx00pUVlbaxIvC0dvutch8d/view

ДОДАТКИ

Додаток А

Сертифікат підвищення кваліфікації

№ 115462
від 28.06.2021,
м. Київ

Центр нової освіти
Івана Іванова

СЕРТИФІКАТ
підвищення кваліфікації

засвідчує, що

Шастіна Анастасія Юріївна

завершив(ла) дистанційне навчання в онлайн-курсі

"Безпека дитини в Інтернеті: від загроз до можливостей"

обсягом 2 акад. год. (0,06 кредиту ЄКТС) згідно програми підвищення кваліфікації за напрямом "інформаційні технології" та вдосконалив(ла) такі компетентності: професійно-педагогічна, інформаційно-цифрова.

Розробник курсу: Олена Черних, засновниця Центру кращого Інтернету; координаторка Дня безпечного Інтернету 2013-2020; кандидатка педагогічних наук; авторка навчально-методичних посібників з безпеки в Інтернеті та прав людини.

Веб-адреса курсу: *https://umity.in.ua/course/?id=112079*

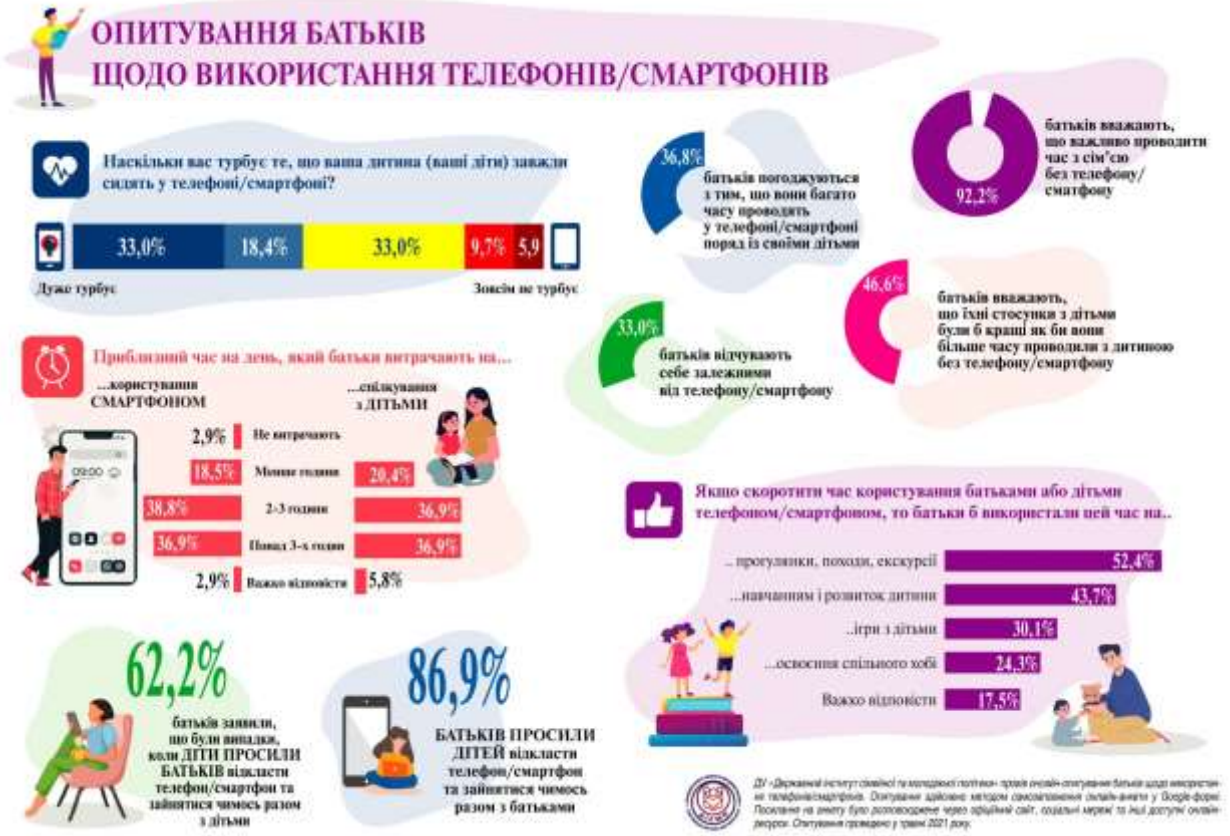
УМІТИ

Навчання відбувалось на веб-платформі УМІТИ.УКР і передбачало опрацювання теоретичних матеріалів, обговорення та підсумкове тестування.

Іван Іванов
засновник Центру нової освіти та платформи "УМІТИ", тренер з інноваційних технологій, педагогічний дизайнер

Додаток Б

Опитування батьків щодо використання телефонів



Додаток В

Діагностика стану організації інформаційної безпеки в школах Херсонщини

Анкета для батьків

Ваша дитина навчається у ____ класі.

1. Які з перерахованих нижче технічних пристроїв є у Вашої дитини?

А. смартфон
Б. комп'ютер
В. планшет

2. Як часто Ваша дитина проводить час у наступних соц. мережах? (5–щоденно, 4–декілька разів на тиждень, 3–декілька разів на місяць, 2–раз на місяць, 1–раз в житті, 0–ніколи)

Viber –____ ;
Instagram –____ ;
Facebook –____ ;
Skype –____ ;
WhatsApp –____ ;
Twitter –____ ;
Telegram –____ ;
TikTok –____ .

3. Хто вирішує скільки часу дитина проведе з використанням технічних пристроїв та що саме вона там робитиме?

А. дитина самостійно вирішує
Б. я вирішую
В. ми разом домовляємось
Г. інша відповідь _____.

4. Чи звертаєте ви увагу на достовірність інформації яку отримуєте через медіа джерела?

А. так
Б. ні

5. Як ви розумієте поняття «критичне оцінювання інформації»?

_____.

6. Як часто Ваша дитина переглядає телевізор?

А. щоденно
Б. декілька разів на тиждень
В. декілька разів на місяць
Г. ніколи

7. Які телепередачі вона найчастіше переглядаєте?

А. мультфільми
Б. фільми/серіали
В. науково–популярні
Г. новини

8. Як часто ви користуєтесь інтернетом?

А. щоденно
Б. декілька разів на тиждень
В. декілька разів на місяць
Г. ніколи

9. Наскільки часто Ваша дитина грає в комп'ютерні ігри?

А. щоденно
Б. декілька разів на тиждень
В. декілька разів на місяць
Г. ніколи

10. Які основні мотиви контактів з інтернетом у Вашої дитини?

А. пошук матеріалів для учбових цілей
Б. прагнення отримати нову інформацію
В. прагнення розважатися та відпочивати
Г. прагнення віртуальної втечі від реального життя

11. Яким чином Ви контролюєте дії своєї дитини в інтернеті?

А. використовую програми батьківського контролю
Б. переглядаю історію браузера
В. запитую у дитини про її дії в інтернеті
Г. я довіряю своїй дитині та не контролюю її

12. Хто повинен вчити дитину безпечній поведінці в інтернеті?

А. вчителі
Б. батьки
В. вчителі та батьки
Г. дитина має навчитись самостійно

13. Чи читаєте Ви разом з дитиною газети або журнали? Якщо так, вкажіть які:

_____ .

Анкета для вчителів

1. У якому класі ви викладаєте?

_____.

2. Який Ваш стаж роботи?

_____.

3. Як Ви розумієте поняття інформаційна безпека учня?

А. стан захищеності життєво важливих інтересів учня

Б. стан учня за якого йому нічого не загрожує в інтернеті

В. гарантування доступу учня тільки до достовірної інформації

Г. важко відповісти

Д. _____(Ваш варіант).

4. Чи вважаєте Ви необхідним цілеспрямоване формування вчителем в учнів навичок безпечного поводження в інтернеті?

А. так

Б. ні

5. Чи використовуєте Ви на уроках створенні власноруч медіапродукти? (презентації, відео, аудіозаписи тощо)?

А. майже на кожному уроці
Б. коли є технічна можливість
В. на відкритих уроках
Г. не маю достатньої підготовки для цього

6. Який педагогічний інструментарій Ви використовуєте для забезпечення інформаційно–безпечного середовища учнів?

_____.

7. Які мотиви спонукають Вас до використання ІКТ на уроках?

А. інтерес до інновацій
Б. вимога керівництва школи
В. полегшує проведення уроків

Г. використання ІКТ робить навчальний процес більш ефективним

8. Які труднощі у Вас виникають під час використання ІКТ?

А. відсутність необхідного технічного забезпечення у класі
Б. недостатньо часу
В. моя недостатня обізнаність у цій сфері
Г. інша відповідь_____.

Додаток Г

КОДЕКС АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ ХЕРСОНСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ

Я, Шастіна Анастасія Юріївна, учасник(ця) освітнього процесу Херсонського державного університету, **УСВІДОМЛЮЮ**, що академічна доброчесність – це фундаментальна етична цінність усієї академічної спільноти світу.

ЗАЯВЛЯЮ, що у своїй освітній і науковій діяльності **ЗОБОВ'ЯЗУЮСЯ**:

– дотримуватися:

- вимог законодавства України та внутрішніх нормативних документів університету, зокрема Статуту Університету;
- принципів та правил академічної доброчесності;
- нульової толерантності до академічного плагіату;
- моральних норм та правил етичної поведінки;
- толерантного ставлення до інших;
- дотримуватися високого рівня культури спілкування;

– надавати згоду на:

- безпосередню перевірку курсових, кваліфікаційних робіт тощо на ознаки наявності академічного плагіату за допомогою спеціалізованих програмних продуктів;
- оброблення, збереження й розміщення кваліфікаційних робіт у відкритому доступі в інституційному репозитарії;
- використання робіт для перевірки на ознаки наявності академічного плагіату в інших роботах виключно з метою виявлення можливих ознак академічного плагіату;

– самостійно виконувати навчальні завдання, завдання поточного й підсумкового контролю результатів навчання;

– надавати достовірну інформацію щодо результатів власної навчальної (наукової, творчої) діяльності, використаних методик досліджень та джерел інформації;

– не використовувати результати досліджень інших авторів без використання покликань на їхню роботу;

– своєю діяльністю сприяти збереженню та примноженню традицій університету, формуванню його позитивного іміджу;

– не чинити правопорушень і не сприяти їхньому скоєнню іншими особами;

– підтримувати атмосферу довіри, взаємної відповідальності та співпраці в освітньому середовищі;

– поважати честь, гідність та особисту недоторканність особи, незважаючи на її стать, вік, матеріальний стан, соціальне становище, расову належність, релігійні й політичні переконання;

– не дискримінувати людей на підставі академічного статусу, а також за національною, расовою, статевою чи іншою належністю;

– відповідально ставитися до своїх обов'язків, вчасно та сумлінно виконувати необхідні навчальні та науково–дослідницькі завдання;

– запобігати виникненню у своїй діяльності конфлікту інтересів, зокрема не використовувати службових і родинних зв'язків з метою отримання нечесної переваги в навчальній, науковій і трудовій діяльності;

– не брати участі в будь–якій діяльності, пов'язаній із обманом, нечесністю, списуванням, фабрикацією;

– не підроблювати документи;

– не поширювати неправдиву та компрометуючу інформацію про інших здобувачів вищої освіти, викладачів і співробітників;

– не отримувати і не пропонувати винагород за несправедливе отримання будь–яких переваг або здійснення впливу на зміну отриманої академічної оцінки;

– не залякувати й не проявляти агресії та насильства проти інших, сексуальні домагання;

– не завдавати шкоди матеріальним цінностям, матеріально–технічній базі університету та особистій власності інших студентів та/або працівників;

– не використовувати без дозволу ректорату (деканату) символіки університету в заходах, не пов'язаних з діяльністю університету;

– не здійснювати і не заохочувати будь–яких спроб, спрямованих на те, щоб за допомогою нечесних і негідних методів досягати власних корисних цілей;

– не завдавати загрози власному здоров'ю або безпеці іншим студентам та/або працівникам.

УСВІДОМЛЮЮ, що відповідно до чинного законодавства у разі недотримання Кодексу академічної доброчесності буду нести академічну та/або інші види відповідальності й до мене можуть бути застосовані заходи дисциплінарного характеру за порушення принципів академічної доброчесності.

20.10.2021 р.	_____	Шастіна Анастасія
(дата)	(підпис)	(ім'я, прізвище)