

**ЗМІСТ**

|  |  |
| --- | --- |
| **ВСТУП**.………………………………………………………………….. | 3 |
| **РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗДОБУВАЧІВ ПОЧАТКОВОЇ ОСВІТИ ………………………..** | 7 |
| * 1. Сутність і зміст поняття «інформаційна безпека» …………………. | 7 |
| * 1. Психолого-педагогічні особливості молодших школярів як важливий аспект в організації інформаційної безпеки ….….………………… | 16 |
| * 1. Зарубіжний досвід із організації інформаційної безпеки дітей……. | 24 |
| **РОЗДІЛ 2. ДОСЛІДЖЕННЯ УМОВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УЧНІВ ПОЧАТКОВОЇ ШКОЛИ………..** | 32 |
| 2.1. Аналіз стану проблеми дослідження………………………………… | 32 |
| 2.2. Підвищення цифрової освіти членів педагогічного колективу як умова інформаційної безпеки здобувачів початкової освіти............................. | 41 |
| 2.3. Виховання культури поведінки молодших школярів під час використання цифрового середовища | 47 |
| 2.4. Інформаційно-консультативна підтримка в початковій школі через систему педагогічного дорадництва | 55 |
| 2.5. Методичні поради вчителям початкової школи, батькам з організації інформаційної безпеки……………………………………………… | 63 |
| **ВИСНОВКИ……………………………………………………………...** | 68 |
| **СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……………………………...** | 72 |
| **ДОДАТКИ…………………………………………………………………** | 80 |

**ВСТУП**

Сучасне суспільство характеризується особливо швидким розвитком інформаційно-цифорових технологій, де Інтернет і гаджети стали невід’ємною частиною повсякденного життя будь-якого члена суспільства, незалежно від віку, статі, раси, національності, приналежності до професії і, навіть, віросповідання. Окрім того, Пандемія COVID-19, повномасштабне вторгнення в Україну спонукали розробників до створення інтернет-продуктів, завдяки яким можна продовжувати освіту, спілкуватися, при цьому, без фізичної присутності в одному місці. З огляду на це, питання інформаційної безпеки набуває особливо актуального значення значення у різних сферах і галузях діяльності людини. Освіта, як основоположний компонент у розвитку особистості, сьогодні отримує багато викликів, на які потрібно реагувати дуже швидко і конструктивно. Однією з таких необхідних для вирішення освітніх проблем є формування інформативної компетентності здобувачів освіти, складовою якої є вміння чітко аналізувати отриману інформацію, адекватно реагувати, в першу чергу, задля збереження ментального і фізичного здоров’я дітей і молоді.

Про формування інформативної компетентності зазначено у Концепції Нової української школи [25], адже починаючи із наймолодшого віку, діти мають отримувати чіткі знання, розуміти правила поведінки у соціальних мережах та можливі наслідки і виклики, які несе неправильні спілкування і дії у цифровому середовищі.

На нашу думку, особливо актуальною є зазначена проблема у початковій освіті оскільки, збільшується кількість інформаційних технологій; підвищується онлайн-активність дітей, адже, починаючи із наймолодшого віку, вони є активними користувачами гаджетами і інтернетом; зростає кількість кіберзагроз. Варто зазначити, що зростання онлайн-активності здобувачів початкової освіти супроводжується низкою ризиків, таких як кібербулінг, доступ до небажаного контенту, загроза з боку онлайн-хижаків та шахраїв. Необхідним на сьогодні стає створення безпечного та захищеного середовища для навчання та розвитку дітей різного віку. Саме у початковій школі з’являється необхідність у формуванні основ безпечного використання інформаційних технологій та відповідального використання цифрових ресурсів.

Інформаційна безпека у початковій школі – це не просто навчання здобувачів початкової освіти правилам користування гаджетами і інтернетом, це створення фундаменту для безпеки у цифровому світі, який продовжує розвиватися і змінюватися. Окрім того, засвоєння школярами основ інформаційної безпеки допоможе уникати небезпек, захищати особисті дані та формувати критичне мислення, необхідне для розпізнавання потенційних загроз. З огляду на це, інформаційна безпека сьогодні є невід’ємною частиною освітнього процесу початкової освіти.

Про актуальність проблеми нашого дослідження зазначається у низці документів національного та міжнародного рівнів. Так, у Статті 17 «Конвенції про права дитини (ООН)» [26] підкреслюється важливість забезпечення доступу дітей до інформації з різних джерел та необхідність створення умов для захисту від шкідливої інформації; у «Рекомендаціях Ради Європи щодо захисту дітей в Інтернеті» [9] включено рекомендації для держав-членів щодо захисту дітей в онлайн-середовищі, включаючи питання кібербезпеки та безпечного використання Інтернету; про спеціальні положення щодо захисту даних дітей та вимоги до організацій щодо забезпечення підвищеного рівня захисту даних дітей вказано у «Директиві Європейського парламенту та Ради про захист персональних даних (GDPR)» [12]: про захист персональних даних, включаючи дані дітей, вказано у Законі України «Про захист персональних даних» [15]; про необхідність навчання дітей основам інформаційної безпеки, формування ключових компетентностей, включаючи цифрову грамотність передбачено у Законах України «Про освіту» [17] та «Про загальну середню освіту» [16]; про забезпечення безпеки дітей в цифровому середовищі та заходи щодо захисту дітей в Інтернеті вказано у «Стратегії кібербезпеки України» [47] та інші.

Окрім того, значна кількість освітніх та громадських організацій розробляють програми, які надають освітні послуги з навчання основам інформаційної безпеки для дітей. Так, наприклад, ЮНІСЕФ розроблено рекомендації та програми для підвищення рівня обізнаності дітей і молоді про кібербезпеку.

Серед науковців, у дослідженнях яких розкрито різні аспекти проблеми інформаційної безпеки, є: Р. Андерсон [64], Б. Шнеєр [68] та інші. Інформаційна безпека є актуальною і серед вітчизняних науковців. Так, у працях Т. Алєксєєнко, Р. Васильєвої, В. Горбуліна, К. Журби, Л. Канішевської, Л. Карнаух, Р. Малиношевського, Ю. Науменка, О. Спіріна, С. Федоренко, Н. Харченко, Є. Чернишової та інших.

Зважаючи на зацікавленість теоретиків і практиків проблемою інформаційної безпеки дітей і молоді, не вивченим є саме період молодшого шкільного віку, що і зумовило вибір теми нашого дослідження: «Умови інформаційної безпеки здобувачів початкової освіти».

**Мета дослідження** полягає у визначенні та обґрунтуванні ефективності умов інформаційної безпеки здобувачів початкової освіти.

**Завдання дослідження:**

1. Розкрити сутність і зміст поняття «інформаційна безпека.
2. Визначити особливості інформаційної безпеки у початковій школі.
3. Вивчити зарубіжний досвід з проблеми інформаційної безпеки у -закладах освіти.
4. Проаналізувати стан проблеми дослідження у сучасних закладах освіти.
5. Визначити та теоретично обґрунтувати умови, розробити методичні поради вчителям з інформаційної безпеки у початковій школі.

**Об’єкт дослідження:** інформаційна безпека здобувачів початкової освіти.

**Предмет дослідження**: умови інформаційної інформаційної безпеки здобувачів початкової освіти.

**Методи дослідження:**

- **теоретичні:** вивчення наукової літератури, аналіз, синтез, узагальнення для уточнення теоретичних основ інформаційної безпеки у початковій школі та визначення умов інформаційної безпеки здобувачів початкової освіти;

- **емпіричні:** спостереження, бесіда, вивчення педагогічного досвіду з метою з’ясування сучасного стану інформаційної безпеки у початковій школі.

**Теоретичне значення дослідження** полягає у визначенні та теоретичному обґрунтуванні умов інформаційної безпеки учнів початкових класів.

**Практичне значення дослідження** полягає у розробці умов, методичних порад вчителям, батькам щодо створення умов для інформаційної безпеки здобувачів початкової освіти.

**Експериментальна база дослідження.** Дослідницьку роботу було проведено у Гвардійському ліцеї Гвардійської сільської ради Хмельницького району Хмельницької області.

**Апробація результатів дослідження.** Результати дипломної роботи були апробовані на міжвузівської науково-практичної конференції «Патріотичне виховання в освіті та соціальній роботі: уроки минулого та сучасний погляд» (Хмельницький, 2024 р.), VІ міжвузівській науково-практичній конференції «Актуальні проблеми соціальної роботи: виклики сучасності» (Хмельницький, 2024) та висвітлені в 2 публікаціях.

**Структура роботи:** робота складається зі вступу, двох розділів, висновків, списку використаних джерел (68 найменувань), 8 додатків на 14 сторінках. Ілюстративний матеріал подано в 9 таблицях. Основний зміст роботи викладено на 70 сторінках. Загальний зміст роботи становить 94 стор.

**РОЗДІЛ 1**

**ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗДОБУВАЧІВ ПОЧАТКОВОЇ ОСВІТИ**

* 1. **Сутність і зміст поняття «інформаційна безпека»**

Суспільні зміни, які обумовлюють стрімкий розвиток інформаційних технологій, що, в свою чергу, вимагає від системи освіти гнучкості і чутливості до запитів, до підбору форм і методів цифрової освіти. Беззаперечним є той факт, що сьогодні відбувається технологічний бум у всіх сферах, у тому числі, освітній: електронні підручники, навчальні курси, освітні системи, віртуальні освітні сайти, екскурсії та багато іншого. Більше того, значний відсоток інформації, задоволення дитячої допитливості відбувається не лише через комунікацію в колі сім’ї, закладу освіти, а через мережу інтернет, що вимагає підготовки дітей до використання гаджетів, соціальних мереж та інших цифрових досягнень. Окрім усіх можливостей, які ми отримуємо завдяки інтернету, великим недоліком, у даному контексті є: витік особистої інформації, кібербулінг, залежність від інтернету, небажаний або шкідливий контент тощо. З метою протидії усім цим недолікам, необхідним є створення певних умов для створення безпечного інформаційного простору у закладах освіти, починаючи з початкової школи.

Аналіз науково-педагогічної і технічної літератури дозволяє зазначити, що єдиного і конкретного визначення поняття «безпека» немає, що обумовлено багатоаспектністю його використання у різних сферах діяльності.

У тлумачному словнику української мови вказано, що «безпека» – це стан, коли нікому, нічому, ніщо не загрожує [5]. Як стан, життєдіяльності особи в суспільстві, однією із характеристик якої є стійкість до впливу чинників, які впливають на рівень і якість життя, розглядається безпека у соціологічному словнику [53, с.67].

Досить широко використовується термін «комп’ютерна безпека», що визначається як сукупність програмних та організаційних засобів для запобігання шкідливим впливам (кібератаки, віруси тощо). Активно сьогодні поряд з поняттям «комп’ютерна безпека» вживається «медіабезпека» – це такий стан захищеності особи, суспільства, держави від недостовірної і неправдивої інфоомації, яка є шкідливою для фізичного і ментального здоров’я [7]. Тобто, медіа безпека забезпечує супротив небажаному і шкідливому впливу на особистісну і суспільну свідомість людей, на джерела отримання інформації. Досить подібними, синонімічними є терміни інтернет-безпека, інформаційний захист, інформаційна безпека.

Про інформаційну безпеку держави, як одну із її найголовніших функцій, йдеться у Конституції України [24]. У Законі України «Про Концепцію Національної програми інформатизації» вказується на те, що інформаційна безпека убезпечує державу і кожного її громадянина від шкоди, яка може бути нанесена [18].

Розглядаючи зміст поняття «інформаційна безпека» зазначимо, що вона охоплює заходи та стратегії, спрямовані на захист інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення цілісності, модифікації або знищення.

Неможливою сьогодні нам вбачається національна безпека без інформаційної. Більше того, інформаційна безпека є великою і дуже важливим напрямом як національної безпеки, суверенітету, демократичного ладу так і окремих її складових: політичної, економічної, військової, освітньої та ін. [45]. Ефективність інформаційної безпеки характеризується захищеністю баз даних, неможливістю отримання персоналізованої, конфіденційної інформації при мінімальних витратах держави. Такий хід речей дозволяє нам зазначити, що підготовка до життя в середовищі, наповненому безліччю різної інформації, доступом до неї, вимагає сьогодні від закладів загальної середньої освіти підготовки школярів до такого сучасного соціуму і початок цього процесу лягає саме на початкову школу.

Розгляд поняття «інформаційна безпека» вимагає визначення поняття «захист інформації». Так, у Законі України «Про інформацію» зазначено, що захистом інформації вважається певна сукупність заходів: організаційних, правових, адміністративних, технічних, спрямованих на її збереження, збирання, забезпечення цілісності та порядку доступу, поширення, захист і протидію зловживання інформацією [45]. Важливо зазначити, що у Рішенні Ради з Національної безпеки йдеться і про несанкціоноване розповсюдження неправдивої інформації, деструктивної пропаганди, маніпуляції з цілісністю інформації з обмеженим доступом [47].

Так, Г. Нестеренко розглядає поняття інформаційної безпеки на кількох рівнях [40]:

Таблиця 1.1

Рівні інформаційної безпеки (Г.Нестеренко)



Ми розглядаємо інформаційну безпеку саме у початковій школі, у якій закладаються основи відповідального і адекватного ставлення до користування цифровим середовищем.

Дане поняття є досить складним для розуміння, оскільки є досить широким та включає різні аспекти у своїй сутності. Однією із характеристик інформаційної безпеки є конфіденційність та захист, тобто інформація має бути доступною тільки обмеженому колу людей і захищеною від несанкціонованого доступу: дані про учнів і працівників, такі як ім’я, адреса, телефонні номери, академічні записи, медичні дані; оцінки, результати тестів, звіти про поведінку та інші академічні документи мають бути доступні лише уповноваженим особам. Окрім того, заклади освіти мають продумати чіткі правила щодо збору, зберігання, використання та обміну особистою інформацією. З метою забезпечення конфіденційності та захисту інформації від несанкціонованого втручання необхідним є використання паролів та систем аутентифікації для обмеження доступу до інформаційного середовища закладу освіти; налаштування прав доступу до даних на основі ролей для уповноважених осіб; шифрування даних під час їх передачі по мережах та зберігання на пристроях; використання антивірусного програмного забезпечення, брандмауерів для захисту від шкідливого програмного забезпечення та кіберзагроз; регулярне створення резервних копій даних для відновлення в разі втрати або пошкодження; постійний моніторинг інформаційних систем для виявлення підозрілої активності; проведення регулярних аудитів для перевірки відповідності політиці безпеки та виявлення загроз. Однак, важливою є навченість здобувачів освіти і колективу школи безпечному користуванню інтернетом та інформаційними системами. Ефективною формою роботи у закладах загальної середньої освіти є тренінги кібербезпеки та політик конфіденційності. Приклад тренінгу подаємо у додатку А.

Ще однією важливою характеристикою є цілісність інформаційної безпеки у закладі загальної середньої освіти, яка має на меті забезпечити, щоб інформація залишалася точною, повною та не змінювалася несанкціоновано. Цілісність є критично важливою для забезпечення достовірності академічних записів, особистих даних здобувачів освіти, працівників, а також іншої важливої інформації. Основні аспекти забезпечення цілісності інформації включають: використання технологій контролю доступу для обмеження доступу до даних лише авторизованим користувачам; впровадження ролей і прав доступу, що визначають, хто може читати, змінювати або видаляти дані; створення резервних копій даних на регулярній основі для захисту від втрати інформації через збої в системі, кібератаки або інші інциденти; зберігання резервних копій у безпечних місцях, зокрема, на віддалених серверах або в хмарних сховищах; ведення журналів змін, що дозволяє відстежувати, хто, коли і які зміни вносив до даних; впровадження системи контролю версій для документів і даних, щоб мати можливість відновити попередні версії в разі помилкових змін або пошкоджень; використання цифрових підписів для забезпечення автентичності та цілісності документів; використання антивірусного програмного забезпечення та інших засобів захисту для запобігання пошкодженню або зміні даних через шкідливі програми; регулярне оновлення антивірусних баз та систем безпеки. Незаперечним є той факт, що члени колективу як працівників, так і здобувачів освіти мають бути готовими до забезпечення цілісності інформаційної безпеки у ЗЗСО. З метою цього, необхідним є проведення навчань для педагогічних працівників та іншого персоналу закладу освіти щодо важливості цілісності даних та методів її забезпечення.

Ще однією характеристикою інформаційної безпеки є забезпечення доступності інформації та ресурсів, коли вони потрібні; підтвердження особи користувача або системи, що намагається отримати доступ до інформації (паролі, біометричні дані або двофакторна аутентифікація); надання прав доступу користувачам і системам на основі їх ролі або ідентифікації; ведення журналів подій та регулярний перегляд їх для виявлення та реагування на підозрілі дії.

Для адміністративного персоналу і батьків досить важливим є моніторинг і батьківський контроль для керування ризиками, оцінки та їх управління, включаючи виявлення вразливих місць та загроз.

Аналіз науково-педагогічної літератури та власні спостереження дозволяють зазначити, що актуальність нашого дослідження зумовлена рядом причин:

- відсутність цензури в мережі інтернет, що призводить до перенесення в реальне життя здобувачами початкової освіти неетичної, деструктивної, суперечливої та неправдивої інформації;

- незахищеність персональних даних, введених здобувачами освіти під час реєстрації в різних інтернет-сервісах (електронна пошта, соціальні мережі тощо);

- незахищеність облікових записів електронної пошти від інформаційного піратства та спаму, масових електронних листів;

- схильність здобувачів початкової освіти до участі в різних акціях, аукціонах, онлайн іграх, лотереях та опитуваннях, які приваблюють молодших школярів призами, бонусами, спонукаючи до необдуманих дій, розповсюдження як особистої конфіденційної інформації, так і інформації про своє оточення, родину;

- порушення молодшими школярами елементарних правил, встановлених адміністраторами інтернет-сайтів (реєстрація на певних поштових серверах дозволена з певного віку, перегляд певних відеоресурсів і завантаження комп’ютерних ігор вимагає, щоб користувачеві було 18 років, замовлення товарів в онлайн магазинах є можливим з 18 років)

Якщо розглядати початкову ланку освіти, то у даному контексті варто зазначити, що сутність інформаційної безпеки в початковій школі полягає в захисті молодших школярів та їхньої персональної інформації під час користування цифровими технологіями та Інтернетом. Тобто, необхідним є накопичення знань та формування умінь, навичок учнів щодо базових принципів безпеки в Інтернеті, дотримання конфіденційності особистої інформації, уникнення спілкування з незнайомцями та розпізнавання підозрілих веб-сайтів.

У роботі із дітьми молодшого шкільного віку досить цінним є формування навички захисту свого особистого простору, розуміння приватності та безпечне збереження власних даних.

Незаперечним є той факт, що Інтернет, при правильному використанні є потужним стимулятором пізнавального інтересу учнів, однак, необхідним є використання програмного забезпечення для контролю доступу до інтернету та моніторингу активності здобувачів початкової освіти в онлайн-середовищі, щоб захистити їх від потенційних загроз. Сьогодні цифрові продукти нам пропонують фільтри та обмеження на небезпечні веб-сайти, які захищають користувачів молодшого шкільного віку від небажаного контенту.

Створення умов для інформаційної безпеки у початковій школі дозволяє сформувати основи безпечного та відповідального використання інформаційних технологій у майбутньому, адже починаючи із наймолодшого віку, діти стають активними користувачами гаджетів, соціальних мереж та, загалом, Інтернету. Саме здобувачі початкової освіти є найбільш потенційними жертвами цифрового світу, оскільки не усвідомлюють, через відсутність досвіду, небезпеки поширення, витоку особистої інформації в Інтернеті. Важливими для вирішення проблемами у початковій школі сьогодні є захист молодших школярів від небезпечних ситуацій, уникнення кібербулінгу; формування критичного мислення, вміння розпізнавати фейки, шахрайство та небезпечні сайти; підвищення відповідальності за власну онлайн-активність, розуміння наслідків своїх дій в Інтернеті; захищеності дітей від шкідливого, небажаного контенту, вивчення правил безпеки поведінки в інтернеті.

Кожна сучасна початкова школа сьогодні, зважаючи на умови в яких ми проживаємо, впроваджувати системну політику безпечного використання технологій у освітньому процесі через заходи, які допомагають захистити дітей від небезпек в Інтернеті та навчити їх безпечного, відповідального користування цифровими технологіями. Ця політика включає:

* впровадження програм з кібербезпеки та етики у навчальний план, щоб виховати відповідальне та обережне ставлення до цифрових технологій з раннього віку;
* запровадження правил використання інформаційних технологій у початковій школі, включаючи використання паролів, шифрування даних та регулярне оновлення програмного забезпечення;
* використання здобувачами початкової освіти лише дозволених і безпечних пристроїв та програмам;
* налагодження співпраці між початковою школою і родинами для спільного захисту дітей від кіберзагроз, з метою чого проведення спільних навчань щодо проблеми забезпечення інформаційної безпеки та виявлення потенційних загроз в освіті.

На нашу думку, досить цінними, у контексті нашого дослідження, є принципи виховання здобувачів освіти в цифровому просторі, розроблені групою науковців Інституту проблем виховання Академії педагогічних наук України: К. Журбою, Л. Канішевською, Р. Малиношевським, Н. Харченко, С. Федоренко [4, с.7]. Серед цих принципів:

* принцип індивідуалізації, який зумовлює отримання та використання знань, умінь, навичок поведінки в інформаційному просторі; створення власної стратегії освіти, використання, спілкування, репрезентації у цифровому середовищі;
* принцип доступності визначає відкритість цифрового середовища, його постійну оновлюваність і актуальність, легку використовуваність;
* принцип доцільності, що вказує на застосуванні тих цифрових технологій і методик, які найбільш є ефективні для вирішення поставленого завдання;
* принцип розвитку дозволяє сформувати моральні якості, простимулювати самовдосконалення, креативність, мобільність через інформаційні технології;
* принцип гнучкості відображає можливості цифрових технологій щодо використання їх у відповідності до індивідуальних, вікових особливостей, до можливостей, ресурсів кожної особистості;
* принцип інноваційності забезпечує використання інтерактивних, дистанційних форм і методів взаємодії зі здобувачами початкової освіти, можливості інформаційних технологій для соціалізації, розвитку;
* принцип інтегрованості дозволяє освоїти і використовувати явища, процеси з різних галузей і наук у своєму становленні.

На нашу думку, компонентами інформаційної безпеки для здобувачів початкової освіти є:

* освіченість та поінформованість, які задовольняються через навчання дітей щодо розпізнавання потенційно небезпечних ситуацій в інтернеті; нерозголошення персональних даних (імені, адреси, номера телефону тощо) як реальному, так і віртуальному житті;
* батьківський контроль та нагляд через спеціальні програми, додатки для контролю за діяльністю дітей в інтернеті, обмеження доступу до певних сайтів та контенту;
* підготовка молодших школярів до використання паролів, антивірусних програм, безпечного зберігання особистої інформації, оновлення програмного забезпечення на пристроях, які використовуються;
* розширення знань молодших школярів, розуміння основ адекватної поведінки у соціальних мережах, зокрема, поваги до інших в інтернеті; засвоєння способів боротьби з кібербулінгом та кіберхейтингом, наслідками ігнорування правил поведінки в цифровому середовищі;
* засвоєння дітьми алгоритму дій у разі того, якщо стаєш жертвою кібершахраїв, кібербулінгу.
* інформаційна безпека у початковій школі є важливою частиною загальної освіти, оскільки допомагає дітям з раннього віку розвивати навички безпечної поведінки в цифровому світі.

Отже, інформаційна безпека у початковій школі – це сукупність заходів, впровадження педагогічних умов, система роботи, спрямовані на захист дітей молодшого шкільного віку від потенційних загроз у цифровому середовищі, розвиток у здобувачів початкової освіти навичок безпечної поведінки у цифровому середовищі та відповідального користування інформаційними технологіями. Такими навичками, у контексті нашого дослідження, є: як нерозголошення особистої інформації (ім’я, прізвище, адреса, номер телефону, паролі з незнайомцями в Інтернеті та ін.), так і розуміння приватності (обов’язкове використання налаштування конфіденційності в онлайн-платформах); як створення складних паролей (створення складних паролей, що містять комбінації літер, цифр і символів), так і не припустимість використання одного і того ж паролю для різних акаунтів; як розпізнавання небезпечного контенту (ідентифікація шахрайства та спаму), так і вміння адекватно на нього реагувати; етичної поведінки в Інтернет-середовищі; безпеки під час онлайн-ігор і спілкування; управління часом, проведеним в Інтернеті; безпечного і ефективного користування гаджетами і програмами, збалансованого використання технологій і запобігання залежності від Інтернету; аналізу достовірності отриманої інформації; навичок зв’язку і допомоги у разі виникнення проблем/неприємностей; відповідальності за дії і наслідки неправомірної поведінки в цифровому середовищі; налаштування конфіденційності своїх акаунтів. Тобто, досить важливим на сьогодні є розуміння учнями початкової школи сутності інформаційної безпеки, потенційних загроз у мережі Інтернет, їхньої вразливості, вироблення правил поведінки в цифровому середовищі. Формування основ такої поведінки ґрунтується, з одного боку, на формуванні зовнішніх умов безпеки молодшого школяра – створенні безпечного Інтернет середовища, з іншого – внутрішніх умов безпеки – набутті здобувачами початкової освіти знань щодо розпізнавання, попередження, уникнення і подолання загроз в Інтернеті та формування у школярів відповідних умінь і навичок.

* 1. **Психолого-педагогічні особливості молодших школярів як важливий аспект в організації інформаційної безпеки**

Розгляд проблеми організації інформаційної безпеки здобувачів початкової освіти у повній мірі пов’язаний з визначенням ступеня розвитку осіб даного віку, які включають, як індивідуальні, так і вікові особливості, у контексті нашого дослідження, молодших школярів.

Вік дитини від 6 до 10 років відповідно до поширених вікових періодизацій вважається молодшим шкільним віком, який характеризується відносною стабільністю психологічних і фізіологічних процесів розвитку, переходом від дошкільного віку, поєднанням у свідомості, поведінці дуже складних і суперечливих рис дошкільного дитинства і ознак школяра. Саме цей вік є сенситивним для розвитку багатьох психічних якостей за умови їх своєчасного ініціювання та підтримки. Тому так важливо виявити резерви, задіяти всі можливі ресурси дітей молодшого шкільного віку для подальшої навчальної і трудової діяльності, у контексті нашого дослідження, формування навичок використання інформаційних технологій, адекватної поведінки у цифровому середовищі, уникнення загроз і проблем.

Сьогодні вражає кількість учнів початкової школи, які є самостійними користувачами, мають власні акаунти у різних соціальних мережах, що порушує правила цих мереж, відповідно яких до 13 років дитина не може мати власної сторінки. Статистика свідчить, що віком до 13 років до 20 млн. учнів мають власні сторінки у Facebook, 40% користувачів Tik Tok – це школярі [27]. Тобто, діти мають вільний доступ до різного виду неконтрольованої за змістом інформації, що зумовлює певні виклики і ризики.

Так, різним аспектам вікових особливостей розвитку дитини присвятили свої дослідження І.Бех, О.Запорожець, О.Кононко, О.Коханова, О.Пасєка, О.Сергєєнкова, О.Столярчук, С. Холл [2; 19; 23; 51] та інші. Думки науковців схилялися до того, що окрім закономірних етапів розвитку на дитину впливають спадковість і навколишнє середовище, у якому дитина зростає. Сьогодні цифрове середовище є вагомим компонентом середовища розвитку дитини. Більше того, доступ до інформації сучасним молодшим школярем має значний вплив на формування цінностей, світосприйняття, на погляди, переконання, життєві принципи та, зрештою, поведінку і дії. Звідси і випливає необхідність врахування вікових та індивідуальних особливостей здобувачів початкової освіти у процесі наповнення соціального середовища необхідною інформацією, яка є визначальною у процесах розвитку і соціалізації кожної особистості.

Серед основних психологічних особливостей молодших школярів варто відмітити смислову пам’ять, словесно-логічне та вербально-дискурсивне мислення, довільну і короткотривалу увагу, ігрову діяльність, яка переходить у навчальну, потребу в руховій активності та отриманні вражень, емоційне сприйняття світу, недостатній моральний досвід. Саме, з метою вивчення навколишнього світу, задоволення пізнавального інтересу з’являється досить значна потреба в отриманні нових знань, умінь і навичок, яку у сучасному світі задовольняє інформація з Інтернету.

Характерною особливістю сучасного покоління дітей є кліпове мислення (від англ. clip – «вирізка (з газети), уривок (фільму)») – це феномен, пов’язаний із сприйняттям інформації у вигляді коротких, незв’язаних фрагментів, подібних до кліпів; сприйняття інформації короткими яскравими кадрами, без встановлення логічних зв’язків. Цей термін описує стиль мислення, що формується під впливом сучасних медіа та інформаційних технологій, таких як соціальні мережі, відео на YouTube, короткі статті, повідомлення у месенджерах тощо. Кліпове мислення, на його основі світогляд, формуються за аналогією: через сприйняття світу як певну послідовність, частини у якої практично не пов’язані між собою. Через кліпове мислення образи не залишаються надовго у свідомості, вони швидко зникають, а на їхньому місці з’являються нові, що стає причиною нездатності виконувати аналітичну функцію.

Окрім того, зазначимо про дуже швидке сприймання картин і образів, підвищену емоційність, асоціативність і візуальність у діяльності молодшого школяра. Такі особливості психічної діяльності призводять до поверхневого та спрощеного накопичення знань, що зумовлює відсутність вміння аналізувати слова, процеси, дії і вчинки [44, с.145].

Аналіз науково-педагогічної літератури дозволив виокремити компоненти діяльності учнів початкової школи в інформаційному середовищі (Таблиця 1.2.) [4, с.4-5; 63].

Виокремлені компоненти діяльності молодших школярів у інформаційному середовищі мають позитивні і негативні моменти. Так, незаперечним є те, що соціальні мережі є досить швидким і зручним середовищем для комунікації; мають значний потенціал для мотивації, стимулювання пізнавального інтересу, розвитку та соціалізації через інформаційні ресурси: онлайн-бібліотеки, онлайн-музеї, навчальні платформи, вебінари тощо; користування цифровим середовищем сприяє розвитку дрібної моторики, виробленню швидкої реакції, розвитку пам’яті, логічного мислення, вміння прогнозувати; сприяє формуванню життєвої позиції, творчості.

Таблиця 1.2

Компоненти діяльності здобувачів початкової освіти в інформаційному просторі [33]



Поряд із названими нами позитивними аспектами використання учнями початкової школи цифрових технологій, назвемо і деякі недоліки: проблеми зі здоров’ям; зосередженість на образі в Інтернеті (аватарі); зниження соціальних навичок (комунікації, емпатії); вплив на чистоту мови, вміння висловлювати власну думку; втягування у віртуальні інтимні стосунки; несформованість ціннісних орієнтирів; невміння відрізнити віртуальну реальність від реальної дійсності; втрата інтересу до отримання знань, ручної роботи, читання тощо.

Сформованість вміння аналізувати події, явища процеси, пропозиції є основою для інформаційної безпеки особи. Тому під час організації роботи з проблеми нашого дослідження педагогу, батькам необхідно є врахувати ці важливі моменти, щоб підібрати ефективні методи, форми роботи з молодшими школярами.

Варто зазначити, що у молодшому шкільному віці вагому роль для здобувачів освіти відіграє значимий дорослий, яким, у першу чергу, є педагог, учитель. На відміну від дошкільного віку, коли система відносин дитини з навколишньою дійсністю вибудовується у двох сферах соціальних відносин: «дитина-дорослий» і «дитина-дитина», у початковій школі починає формуватися абсолютно інша система «дитина-дорослий», яка розгалужується на «дитина -вчитель», «дитина-батьки», «дитина-діти», де визначальною є, безперечно, «дитина-вчитель» [61]. За умови тісного, довірливого зв’язку між вчителем і молодшим школярем налагоджується адекватна система взаємовідносин між учнями в класі, яка стає основою стосунків з дорослими, із суспільством загалом. Незаперечним є той факт, що к у початковій школі, так і суспільстві, така система може бути вибудована на основі певних правил, яких має дотримуватися кожен член колективу класу, закладу освіти. Тобто, тільки той вчитель, якому не властиве упереджене ставлення до учнів, який сам дотримується чітко кожного правила, зможе досягнути розуміння дітьми тих основ і постулатів, які є необхідними для збереження їхнього ментального і фізичного здоров’я.

Беручи до уваги схильність учнів початкових класів до наслідування значимих дорослих, а це, як ми зазначали, педагоги і батьки, вирішення проблеми інформаційної безпеки ми вбачаємо у підготовці вчителів і членів сімей до адекватного використання цифрового середовища.

З метою просвітницької роботи вчителів і батьків щодо підготовки дітей до безпечного та відповідального користування цифровими технологіями, досить ефективними є: Digital Citizenship Curriculum від Common Sense Media – набір уроків, відео та різних видів діяльності для вчителів і батьків; NetSmartz Workshop – інтерактивні уроки та відео з навчальними матеріалами для вчителів та батьків з основ безпеки в Інтернеті. Використання цих програм, інтернет-ресурсів батьками і вчителями дозволить створити цілісну систему розвитку інформаційної безпеки в початковій школі, допоможе дітям краще зрозуміти важливість безпеки в Інтернеті та навчитися дотримуватися основних правил.

Як зазначав Ж.Піаже досить важливим для дітей молодшого шкільного віку усвідомлюваність ними понять і підсвідома інтуітивність [56], тобто розуміння і усвідомлення того, що пропонується до вивчення і виконання, прийняття інформації учнем, що є усвідомленим, а що ще ні, над чим потрібно працювати.

Із початком шкільного життя у здобувачів початкової освіти з’являється внутрішня позиція, як наступний рівень самосвідомості, який свідчить про усвідомлення себе серед інших людей, явищ, ситуацій, подій. Це усвідомлення, яке проявляється у висловлюваннях, вчинках і діях, є початком самостійного особистісного розвитку молодшого школяра. Поява внутрішньої позиції зумовлюється моральними цінностями і нормами, які починає усвідомлювати дитина молодшого шкільного віку, слідувати їм [56]. Головним завдання початкової школи є формування вміння у школярів свідомого, самостійного виявлення, уникнення, захисту себе від інформаційних загроз і небезпек. Тобто, як зазначає К. Шишкіна, у роботі зі здобувачами початкової освіти під час формування навичок інформаційної безпеки ефективними є використання проблемних ситуацій, для вирішення яких необхідним є моральний вибір.

Так, під час організації інформаційної безпеки учнів початкових класів важливо враховувати особливості їхнього когнітивного розвитку, оскільки дітям даного віку властиве обмежене розуміння абстрактних концепцій, таких як складні терміни безпеки або поняття кіберзлочинності. Роз’яснення сутності і змісту понять мають бути конкретними, розкриватися через прості, зрозумілі приклади, різні види унаочнення, вузуалізації конкретних матеріалів. Досить ефективними, у контексті зазначеного, є малюнки, комікси та відео, які демонструють основи безпеки у формі, зрозумілій для дітей.

Не можна оминути увагою і соціально-емоційний розвиток молодших школярів, які є дуже емоційними і чутливими до сприйняття негативних ситуацій або новин. Пояснення можливих загроз мають роз’яснюватися без страху, паніки, залякування, з акцентом на позитивні практичні рішення і конкретні дії, алгоритми вирішення проблеми. Дієвим методом, у контексті розвитку інформаційної безпеки, є заохочення, мотивація до адекватної поведінки у цифровому середовищі, використання системи нагород і похвали.

Зважаючи на те, що у 1 і 2 класах початкової школи переважаючим видом діяльності залишається ігрова, яка поступово замінюється навчальною, необхідним є використання різних видів ігор: дидактичних, сюжетно-рольових та інших. Так, сюжетно-рольові ігри допоможуть дітям вчитися реагувати на можливі небезпеки без спокійно, виважено, знаючи до кого звернутися про допомогу у разі виникнення проблеми, як убезпечити себе від шахрайства, кібербулінгу, хейту тощо.

Варто зазначити, що відповідно вікових особливостей дітей молодшого шкільного віку, структурування дій, ознайомлення і засвоєння чітких і простих правил, є досить важливим у вирішенні проблеми інформаційної безпеки. Більше того, для детального запам’ятовування необхідного матеріалу важливо дотримуватися регулярності у проведені тематичних занять, повторення, закріплення знань і навичок безпеки.

Розглядаючи молодший шкільний вік, варто не оминути той момент, що здобувачі початкової освіти мають короткотривалу увагу, що вимагає поділу інформації невеликі, легко засвоювані частини, для утримування якої необхідним є використання інтерактивних методів навчання для утримування їх уваги. Окрім короткотривалої уваги, для активної розумової діяльності, засвоєння знань від молодших школярів вимагається ще й прояв сили волі, наполегливості, посидючості, керування емоціями та руховою активністю, управління власними бажаннями протягом тривалого часу, що в початковій школі стає викликом і проблемою для суб’єктів освітнього процесу. У свою чергу, гаджети, Інтернет, соціальні мережі стають своєрідним джерелом розвантаження і зацікавленості, що зумовлює попит і, досить часто, залежність не тільки у дітей молодшого шкільного віку. Вирішення цієї проблеми лежить у формуванні культури використання цифрових технологій, розвитку інформаційної безпеки у початковій школі.

Ще однією характерною особливістю здобувачів початкової освіти, яку необхідно врахувати під час вирішення проблеми дослідження, є несформована здатність до самообмеження, контролю за часом проведеного в Інтернеті, що зумовлює використання вчителями, батьками інструментів для обмеження доступу до небажаного контенту, інформації та контролю часу.

Для дітей молодшого шкільного віку, які оперують конкретними категоріями, у яких досить слабко розвинуте абстрактне, і переважає конкретне мислення, досить ефективними є розміщування у соціальному середовищі нагадувань про правила безпеки і підказки, у вигляді закликів до дії, які допомагають дітям дотримуватися їх. При чому, ці нагадування і підказки мають бути простими, чіткими і повторюваними, варто задіювати максимально можливі сенсорні системи: зорову, слухову. Прикладом можуть бути плакати, стікери з правилами, написаними як пам’ятка в класі. Перед використанням гаджетів, Інтернету ефективними будуть прослуховування аудіо-правил чи читання вчителем/кимось із дітей/ відомою особистістю в колі дітей (відомими місцевим блогером). Наприклад:

1. Не розголошуй особисту інформацію (своє ім’я, адресу, номер телефону або іншу особисту інформацію в Інтернеті.
2. Тримай паролі у секреті, навіть від друзів.
3. Обмірковуй перед тим, які публікувати фото чи відео.
4. Не розмовляй з незнайомцями в Інтернеті, як і в реальному житті.
5. Повідомляй батькам або вчителям про дивну поведінку, незручні питання чи коментарі в Інтернеті.
6. Використовуй безпечні дитячі сайти та програми (Duolingo ABC, ABCmouse.com, Toca Boca, YouTube Kids, Netflix Kids, Scratch, LEGO Life).

Досить ефективним для розвитку інформаційної безпеки у початковій школі є постійне нагадування і залучення дітей до активного складання, обговорення пам’яток, правил, що допоможе їм краще зрозуміти, усвідомити і, відповідно, дотримуватися безпечної поведінки в Інтернеті.

На перервах, під час групи продовженого дня варто організовувати інформаційні хвилини, які пояснюють правила безпеки в інтернеті, з використанням навчальних програм та відео: Google's Be Internet Awesome, NetSmartz Kids, Kiddle, Покемон і правила безпеки в інтернеті, Safer Internet Day TV, Common Sense Education, Cyberwise, Childnet, BrainPOP та ін.

Отже, визначені нами вікові особливості молодших школярів є визначальними в організації інформаційної безпеки, адже підбір методів, форм роботи в повній мірі залежить від комплексу знань, умінь і навичок, розуміння небезпек, які зустрічаються у цифровому просторі. Незаперечним є той факт, що організація інформаційної безпеки в початковій школі залежить від педагога, союзниками у якого мають бути усі учасники освітнього процесу, тому важливе значення, у контексті нашого дослідження, належить педагогічній просвіті вчителів і батьків, мотивації дітей, розуміння ними дотримання правил користування цифровими технологіями.

* 1. **Зарубіжний досвід із організації інформаційної безпеки дітей**

Аналіз науково-педагогічної літератури дозволяє зазначити, що більшість розвинутих країн у світі ведуть чітку державну політику щодо дотримання інформаційної безпеки, формування навичок якої є одним із пріоритетних завдань закладів освіти, зокрема, початкової школи.

Досить детально проблему інформатизації суспільства за кордоном описано у монографії В. Ліпкан, І. Сопілко, В. Кір’ян [34], які проаналізували державну політику з інформатизації у 20 країнах світу. Зарубіжний досвід правового захисту дітей в цифровому середовищі розкрито у дослідженнях В. Куницького [30], О. Лисенко [35, с.26] та інших. Дослідники проблеми інформаційної безпеки засвідчують про об’єднання країн світу для розробки, впровадження, пошуку новітніх підходів, які нам необхідно вивчати і використовувати найкращі практики в Україні. З іншої сторони, нам потрібно досліджувати і винаходити свої підходи, які будуть задовольняти потреби і реагувати на виклики нашої країни, зумовлені війною, постійними кібератаками з боку ворожої країни; шаленим розвитком інформаційних технологій, які заповнюють усі сфери життя сучасної людини.

Дослідження діяльності країн зарубіжжя щодо кроків з розвитку інформаційної безпеки дозволяють зазначити, що відслідковується тенденція до атрибуції текстів, що дозволить у подальшому встановлювати різні ознаки правопорушників з девіаціями, метою яких є розбещення дітей молодшого шкільного віку через фальсифікацію персональних даних дітей у соціальних мережах, гаджетах, месенджерах [66]. Така діяльність є важливою для попередження торгівлі людьми, розповсюдження дитячої порнографії, розшуку зниклих дітей.

На сьогодні, у країнах зарубіжжя серйозна увага приділяється дитячим агресивним висловлюванням, у змісті яких приниження за ознаками віку, національності, статі тощо. Більше того, такі висловлювання можуть бути підставою для притягнення до відповідальності судовими органами. Варто вказати на порушення питання щодо підготовки методів і методик для вивчення комунікативної поведінки дітей [65]. На жаль, в Україні питання комунікації дітей молодшого шкільного віку не є предметом досліджень науковців, як і не розглядається на рівні державних організацій і установ.

Важливим аспектом в організації інформаційної безпеки у зарубіжних країнах виступає батьківський контроль, адміністративна відповідальність батьків за забезпечення правомірної поведінки, недопущення ризиків, захист в цифровому середовищі дітей молодшого шкільного віку. Маємо на увазі не лише встановлення на гаджетах програм батьківського контролю, а відповідальність батьків за належну підтримку дитини, її розвиток і соціалізацію, з недопущенням впливу загрозливого контенту. Варто констатувати той факт, що в нашій країні дане питання знаходиться не в першій десятці нагальних до вирішення проблем, що ускладнює мінімалізацію впливу соціальних мереж, месенджерів на поведінку і дії дітей і молоді [57].

З точки зору державної політики, підтримки ініціатив громадськості, діяльності приватних відомств, то варто зазначити, що Велика Британія є найбезпечнішою країною світу з розвитку інформаційної безпеки дітей і молоді. Згідно прийнятого акту Online Safety Act з метою захисту як дітей, так і дорослих від небезпечного контенту в мережі Інтернет вводяться безпрецедентні обмеження і відповідальність для власників інформаційних месенджерів, платформ, соціальних мереж, пошукових систем щодо публікації нелегального, небезпечного, шкідливого контенту, особливо, для дітей. Більше того, необхідним є забезпечення ефективних механізмів, аудиту щодо встановлення, виявлення, видалення такого контенту, розповсюдження відомостей про результати перевірки своїх ресурсів щодо безпеки інформації, яка ними публікується [13]. Законом передбачено створення процедур для запобігання поширення небезпечного і шкідливого для дітей контенту. Важливо зазначити, що даний документ має на увазі саме захист ментального здоров’я, життя користувачів, захист персональної інформації репутації особи.

Серйозність державної політики Великобританії щодо організації інформаційної безпеки дітей підтверджується ще й створенням державного органу Ofcom – це агентство з регулювання і перевірки приватних теле- і радіокомпаній на дотримання закону про контент, який розповсюджується. Ті ж самі компанії при створенні певного продукту, мають дотримуватися цінностей Safety by Design, відповідно якого необхідно вважати на шкоду, яку він може завдати користувачам, надати дітям і батькам зрозумілі інструменти для виявлення ризикованого контенту, посилення обмежень доступу дітей, віком до 13 років, до створення власних акаунтів у соціальних мережах, серйозні перевірки віку. Чітко є перерахованими порушення, за які несеться кримінальна відповідальність як окремо взятої особи, так і організації [58].

Основоположним документом з інформаційної безпеки у закладах освіти Великобританії є «Keeping Children Safe in Education» (KCSIE) від Департаменту освіти, який визначає обов’язки шкіл щодо захисту дітей від онлайн-загроз [43]. (Додаток Б)

Обов’язковим для кожного закладу освіти у Великобританії є створення системи фільтрації та моніторингу доступу до Інтернету, а також регулярне навчати персоналу з питань кібербезпеки​ (GOV.UK)​​ (NSPCC Learning)​.

Окрім того, значна кількість організацій і установ працюють над вирішенням проблеми інформаційної безпеки у початковій школі. Так, Національний центр кібербезпеки (NCSC) надає рекомендації для шкіл, включаючи розробку інструкцій та протоколів реагування на кіберінциденти, регулярне навчання персоналу і резервне копіювання даних​ (National Cyber Security Centre)​. Організація SWGfL пропонує контрольний список з кібербезпеки, який містить рекомендації щодо навчання персоналу, підготовки до кібератак та резервного копіювання даних​ (SWGfL) [20]​.

Аналіз науково-педагогічної літератури, державної політики Іспанії дозволяють зазначити, що проблема інформаційної безпеки молодших школярів стає все більш актуальною у цій країні. Більше того, цей рік став особливо визначальним у контексті нашого дослідження для Іспанії. Адже на найвищому державницькому рівні, починаючи від Прем’єр-міністра, в Уряді активною стала компанія щодо посилених дій та заходів із недопущення доступу дітей до небезпечного контенту в Інтернеті, обмеження доступу до сумнівних сайтів, до порнографічної продукції та інших небезпек цифрового середовища [32].

Основою інформаційної безпеки дітей в Іспанії є Закон про захист персональних даних (Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales - LOPDGDD), який регулює збір, обробку та зберігання персональних даних, включаючи дані дітей; Загальний регламент про захист даних (General Data Protection Regulation – GDPR), який застосовується в усіх країнах ЄС, включаючи Іспанію, згідно якого встановлюються строгі правила щодо захисту персональних даних, зокрема даних дітей, і вимагається отримання чіткої згоди від батьків або опікунів для обробки даних дітей до 16 років; Королівський декрет 3/2018 (Real Decreto-ley 3/2018), який адаптовує національне законодавство до вимог GDPR, включаючи заходи щодо захисту даних дітей в Інтернеті; Національний план з кібербезпеки (Estrategia Nacional de Ciberseguridad) – стратегічний документ, який визначає основні напрями державної політики в галузі кібербезпеки, включаючи захист дітей в Інтернеті; Internet Segura for Kids (IS4K) – це ініціатива, яка віграє важливу роль у забезпеченні безпеки дітей в інтернеті, надаючи ресурси, навчальні матеріали та консультаційну підтримку для дітей, батьків і вчителів; Закон про телекомунікації (Ley General de Telecomunicaciones), який регулює діяльність телекомунікаційних компаній і включає положення щодо захисту дітей від небажаного контенту та кібербулінгу; Національний план проти кібербулінгу (Plan Nacional contra el Ciberacoso), який включає освітні програми, кампанії з підвищення обізнаності та заходи з підтримки жертв кібербулінгу серед дітей та молоді.

У багатьох школах Іспанії, як і в інших країнах Європи активно впроваджують програми цифрової грамотності та інформаційної безпеки. Для дітей пропонуються предмети, де діти навчаються основам безпечного користування Інтернетом, створення надійних паролів та захисту особистих даних. Школи, шкільні бібліотеки та комп’ютерні класи обладнуються програмним забезпеченням для фільтрації контенту та захисту від небажаних онлайн-загроз. У закладах освіти організовують семінари та тренінги для батьків, з метою навчання батьків ефективним методам захисту дітей в Інтернеті, контролю та обмеження доступу дітей до небажаних сайтів.

Варто зазначити, що практика чіткої державної політики, стратегій діяльності закладів освіти проти кібербулінгу відслідковується, окрім названих нами країн, у Португалії, Швеції, Ірландії, Франції, Німеччині, Румунії, Словаччині, Польщі. Відповідальність за кібербулінг внесено у Кримінальні і Цивільні кодекси, антидискримінаційне законодавство (якщо відбувається дискримінація через національність, стать, колір шкіри, расу, релігію, інвалідність) багатьох країн.

Особлива відповідальність на постачальників інтернет-послуг покладається в Італії та Нідерландах. У Нідерландах є обов’язковим значок від провайдерів про контент, який містить шкідливий контент. У Італії розроблено Кодекс поведінки проти кібербулінгу, відповідно якого постачальники послуг доступу до мережі Інтернет зобов’язані розробити механізми інформування про шкідливий і небезпечний контент [59].

Особливо активно ведеться політика із організації інформаційної безпеки у роботі із дітьми у закладах освіти Сполучених Штатів Америки. Не зважаючи на певну автономність у закладах освіти США, одними із основоположних законів якими послуговуються усі заклади освіти, у контексті нашого дослідження, є: Закон «Про захист конфіденційності дітей в Інтернеті» COPPA (Children’s Online Privacy Protection Act), який регулює збір особистих даних дітей віком до 13 років компаніями, зобов’язуючи веб-сайти та онлайн-сервіси отримувати згоду від батьків перед збиранням особистої інформації дітей; Закон «Про інтернет-захист» (Children’s Internet Protection Act (CIPA) [67], у якому йдеться про обов’язкове застосування спеціалізованих програм, засобів для блокування доступу до небезпечного контенту в організаціях таких як заклади освіти, бібліотеки.

Названі функції у закладах освіти, бібліотеках виконує системний адміністратор, який контролює сайти і сторінки, які відвідують здобувачі освіти даного закладу. Більше того, на тлі демократичності США відбувається дуже жорсткий контроль за дотриманням правил, притягненням до відповідальності за їх порушення. Так, на початку року кожен учень підписує своєрідну розписку про те, що знайомий/знайома із правилами закладу освіти, про усвідомлення змісту інформаційних правопорушень, про розуміння відповідальності і покарання за інформаційні правопорушення, до речі, серед цих правил у більшості інституцій є заборона щодо використання власних гаджетів під час навчання. Такі самі розписки підписують як батьки дітей, так і представники адміністрації закладу освіти. Тобто, до створення безпечного інформаційного середовища залучаються також і батьки, всі учасники освітнього процесу.

Досить поширеними у США є навчальні програми з кібербезпеки, які навчають дітей основам безпечного використання Інтернету, включаючи навчальні матеріали про створення надійних паролів, розпізнавання фішингових атак та захист особистих даних. Пропонуємо перелік можливих онлайн-ресурсів для підготовки дітей, учителів і батьків основним аспектам інформаційної безпеки [14]:

* Common Sense Education – це інформаційний освітній продукт, який пропонує різноманітні навчальні матеріали та ресурси для вчителів і батьків, охоплюючи теми цифрової грамотності, етичного використання технологій та безпеки в Інтернеті;
* NetSmartz – це програма Національного центру зниклих та експлуатованих дітей, яка надає інтерактивні уроки та ресурси для дітей, батьків і вчителів, включаючи відео, ігри та практичні поради щодо безпечного користування Інтернетом;
* CyberSmart! Curriculum – це навчальна платформа з уроками для учнів різного віку та ресурсами для вчителів, яка охоплює основні аспекти інформаційної безпеки та цифрової грамотності;
* Be Internet Awesome (Google) – це програма від Google, яка включає навчальні матеріали та інтерактивну гру Interland, спрямовану на навчання дітей правилам безпечного користування Інтернетом, захисту особистих даних та розпізнаванню онлайн-загроз;
* Digital Citizenship (ISTE) – це Міжнародне товариство з технологій в освіті, яке пропонує програми та ресурси, що охоплюють цифрову грамотність та інформаційну безпеку, спрямовані на розвиток навичок відповідального та етичного користування інформаційними технологіями;
* SafeKids.com and SafeTeens.com – це веб-сайти, які пропонують різноманітні ресурси та поради для дітей, підлітків і батьків щодо безпечного користування Інтернетом, соціальними мережами, месенджерами та іншими онлайн-сервісами;
* ІKeepSafe (Internet Keep Safe Coalition) – це некомерційна організація, яка займається питаннями безпеки дітей в Інтернеті, наданні освітніх ресурсів та інструментів безпечного використання інформаційних технологій, а також захистом конфіденційності та безпеки в цифровому середовищі.

Це далеко неповний перелік ресурсів у США для отримання знань щодо безпечного використання цифрових технологій, інформаційного контенту. Адже багато шкіл проводять семінари та тренінги для батьків, щоб надати важливу інформацію, забезпечити основам цифрової грамотності та методам захисту дітей в Інтернеті, заохочуючи до обговорень з дітьми правил безпечного користування інтернетом і встановлення сімейних правил щодо часу, проведеного в мережі. Абсолютний контроль за дотриманням правил користування Інтернетом відбувається з боку вчителів та інших членів колективу школи [13].

Отже, проведене дослідження з вивчення зарубіжного досвіду країн з інформаційної безпеки дітей дозволяє зробити висновок про те, що більшість країн розуміють небезпеку неконтрольованого використання молодшими школярами цифрового контенту. З метою недопущення доступу дітей до небезпечної інформації, небажаних сайтів, захисту ментального і фізичного здоров’я дітей проводиться активна державна політика щодо вирішення проблеми інформаційної безпеки дітей, залучення до цього процесу батьків та педагогів. Так, більшість країн світу ратифікують і послуговуються рядом документів для захисту дітей у цифровому середовищі, які подано у таблиці 1.3 (Додаток В).

Окрім того, країни ЄС часто розробляють національні стратегії та плани дій для забезпечення безпеки дітей в Інтернеті. Наприклад, у Великій Британії діє «UK Safer Internet Centre», а в Іспанії – «Internet Segura for Kids (IS4K)», Франція має закон «Loi sur la protection des mineurs sur Internet». Як ми зазначали вище, ці документи включають національні ініціативи, освітні програми та консультаційні послуги для організації безпеки дітей в цифровому середовищі. Також компанії та організації приймають добровільні кодекси поведінки для організації безпеки дітей в Інтернеті, убезпечуючи їх від онлайн-загроз, шкідливого контенту та зловживань.

Необхідним для Україні є використання досвіду і практик провідних країн світу щодо ІБ дітей. Ми звертали увагу на міжнародні нормативні документи, які ратифіковані в Україні, на прийняті закони та підзаконні акти, законодавчі ініціативи в нашій країні щодо проблеми нашого дослідження, однак необхідним є втілення усіх норм законів у практику, у життя кожного громадянина України.

**РОЗДІЛ 2**

**ДОСЛІДЖЕННЯ УМОВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УЧНІВ ПОЧАТКОВОЇ ШКОЛИ**

**2.1. Аналіз стану проблеми дослідження**

Аналіз стану інформаційної безпеки в початковій школі є важливим аспектом у контексті нашого дослідження, оскільки, на сьогодні цифрові технології стали невід’ємною частиною як нашого життя, так і освітнього процесу школи. Даний аналіз дозволить враховувати ризики, пов’язані з використанням інформаційних систем у діяльності з молодшими школярами, відповідно, продумати ефективну систему захисту ментального і фізичного здоров’я дітей, персональних даних суб’єктів процесу навчання, убезпечити їх від небажаного шкідливого контенту, сформувати навички аналізу отримуваної інформації з різних джерел. В умовах швидкого розвитку технологій та зростання кіберзагроз необхідним є впровадження систем, які дозволяють вчасно виявляти та реагувати на ризики. Тобто, заклади загальної середньої освіти мають бути готовими до реагування на такі загрози, підготовку дітей, починаючи з початкової школи, до безпечної поведінки, у сповненому викликів і загроз середовищі.

Політика інформаційної безпеки в початкових школах України значною мірою формується на основі державних нормативно-правових актів, які регулюють захист інформації та персональних даних. Як зазначалося у попередніх підрозділах нашого дослідження, Міністерство освіти і науки України розробляє законодавство, рекомендації та інструкції щодо забезпечення кібербезпеки в школах. Проте, рівень впровадження цих політик може варіюватися в залежності від конкретного закладу освіти, його фінансових можливостей та обізнаності керівництва.

Стан технічної інфраструктури є одним із ключових факторів інформаційної безпеки. Аналіз науково-педагогічної літератури, власні спостереження дозволяють зазначити, що багато шкіл забезпечені базовими технічними засобами, такими як комп’ютери, планшети та доступ до Інтернету. Проте, наявність сучасних захисних технологій, таких як антивірусні програми, брандмауери та системи фільтрації контенту, може бути недостатньою через обмежене фінансування. Важливою складовою є регулярне оновлення програмного забезпечення та навчання персоналу основам технічного захисту.

Важливим етапом у вирішенні проблеми створення безпечного цифрового середовища у закладах загальної середньої освіти, починаючи з 2012 року, у навчальні плани початкової освіти було введено предмет «Сходинки до інформатики». Даний курс було спрямований на досягнення мети і вирішення завдань освітньої галузі «Технології», передбаченої у Державному стандарті початкової загальної освіти [8], у якому було враховано рекомендації Концепції Нової української школи [25] та постанову ЮНЕСКО про запровадження курсу «Інформатика в початковій школі» [37].

Предмет «Сходинки до інформатики» - це підготовчий курс до вивчення інформатики у старших класах загальноосвітньої середньої школи, він носить ознайомчий характер із основами інформатики. Незаперечним є той факт, що системне вивчення молодшими школярами інформаційних технологій забезпечує формування інформаційно-комунікативної компетентності учнів, сприяє мобільності та розвитку комунікативних навичок учнів початкової школи засобами цифрового середовища. Разом з тим, виникає потреба у формуванні навичок у користувачів мереж безпечного користування різним контентом.

Окрім того, заклади загальної середньої освіти, які розуміють свою роль у підготовці молодших школярів до безпечного використання цифрового середовища, вводять навчальні програми для початкової школи, які включають елементи інформаційної безпеки, проте їх зміст та глибина можуть відрізнятися. Деякі школи активно проводять уроки, присвячені кібербезпеці, на яких учнів знайомлять з основними правилами безпечного користування Інтернетом, захисту персональних даних та розпізнавання кіберзагроз. Тренінги для вчителів з питань кібербезпеки також є важливим аспектом, оскільки вони повинні бути готові до швидкого реагування на інциденти та надання допомоги учням.

Рівень обізнаності вчителів і батьків про інформаційну безпеку є критично важливим. Учителі повинні бути добре обізнані з актуальними загрозами та методами захисту, щоб ефективно передавати ці знання учням. Батьки також відіграють значну роль, оскільки вони контролюють використання дітьми цифрових пристроїв вдома. Підвищення обізнаності батьків через семінари, тренінги та інформаційні матеріали є необхідним кроком для створення безпечного цифрового середовища для дітей.

Попри зусилля, спрямовані на забезпечення інформаційної безпеки, існує низка проблем та викликів. Однією з головних проблем є недостатнє фінансування, що обмежує можливості шкіл у придбанні сучасного захисного обладнання та програмного забезпечення. Крім того, варіативність у впровадженні політик кібербезпеки та нерівномірний рівень підготовки педагогічних працівників можуть призводити до різниці в рівні захисту між закладами освіти.

Громадські організації активно залучаються до процесу підвищення інформаційної безпеки в школах. Вони проводять освітні кампанії, тренінги та семінари для учнів, вчителів та батьків. Наприклад, організації з кібербезпеки часто пропонують безкоштовні ресурси, які можуть використовувати школи для підвищення рівня обізнаності про кіберзагрози та методи захисту.

Державні ініціативи та програми співпраці з міжнародними організаціями відіграють значну роль у розвитку інформаційної безпеки в школах. Співпраця з міжнародними партнерами допомагає впроваджувати передові практики та стандарти, адаптовані до місцевих умов. Проєкти, спрямовані на розвиток цифрової грамотності та кібербезпеки, отримують підтримку від міжнародних донорів та урядових програм.

Інформаційна безпека також включає психологічну підготовку учнів до взаємодії в цифровому середовищі. Важливо створити умови, за яких діти можуть безпечно обговорювати свої проблеми, пов’язані з Інтернетом, отримувати підтримку від дорослих та не боятися звертатися за допомогою. Шкільні психологи, соціальні педагоги повинні бути залучені до процесу забезпечення інформаційної безпеки, оскільки кібербулінг та інші форми онлайн-насильства можуть мати серйозні наслідки для психічного здоров’я дітей.

З метою аналізу стану інформаційної безпеки у початковій школі нами було проведено дослідження у Гвардійському ліцеї Гвардійської сільської ради Хмельницького району Хмельницької області, у якому взяло участь 94 дитини, 14 педагогічних працівників, серед яких: 7 вчителів, 2 асистента вчителя, директор, 2 заступників директора з навчально-виховної роботи, заступник директора з виховної роботи, психолог/соціальний педагог.

Першим етапом нашої дослідницької роботи було проведення опитування членів педагогічного колективу щодо стану інформаційної безпеки в початковій школі, з’ясування нагальних проблем та визначення можливих шляхів ефективного формування інформативно-комунікативної компетентності здобувачів початкової освіти (Додаток Д).

На перше питання «Як ви оцінюєте свою обізнаність про інформаційну безпеку» 12 членів педагогічного колективу визначили середній рівень обізнаності (86%), 2 – «добре обізнаний» (14%), що, у контексті нашого дослідження, свідчить про необхідність проведення навчань із педагогічними працівниками саме за темою інформаційної безпеки у початковій школі.

На питання «Чи проходили ви навчання або курси з дотримання інформаційної безпеки у початковій школі?» 11 опитаних дали схвальну відповідь (79%), хоча назви курсів не зазначили і 3 опитаних (21%) зазначили, що є потреба у навчанні членів педагогічного колективу щодо забезпечення інформаційної безпеки у початковій школі.

Відповіді на питання «Які технології ви використовуєте у навчальному процесі?» розподілилися таким чином: 14 (100%) опитаних членів колективу відповіли, що у своїй роботі вони постійно використовують стаціонарні комп’ютери, ноутбуки, інтерактивні дошки, телефони, тобто кожен представник колективу є активним користувачем гаджетів, відповідно, Інтернету для організації освітнього процесу у початковій школі Гвардійського ліцею. Таке широке використання технічних засобів та мережі Інтернет зумовлює загрози цифрового середовища як для членів колективу працівників, так і для здобувачів початкової освіти. Вимогою часу стає готовність вчителів та учнів до безпечного використання інтерне-продуктів.

У відповідях на питання «Які заходи ви вживаєте для забезпечення інформаційної безпеки під час навчання?» найпоширенішою були: проведення роз’яснювальних бесід; контроль за кількістю часу, який учні використовують для використання Інтернету; обмеження вільного доступу до мережі Інтернет в школі.

Даючи відповідь на питання «Чи маєте ви доступ до програмних продуктів із забезпечення інформаційної безпеки» більшість респондентів дали схвальну відповідь 12 опитаних (85,7%), 2 опитаних (14,3%) відповіли, що не цікавилися даним питанням.

Щодо питання про ресурси, які вважають члени колективу корисними для забезпечення інформаційної безпеки в класі, більшість опитаних – це 13 осіб (93%) назвали (навчальні відео, мультиплікаційну продукцію (ЮНІСЕФ)), 1 особа (7%) назвала спеціалізовані веб-сайти. Такі відповіді дозволяють зробити висновок про обізнаність членами педагогічного колективу онлайн-засобів для організації інформаційної безпеки у початковій школі.

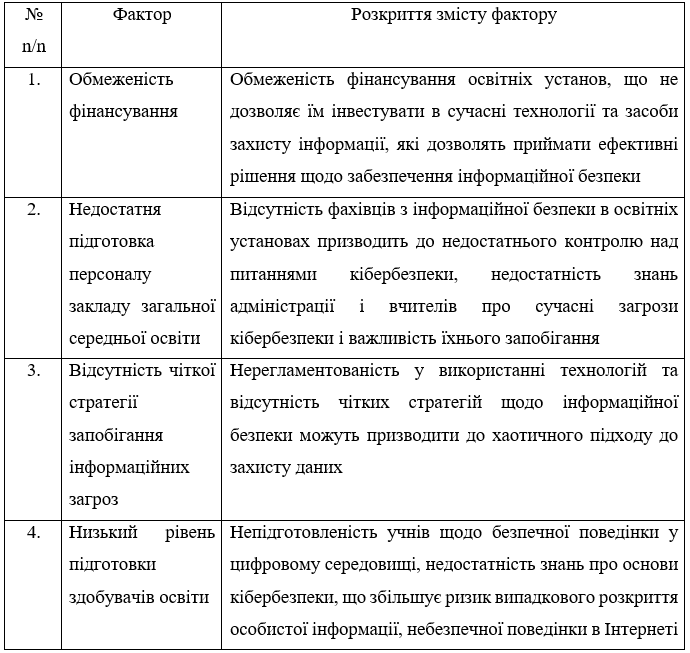
У відповідях на питання «Як ви вважаєте, чи важливо залучати батьків до питань інформаційної безпеки?» усі 14 респондентів (100%) надали стверджувальну відповідь, що свідчить про розуміння важливості співпраці між батьками та членами колективу, яка дозволить досягнути швидшого результату щодо підготовки дітей до безпечного використання цифрового середовища.

Відповіді на питання про заходи щодо забезпечення інформаційної безпеки, які ви б вчителі хотіли втілити разом з батьками? 8 респондентів (57%) запропонували: освітні семінари, консультації з кібербезпеки, обговорення правил користування інтернетом. 6 респондентів (43%) запропонували створити спільно з батьками інформаційні бюлетені та організувати симуляції, які допоможуть батькам і дітям разом вчитися розпізнавати потенційні загрози в інтернеті, такі як фішинг або соціальна інженерія. Отже, ми можемо зробити висновок про те, що вчителі готові до співпраці із батьками, організації та проведення різних заходів із забезпечення інформаційної безпеки у початковій школі.

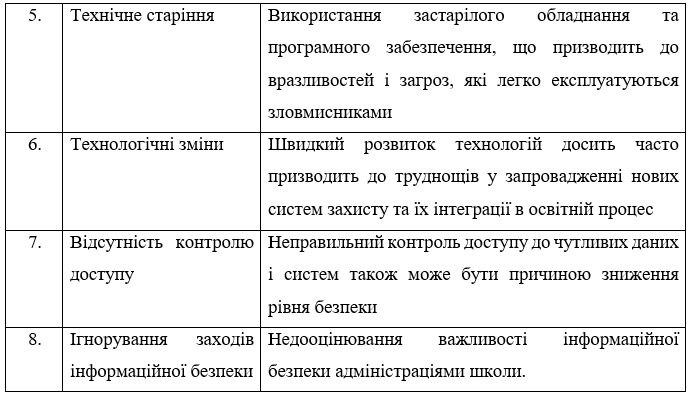
Окрім того, нами було проведено круглий стіл із працівниками і батьками Гвардійського ліцею на тему «Захист дітей у цифровому світі: актуальність проблеми і перспективи вирішення», план проведення якого подано у додатку Е. Дане обговорення дозволило виокремити фактори недостатньої організації інформаційної безпеки у початковій школі (Таблиця 2.1).

Таблиця 2.1.

Фактори недостатньої організації інформаційної безпеки у початковій школі



Продовження таблиці 2.1



Визначення факторів, які впливають на організацію інформаційної безпеки у закладах загальної середньої освіти, підготовку до безпечного використання цифрового середовища молодшими школярами, дозволили нам визначити умови ефективної роботи з проблеми нашого дослідження, про що йтиметься у наступному підрозділі.

Окрім опитування членів педагогічного колективу початкової школи Гвардійського ліцею, нами було проведено опитування здобувачів початкової освіти. Нашим дослідженням було охоплено дітей 2-их, 3-іх, 4-их класів (94 молодших школярі), оскільки у перших класах проходив ще адаптаційний період.

Наші бесіди складалися із питань, які подано у Додатку Є. Відповіді молодших школярів дозволили розширити розуміння проблеми дослідження та знайти ефективні умови її вирішення.

Так, на питання «Чи користуєшся ти комп’ютером або планшетом» 81 дитина (86%) дала схвальну відповідь, а 13 дітей (14%) зазначили, що більше користуються мобільними телефонами. Тобто, усі учні початкової школи є користувачами комп’ютерів, ноутбуків та інших гаджетів, для користування якими вони використовують мережу Інтернет, про що зазначили усі діти.

Підтвердженням актуальності досліджуваної нами проблеми стали відповіді на питання «Як часто ти використовуєш Інтернет?»: 89 дітей (95%) використовують Інтернет щодня і тільки 5 дітей (5%) користуються Інтернетом кілька разів на тиждень. Уточнюючи дану інформацію, діти зазначили, що, як правило користуються інтернетом без нагляду батьків, самостійно.

Даючи відповідь на питання «Які сайти чи програми ти часто використовуєш?» більшість дітей зазначили ТікТок, YouTube, Instagram, Netflix, Disney+, Рixar; відеоігри (Roblox, Мinecraft). Дані відповіді дозволяють зазначити про розважальний контент, який використовують діти, хоча сьогодні є досить значна кількість освітнього контенту для мотивації у навчанні та стимулюванні пізнавального інтересу. Майже 56% дітей мають власні акаунти у Instagram, ТікТок, хоча це заборонено політикою даних соціальних мереж, у яких неймовірна кількість небезпечного, шкідливого, принизливого контенту для дітей молодшого шкільного віку.

Про необізнаність дітей із небезпечними сайтами та їх ознаками вказують відповіді дітей на питання «Чи знаєш ти, які сайти є небезпечні?», оскільки жоден молодший школяр не назвав особливості, ознаки небезпечних сайтів. Більше того, інформація про те, що є небезпечні сайти викликала у дітей здивування.

Більшість дітей зазначили, що спілкуються із незнайомими людьми в Інтернеті, особливо під час участі у колективних відеоіграх. У контексті нашого дослідження цей факт означає, що є великий ризик, неконтрольованого спілкування дітей молодшого шкільного віку із незнайомими людьми під час ігор, під час використання соціальних мереж.

На питання «Чи говорили вам у школі про безпеку в Інтернеті?» 42 опитаних дітей (45%) дали схвальну відповідь, 4 дитини (4%) зазначили, що їм про небезпеку в Інтернеті розповідали батьки, 48 дитини (51%) не дали ніякої відповіді. Такий стан речей свідчить про необхідність впровадження умов, системи роботи із забезпечення інформаційної безпеки у початковій школі.

Найбільше із наданої інформації діти запам’ятали, що не можна ділитися особистою інформацією: ім’ям і прізвищем, адресою; не підходити до незнайомих людей, особливо авто; повідомити дорослих, якщо були такі випадки. З’являється необхідність системної роботи із молодшими школярами щодо вивчення основ кібербезпеки, правил поведінки у цифровому середовищі, алгоритму дій у разі небезпечної ситуації у цифровому середовищі та ін.

Проведене нами опитування учнів початкової школи дозволяє зробити деякі висновки: діти є активними користувачами мережі Інтернет, у більше 50% дітей є власні сторінки у соціальних мережах; досить частим, щоденним, неконтрольованим у часі є використання різної цифрової інформації, різних сайтів і мереж розважального контенту здобувачами початкової освіти; молодші школярі, практично, не обізнані і не усвідомлюють ризиків, шкідливості використання інформації різної за змістом, не знають послідовності дій, якщо стали жертвою кіберзлочинців; у початковій школі досить обмеженою є робота щодо забезпечення педагогічним колективом інформаційної безпеки. Опитування членів педагогічного колективу дозволяє зазначити, що у початковій школі практично відсутня система роботи із забезпечення і організації інформаційної безпеки, більше того, адміністрація, вчителі недооцінюють важливість вирішення даної проблеми підготовки дітей і дорослих до життя в цифровому середовищі інформаційної безпеки. Однак, для членів педагогічного колективу є доступними у використанні як технічні засоби: комп’ютери, ноутбуки, інтерактивні дошки, різні гаджети тощо, так і Інтернет, відповідно, доступні соціальні мережі, сайти, платформи та ін. Представники адміністрації зазначили про нестачу коштів для придбання захисних систем, антивірусного програмного забезпечення та фаєрволів для захисту комп’ютерних систем, сайтів, регулярного оновлення програмного забезпечення та систем безпеки у школі. Ще однією проблемою, яку означили члени адміністрації є відсутність підготовлених до роботи в закладі освіти системних адміністраторів, функціональними обов’язками яких є створення системи обмеження доступу до чутливих даних та відкриття доступу до неї лише для авторизованих користувачів, використання паролей та інших методів аутентифікації. Дана проблема стосується і створення, придбання платформ для онлайн-навчання, дистанційного навчання, створення різноманітних електронних ресурсів та їх захист від недоброчесного використання, зовнішнього втручання.

Аналіз науково-педагогічної літератури, вивчення досвіду зарубіжних країн, власні спостереження за діяльністю початкової школи, дослідження стану забезпечення інформаційної безпеки, яке включало опитування педагогічного колективу і здобувачів початкової освіти, дозволили визначити умови організації інформаційної безпеки у сучасній початковій школі: підвищення цифрової освіти членів педагогічного колективу початкової школи; виховання культури поведінки молодших школярів під час використання цифрового середовища; інформаційно-консультативна підтримка в початковій школі через систему педагогічного дорадництва.

**2.2. Підвищення цифрової освіти членів педагогічного колективу як умова інформаційної безпеки здобувачів початкової освіти**

Вивчення проблеми інформаційної безпеки у початковій школі дозволяє зазначити, що вона у повній мірі залежить від представників педагогічних колективів, від їхньої готовності, компетентності створення безпечного інформаційного середовища, впровадження ефективної системи підготовки здобувачів початкової освіти до користування соціальними мережами, сайтами, пошуковими системами та Інтернетом загалом, до виховання культури поведінки молодших школярів у цифровому середовищі, формування вміння виокремити ризики, фішинг, шахрайські схеми тощо. Зважаючи на швидкість і стрімкість розвитку інформаційних технологій члени педагогічних колективів мають постійно підвищувати свої цифрові навички, що сприятиме розвитку освітнього процесу, покращуватиме взаємодію з учнями та створюватиме сприятливе середовище для навчання. Отримані знання з цифрової освіти, новітніх інформаційних технологій освітяни зуміють використати як для особистісного, професійного розвитку, так і для навчання молодших школярів. Особливу увагу ми звертаємо на знання щодо інформаційної безпеки, адже у сучасному світі кожна людина, починаючи із наймолодшого віку, активно використовує Інтернет та всі його можливості, разом із тим, ризикує стати жертвою цього самого середовища.

Як ми зазначали у попередніх підрозділах нашого дослідження, зважаючи на стрімкий розвиток технологій, діти все частіше стикаються з різними онлайн-ресурсами, соціальними мережами, а також потенційними загрозами, пов’язаними з використанням Інтернету. Підвищення цифрової грамотності вчителів є необхідною умовою для забезпечення інформаційної безпеки дітей, оскільки дозволяє усвідомлено і відповідально користуватися цифровими технологіями, стає критично важливою для забезпечення інформаційної безпеки молодших школярів. Вчителі виконують ключову роль у формуванні цифрових навичок у дітей, і їхній рівень знань та умінь безпосередньо впливає на безпечне користування технологіями учнями.

Про підвищення цифрової грамотності освітян і їхню ключову роль в забезпечені інформаційної безпеки зазначено у статті «Як учителям підвищити цифрові компетентності» [60], де вказано про ухвалення Концепції розвитку цифрових компетентностей до 2025 року [28]. У даному документі 21 компетентність сформовано у 5 сфер, одна з яких є саме «Розвиток цифрової компетентності учнів», важливим аспектом якої є знання і навички з кібербезпеки. Веб-ресурс НУШ пропонує 7 порад для вчителів про те, як навчити учнів безпечної поведінки в Інтернеті [52].

Тобто, цифрова грамотність вчителів є першим кроком до створення безпечного інформаційного середовища для учнів початкової школи. Вчителі, які мають високий рівень знань про технології, можуть ефективно навчати дітей основам роботи з інформацією, включаючи критичний аналіз джерел, визначення фейкових новин та безпеку в Інтернеті. Завдяки цьому учні отримують необхідні навички для розпізнавання потенційних загроз, що формує їхню інформаційну свідомість.

Вчителі, які добре розуміють цифрові інструменти, можуть інтегрувати їх у освітній процес, створюючи інтерактивні уроки, що мотивують пізнання здобувачів початкової освіти. Використання вчителем у роботі з молодшими школярами ресурсів мережі Інтернет, демонстрування правильного використання ресурсів, не лише покращує засвоєння матеріалу, але й навчає дітей безпечного використання інформаційних технологій. Так, наприклад, вчителі, використовуючи онлайн-платформи для проведення уроків, можуть одночасно пояснювати правила безпеки роботи в Інтернеті.

Варто зазначити і той момент, що вчителі є моделями поведінки для своїх учнів, а отже, якщо вчитель демонструє відповідальне ставлення до цифрових технологій, дотримуючись правил безпеки, учні, будуть переймати ці практики. Наприклад, вчителі демонструють правильний захист своїх акаунтів, як уникати небезпечного контенту та безпечно спілкуватися в мережі, що дозволить формувати культуру безпеки не лише на рівні знань, але й на рівні поведінки.

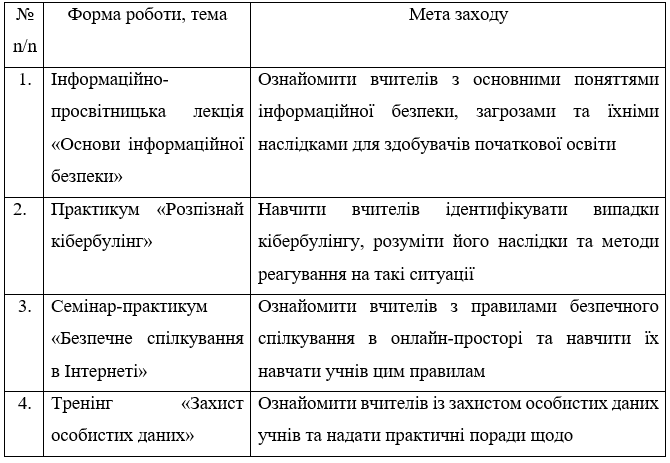
Окрім того, цифрова грамотність вчителів дозволяє їм активніше взаємодіяти з батьками учнів та місцевою громадою. Досить ефективними формами роботи є семінари та інформаційні сесії для батьків, де іде роз’яснювальна робота щодо безпеки вдома, інтернет-просторі, як підтримувати дітей у розвитку цифрових навичок. Варто зазначити, що таке співробітництво допомагає створити єдину стратегію захисту дітей в інформаційній сфері.

Обізнаність у цифровій грамотності вчителів сприяє швидкому реагуванню на потенційні загрози, такі як кібербулінг чи викриття особистих даних учнів. Тільки за умови особистої готовності вчителя вбачається нам можливим навчити дітей правилам поведінки в небезпечних ситуаціях, сформувати вміння захисту своїх прав в інформаційному просторі.

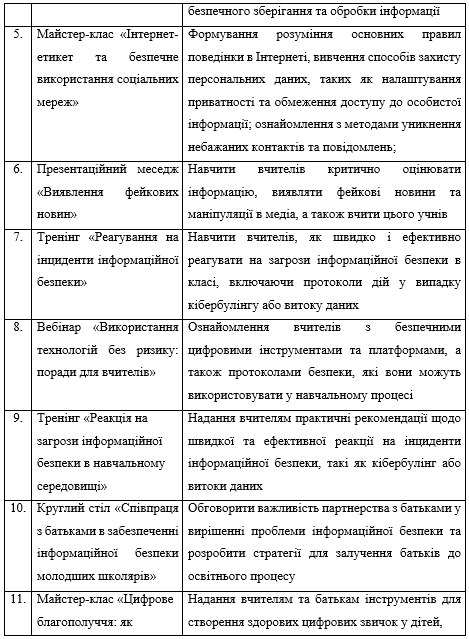
Тобто, цифрова грамотність вчителів має вирішальний вплив на інформаційну безпеку молодших школярів. Вчителі, які володіють сучасними технологіями та знаннями про інформаційну безпеку, можуть ефективно навчати учнів, формуючи в них навички, які допоможуть їм безпечно орієнтуватися в цифровому середовищі. Співпраця між вчителями, учнями та батьками сприяє створенню безпечного простору для навчання, де діти можуть розвиватися, не боячись загроз з боку сучасних технологій. Забезпечення інформаційної безпеки молодших школярів через підвищення цифрової грамотності вчителів – це інвестиція в їхнє здорове та безпечне майбутнє.

Досить ефективними серед форм навчання і підготовки вчителів до забезпечення інформаційної роботи є: тренінги, практичні сесії, семінари (семінари з експертами, обговорення кейсів), вебінари (онлайн-навчання, записані сесії), майстер-класи, круглі столи та ін.

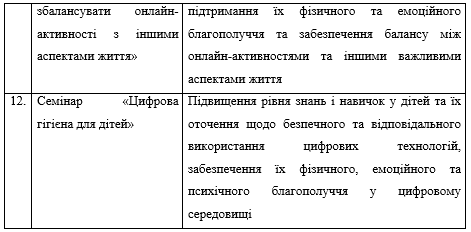
Розуміючи роль вчителя у формуванні навичок інформаційної безпеки у молодших школярів нами було запропоновано цикл заходів для вчителів Гвардійського ліцею, зміст яких розкривав різні аспекти поведінки у цифровому середовищі. План роботи було продумано на ІІ семестр навчального року. Метою заходів було підвищення цифрової грамотності вчителів, знайомство із законодавством, способами, алгоритмами захисту користувачів інформаційними ресурсами, зокрема дітей молодшого шкільного віку. Пропонуємо план роботи із проведення заходів для вчителів з підготовки їх до забезпечення інформаційної безпеки здобувачів початкової освіти (Таблиця 2.2).

Таблиця 2.2

Продовження таблиці 2.2.



Продовження таблиці 2.2.



Проведення заходів з вчителями початкової школи на тему інформаційної безпеки та цифрової гігієни принесли позитивні результати, які ми відслідковували під час спілкування і спостереження за роботою вчителів початкової школи: вчителі отримали актуальну інформацію про загрози та ризики, пов’язані з використанням Інтернету та цифрових технологій, над якими вони часто і не замислювалися; отримали знання про методи захисту персональних даних та ознайомилися з основними принципами кібербезпеки; деякі теми цифрової безпеки вчителі змогли інтегрувати у інші предмети; вчителі почали більше звертати увагу на загрози в Інтернеті, розповідати про ризики. Проведені спільні зустрічі для батьків і вчителів сприяли тому, що батьки почали опікуватися проблемою інформаційної безпеки, встановлювати програми з батьківським контролем, цікавитися сайтами, платформами, іграми, які використовують діти.

Дуже важливим, у контексті нашого дослідження, є усвідомлення вчителями необхідності продуманих дій і кроків щодо інформаційної безпеки дітей, формування навичок безпечного користування інформаційними технологіями, які необхідними для навчання, вибору і виконання функцій у майбутній професійній діяльності.

Забезпечення інформаційної безпеки молодших школярів вимагає систематичної роботи з вчителями, використання різноманітних форм навчання та активної взаємодії з учасниками. Включення цих форм у процес підготовки педагогів сприятиме формуванню безпечного навчального середовища для дітей.

**2.3. Виховання культури поведінки молодших школярів під час використання цифрового середовища**

Наступну умову інформаційної безпеки молодших школярів ми визначили, як виховання культури поведінки молодших школярів під час використання цифрового середовища.

Культуру поведінки дитини у цифровому середовищі ми розглядаємо як сукупність норм, правил та етичних принципів, які визначають поведінку дитини в Інтернеті та з цифровими технологіями. Культура поведінки є проявом сформованості моральних почуттів і моральної свідомості особистості у процесі знайомства із оточуючим світом. Вона включає знання про совість, добро і зло, честь і гідність, які проявляються у спілкуванні і діяльності, принципах, нормах життя людини, навіть тоді, коли ситуації і події не є контрольованими. Спілкування у інформаційному просторі, у більшості випадків, носить анонімний характер, коли ти можеш приховати чи змінити ім’я, використовуєш лінки, що дозволяє поводити себе не так, як у реальному житті. Така особливість онлайн-взаємодії вимагає високого рівня сформованості культури поведінки молодших школярів.

У свою чергу, формування культури поведінки нерозривно пов’язана із морально-правовим вихованням молодших школярів, яке включає формування вміння відстоювання власних кордонів, убезпечення від злочинних і шахрайських дій, відповідальності за власні дії та наслідки порушень законів, непримиримості до порушення загальноприйнятих прав кожної особистості, дотримання норм законодавства, розуміння верховенства права, освоєння правових і моральних норм поведінки [2].

Незаперечним є той факт, що культура поведінки пов’язана із етикою, яка визначає систему моральних принципів та правил, що регулюють моральну поведінку людини, вказує на те, що є правильним чи неправильним, добрим чи злим. З метою відображення взаємозв’язку між культурою поведінки і етикою ми зробили порівняльний аналіз між цими поняттями, який подали у таблиці 2.3.

Таблиця 2.3

Взаємозв’язок між поняттями «культура поведінки» і «етика»

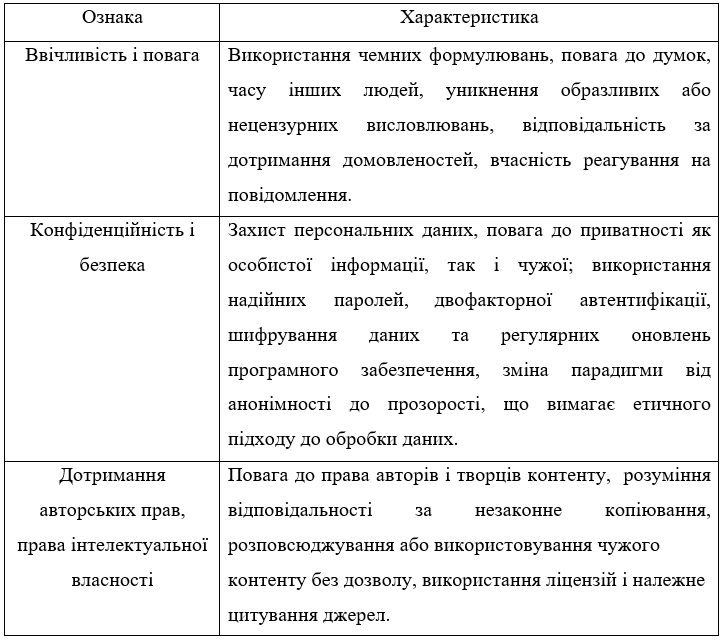


Таким чином, культура поведінки і етика взаємодоповнюють і впливають одна на одну, допомагаючи людям співіснувати в суспільстві та підтримувати гармонійні взаємини. Моральні принципи та цінності проявляються у манерах, стилі спілкування та поведінці, впливаючи на формування соціальних норм і традицій, які є основою культури поведінки [3]. Саме етика формує основу для культури поведінки, яка, в свою чергу, відображає етичні цінності. Культура поведінки є досить специфічним поняттям, яке відрізнятися в різних культурах, на відміну від якої етичні принципи мають універсальний характер. Так, наприклад, повага до інших людей – це універсальний етичний принцип, але спосіб вираження цієї поваги може відрізнятися в різних культурах.

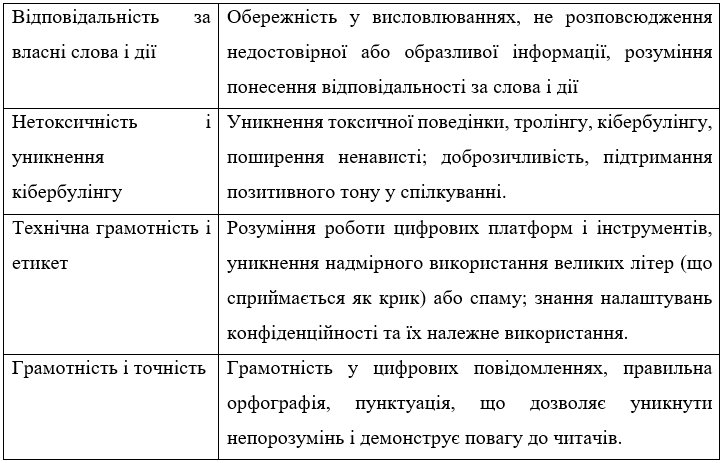
Особлива культура поведінки властива цифровому середовищу, характерні ознаки якого ми подали у таблиці 2.4.

Таблиця 2.4

Ознаки культури поведінки у інформаційному середовищі



Продовження табл. 2.4.



Культура поведінки у цифровому середовищі, часто названа цифровим етикетом або нетикетом, є важливим аспектом сучасного життя, оскільки значна частина нашого спілкування та взаємодії відбувається онлайн.

Загалом, культура поведінки у цифровому середовищі відображає основні принципи етики та моралі, адаптовані до нових умов комунікації. Вона спрямована на підтримання здорового і безпечного середовища для всіх користувачів Інтернету, сприяючи взаємній повазі, відповідальності і безпеці.

Саме одним із завдань сучасної початкової школи є убезпечення молодших школярів від негативного впливу інформаційних технологій, про що ми зазначали у попередніх підрозділах нашого дослідження. Небезпечними для дітей даного віку у контексті цифрового середовища, як зазначають О. Кузнєцова та О.Удалова [29], є кібербулінг, ігрова залежність, дитяча парнографія, кібергрумінг. Саме цілеспрямована діяльність початкової школи із підвищення правової свідомості батьків і дітей, рівня готовності і обізнаності в проблемі порушення безпечного користування цифровими технологіями, формування вміння протистояти негативним моментам під час користування, здатна вибудувати міцні основи для інформаційної безпеки особистості. Зазначимо, що недостатньою є тільки обізнаність дітей у правових нормах, а особливо важливою є готовність діяти відповідно до законодавства.

Поведінка, в основі якої лежать етичні принципи, характеризується:

- дотриманням ввічливості при спілкуванні з іншими в онлайн-спільнотах, соціальних мережах та іграх;

- повагою до різноманітності думок, культур і досвіду інших користувачів;

- усвідомленням наслідків своїх дій в Інтернеті, включаючи обмін інформацією та коментарями;

- відповідальністю за дотриманням авторських прав та уникнення плагіату;

- збереженням конфіденційності особистої інформації та дотримання правил приватності;

- уникнення надання особистих даних стороннім особам або підозрілим ресурсам;

- оцінка достовірності інформації та джерел в Інтернеті, уникнення поширення фейків та дезінформації;

- уміння розпізнавати маніпуляції та захищатися від кіберзагроз, таких як фішинг;

- налаштувань конфіденційності для захисту особистих даних;

- усвідомлення потенційних небезпек, таких як кібербулінг, та способів реагування на них;

- усвідомлення важливості збереження позитивного онлайн-іміджу;

- усвідомлення важливості збереження здорового балансу між використанням цифрових технологій та іншими аспектами життя, такими як фізична активність, хобі та спілкування офлайн;

- вміння допомагати іншим користувачам в Інтернеті та звертатися за допомогою, коли виникають проблеми.

Формування культури поведінки у цифровому середовищі є важливою складовою виховання сучасних дітей, оскільки вона допомагає їм стати відповідальними та усвідомленими користувачами цифрових технологій.

Ми запропонували роботу для дітей початкової школи Гвардійського ліцею взяти участь у діяльності гуртка «Дружній Інтернет». Нами було проведено рекламну компанію щодо участі у гуртку серед дітей і батьків 2, 3, 4 класів початкової школи, розіслано інформацію щодо набору у гурток у вайбер і телеграм групи. До роботи гуртка долучилося 24 дитини.

Мета гуртка: створення позитивного і безпечного інтернет-середовища для здобувачів початкової освіти, формування корисних навичок щодо дотримування етичних принципів і відповідального користування цифровими технологіями.

Завдання гуртка:

1. Розвивати цифрову грамотність, ознайомити і закріпити знання дітей з основ користування Інтернетом, з пошуку інформації, використання соціальних мереж, електронної пошти та інших онлайн-сервісів.
2. Ознайомити з основами кібербезпеки, розвивати вміння щодо розпізнавання потенційних загроз: фішинг, кібербулінг, шахрайство, навички захисту особистих даних.
3. Формувати відповідальне ставлення за свої дії в Інтернеті, включаючи дотримання авторських прав і прав інтелектуальної власності.
4. Розвивати критичне мислення, вміння аналізувати інформацію, розрізняти фейкові новини та надійні джерела, розуміти наслідки поширення недостовірної інформації.
5. Виховувати культуру поведінки у цифровому середовищі: принципи ввічливості та поваги в інтернет-спілкуванні, правила етикету, уникнення некоректної поведінки.
6. Сприяти формуванню позитивного і доброзичливого середовища для спілкування в Інтернеті, заохочувати підтримку і взаємодопомогу серед учасників.

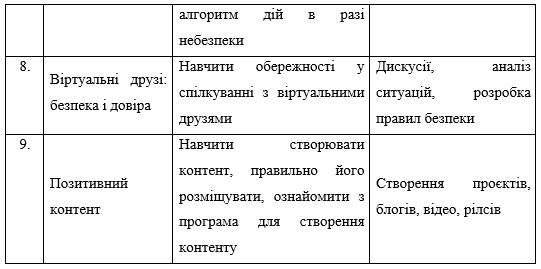
План роботи гуртка подано у таблиці 2.5.

Таблиця 2.5

План роботи гуртка «Дружній Інтернет»



Продовження табл.2.5



|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Участь здобувачів початкової освіти у гуртку «Дружній інтернет» протягом ІІ півріччя, спостереження за ними, дозволяє нам зазначити, що поведінка дітей, які відвідували гурток, має значні позитивні зміни, які сприяють всебічному розвитку дітей та підготовці до сучасного цифрового світу. Так, учні отримували знання про основи Інтернету, вивчали навігації, основи пошуку інформації та використання сучасних технологій для навчання і розваг. Окрім того, участь у гуртку допомогла дітям розвивати навички ввічливого і коректного спілкування як в Інтернеті, так і в звичайному середовищі. Школярі вивчали правила етикету поведінки і діяльності у цифрових мережах, поваги до інших користувачів та уникнення конфліктів, негативної поведінки, розвивали вміння захисту своїх особистих даних та уникнення онлайн-загроз, таких як фішинг, шахрайство, кібербулінг. Досить цікавим за відгуками здобувачів початкової освіти було заняття щодо створення надійних паролей і налаштовувань в онлайн-просторі.

Завдяки участі у гуртку поглибилися знання молодших школярів про аналіз і критичне оцінювання інформації в Інтернеті, розпізнавання фейків та аналіз джерел. Оскільки значна увага приділялася спілкуванню в цифровому середовищі, деякі діти стали більш доброзичливими один до одного. У роботі гуртка «Дружній інтернет» значна кількість годин була практичного спрямування, тому здобувачі початкової освіти знайомилися із особливостями, правилами створення позитивного контенту, такого як блоги, відео, рілс та інші проєкти, що дозволило розкривати їхній потенціал, творчість, публічність.

**2.4. Інформаційно-консультативну підтримка в початковій школі через систему педагогічного дорадництва**

Інформаційно-консультативну підтримку в початковій школі через систему педагогічного дорадництва визначено ще однією умовою створення безпечного інформаційного середовища для здобувачів початкової освіти.

Як зазначає Саюк В., педагогічне дорадництво є діяльністю професіоналів, консультантів, які володіють теоретичними знаннями та практичними навичками з консультаційних послуг, науково-методичного супроводу, моніторингу проблем педагогічних працівників, підготовки рекомендацій для вирішення проблем, надання інформаційної допомоги, у контексті нашого дослідження, з метою забезпечення інформаційної безпеки молодших школярів [50]. Тобто, педагогічним дорадником вважається той, хто дає поради, супроводжує до вирішення проблеми, протягом отримання знань і формування умінь у молодших школярів, з убезпечення суб’єктів освітнього процесу: молодших школярів, працівників закладу освіти, батьків від негативного впливу цифрового середовища.

Педагогічне дорадництво з інформаційної безпеки у закладі загальної середньої освіти відіграє ключову роль у вихованні свідомого ставлення та навичок, необхідних для безпечного користування Інтернетом, цифровими пристроями та гаджетами, соціальними мережами та платформами.

Розглядаючи сутність педагогічного дорадництва в початковій школі зазначимо, що це процес надання підтримки та рекомендацій, спрямованих на забезпечення ефективного навчання та розвитку учнів, а також створення безпечного та сприятливого навчального середовища. Дорадництво включає в себе не лише академічну підтримку, але й соціально-емоційний розвиток, безпеку в інформаційному середовищі та взаємодію з батьками.

Зазначимо, що педагогічне дорадництво в початковій школі, в контексті інформаційної безпеки, розвивалося у відповідь на зростання цифрових технологій та їхнього впливу на суспільство.

Варто зазначити, що з появою персональних комп’ютерів у 1980-х роках та їх поступовим проникненням у школи, з’явилася потреба навчати дітей безпечному користуванню цими пристроями. Саме цей період вважається початком цифрової епохи та виникнення потреби у дорадництві. Початкові програми з інформаційної безпеки були орієнтовані на базові навички роботи з комп’ютером та знайомство з етичними нормами використання технологій.

У 1990-х роках з масовим впровадженням Інтернету виникла необхідність навчати дітей новим аспектам безпеки, пов’язаним з онлайн-комунікацією. На той час інформаційна безпека охоплювала такі теми, як захист особистих даних, уникнення шкідливого контенту та боротьба з кібербулінгом, що вимагало інтеграції нових підходів у навчальні програми початкових шкіл.

Починаючи з 2000-х років багато країн почали офіційно включати інформаційну безпеку до навчальних програм шкіл. Вчителі проходили спеціалізовані тренінги, а у школах з’явилися посади консультантів з інформаційної безпеки. Ці заходи були спрямовані на створення безпечного цифрового середовища для дітей та формування в них свідомого ставлення до використання технологій.

Сучасний етап розвитку дорадництва з інформаційної безпеки в початковій школі характеризується інтенсивною інтеграцією цифрових технологій в освітній процес і повсякденне життя молодших школярів, що вимагає вдосконалення підходів до навчання інформаційної безпеки та розвитку нових навичок. І на сьогодні педагогічне дорадництво з інформаційної безпеки у початковій школі стає невід’ємним компонентом сучасної освітньої системи, який охоплює різноманітні аспекти, пов’язані з захистом учнів, їхньою інформаційною безпекою та наданням підтримки в освітньому процесі.

Незаперечним є той факт, що ефективність педагогічного дорадництва полягає у системній і послідовній взаємодії суб’єктів освітнього процесу, заходів та загальної політики із забезпечення інформаційної безпеки у початковій школі.

Так, система педагогічного дорадництва з інформаційної безпеки у початковій школі включає:

По-перше, навчальні програми, які сприяють формуванню у дітей основ інформаційної безпеки. Прикладом є інтеграція теми кібербезпеки як у загальний навчальний план, так і окремі заняття з безпечного використання Інтернету та цифрових технологій. Однак, існуючі навчальні програми часто не відповідають актуальним загрозам, з якими стикаються здобувачі. Багато з них не враховують новітні технології, такі як соціальні мережі чи мобільні додатки, що може призвести до недостатньої обізнаності дітей щодо ризиків, які вони можуть зустріти в Інтернеті. Важливим є оновлення навчального контенту, щоб він включав сучасні питання кібербезпеки. На жаль, будемо константувати той факт, що у Гвардійському ліцеї система дорадництва з інформаційної безпеки знаходиться лише у стані розробки, що свідчить про актуальність проблеми інформаційної безпеки та пошуку напрямів, шляхів її вирішення у початковій школі.

По-друге, в школі працюють фахівці, які надають психологічну та консультаційну підтримку здобувачам початкової освіти, які допомагають вирішувати проблеми, пов’язані з булінгом, неналежною поведінкою в мережах та іншими викликами, що можуть загрожувати інформаційній безпеці дітей початкової школи. Тому, необхідно забезпечити доступ до кваліфікованих спеціалістів у всіх закладах освіти, щоб кожна дитина могла отримати інформацію щодо захисту, аналізу інформації, належну підтримку тощо.

По-третє, включення батьків до забезпечення інформаційної безпеки здобувачів початкової освіти, роз’яснювально-інформаційна робота з батьками щодо питань безпеки в Інтернеті, дозволяє створити сприятливе безпечне середовище для учнів і підтримувати їхню інформаційну безпеку. Варто зазначити, що досить часто батьки не мають достатньої інформації про ризики, з якими стикаються їхні діти. Розробка програм навчання для батьків може суттєво підвищити їхню обізнаність, а отже, й здатність підтримувати дітей у безпечному користуванні Інтернетом.

Соціально-психологічний клімат у школі також відіграє важливу роль у забезпеченні інформаційної безпеки. Створення відкритого та довірливого середовища дозволяє дітям вільно говорити про свої проблеми. Важливо забезпечити умови, в яких вони можуть анонімно повідомляти про інциденти, пов’язані з інформаційною безпекою, без страху перед наслідками.

Останнім, але не менш важливим аспектом, є необхідність моніторингу та оцінки ефективності реалізації системи дорадництва. Впровадження систем, що дозволяють виявляти проблеми та коригувати програми відповідно до потреб учнів, може суттєво підвищити їхню ефективність.

Дорадницькі послуги з інформаційної безпеки в початковій школі можуть бути надзвичайно різноманітними та охоплювати широкий спектр напрямів, починаючи від базової обізнаності про безпеку в Інтернеті до більш спеціалізованих аспектів захисту особистої інформації.

Аналіз наукової літератури дозволив виокремити перелік послуг, які можуть бути надані в початковій школі через педагогічне дорадництво.

Так, важливим є забезпечення здобувачів початкової освіти базовими навичками основ інформаційної безпеки через освітні програми та тренінги, спрямовані на пояснення основних понять, таких як паролі, безпечне користування Інтернетом, способи уникнення потенційних загроз, таких як фішинг або шкідливе програмне забезпечення. Беззаперечно, що навчання має бути адаптоване до віку дітей, з використанням інтерактивних методів, які допомагають зробити матеріал цікавим і зрозумілим.

Окрім того, важливим є формування умінь у школярів щодо розпізнавання ознак кібербулінгу та алгоритмів дій у ситуаціях, коли стаєш жертвою онлайн-цькування. У даному контексті значний потенціал мають спеціальні воркшопи, рольові ігри, де розглядаються реальні сценарії та обговорюються ефективні стратегії боротьби з кібербулінгом, практикуються навички реагування у небезпечних ситуаціях.

Окремим важливим аспектом є консультування щодо конфіденційності в Інтернеті, збереження особистої інформації в таємниці, налаштування параметрів конфіденційності на різних платформах, розпізнавання потенційно небезпечних запитів. Ці знання допоможуть дітям усвідомити важливість захисту своїх особистих даних і уникнення ризикованих ситуацій.

Як ми зазначали вище, необхідним є консультування батьків і вчителів через регулярні заходи, консультаційні години, де розглядаються найновіші тенденції та загрози в сфері інформаційної безпеки, а також обговорюються найкращі практики для захисту дітей в Інтернеті. Батьки та вчителі мають бути обізнані про можливі небезпеки, про створення безпечного онлайн-середовища для дітей; мають вміти розпізнавати ознаки проблем та знати, до кого звертатися за допомогою у випадку потреби.

Окремо виділимо послуги з технічної підтримки, які включають допомогу в налаштуванні програмного забезпечення для захисту дітей в Інтернеті, таких як батьківський контроль та антивірусні програми. Таку допомогу під час педагогічного дорадництва фахівці (вчителі інформатики, адміністратори) можуть проводити через індивідуальні консультації з налаштування цих програм, а також через надання рекомендацій щодо безпечного використання різних онлайн-платформ.

З метою реалізації запропонованої умови у Гвардійському ліцеї нами запропоновано створення на базі кабінету інформатики «Дорадницького пункту з інформаційнрої безпеки», проведено інформаційно-інструктивну бесіду з батьками щодо проблеми інформаційної безпеки, повідомлено про відкриття дорадницького пункту в початковій школі, розроблено та нідіслано план роботи у вайбер-групи батьків усіх класів (Таблиця 2.6). Даний пункт, у більшій мірі, було створено для забезпечення технічно-консультаційного супроводу батьківської спільноти з питань безпеки в Інтернеті, соціальних мережах, встановлення паролей та програм.

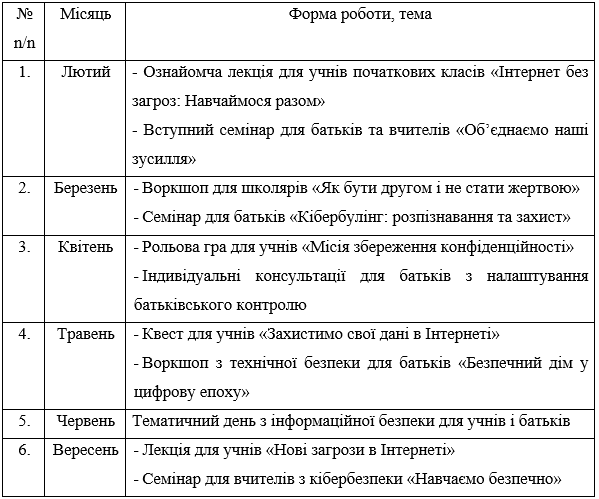
Мета дорадницького пункту: забезпечення здобувачів початкової освіти, батьків, вчителів знаннями та навичками для безпечного користування Інтернетом та сучасними технологіями.

Завдання дорадницького пункту:

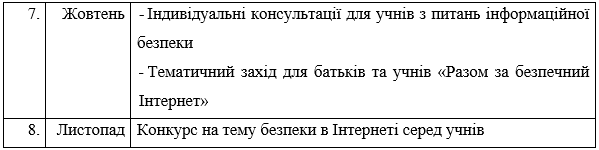
1. Надання базової інформації про загрози в Інтернеті та способи вирішення проблеми.
2. Формування у суб’єктів освітнього процесу початкової школи навичок з розпізнавання та уникнення кібербулінгу. захисту особистої інформації, створення безпечного онлайн-середовища для дітей.
3. Надання технічної підтримки в налаштуванні програмного забезпечення для захисту дітей.

Таблиця 2.6

План заходів дорадницького пункту



Продовження табл. 2.6



З метою оцінки ефективності роботи дорадницького пункту нами проведено опитування батьків Гвардійського ліцею початкової школи (Додаток Ж). Протягом роботи консультаційного пункту постійну участь у заходах брало 38 батьків, тому опитування ми проводили саме з активними учасниками.

Так, на питання опитувальника «Як ви оцінюєте свою обізнаність з основ інформаційної безпеки до участі в дорадницькому пункті?» більшість батьків 36 осіб (94%) зазначили, що за 5-бальною системою їхня обізнаність становила 2-3 б, 2 батьків (6%) зазначили про розуміння ризиків, контроль дітей під час використання ними у онлайн-середовища. Тобто, більшість батьків, фактично, не переймалися проблемою убезпечення дітей від загроз цифрового середовища, хоча зазначили, що усі діти є активними користувачами Інтернету та різних соціальних мереж.

На питання «На скільки ви оцінюєте свою обізнаність з основ інформаційної безпеки після участі в дорадницькому пункті?» думки батьків розділилися: 20 (52,6%) батьків дали відповідь 5 балів за 5-бальною системою оцінювання, 11 батьків (29%) – 4 бали, 7 батьків (18,4%). Для нас такі відповіді дозволяють стверджувати про позитивну роль у забезпечені інформаційної безпеки у початковій школі дорадницького пункту.

Щодо відповідей на 3 питання, батьки відзначали про важливість усіх запропонованих тем, зазначивши про важливість саме технічної підтримки з установок програмного забезпечення, розпізнавання загроз, роз’яснення алгоритму дій у разі небезпеки.

На питання «Які навички ви отримали після участі в дорадницькому пункті?», то респонденти вказали на те, що вони почали акцентувати увагу на контенті, який дивляться і слухають діти, проводять бесіди з правил поведінки у цифровому середовищі, значна частина батьків попросили допомоги щодо установки програми батьківського контролю.

«Чи змінився ваш підхід до використання технологій після участі в дорадницькому пункті?» – на це питання позитивну відповідь дало 38 батьків (100%), що свідчить про необхідність відкриття таких пунктів, оскільки вони сприяють просвітницькій роботі з батьками щодо проблеми дослідження.

29 батьків (76%) визначили середній рівень готовності дитини до безпечного користування Інтернетом після участі в дорадницькому пункті, 4 батьків (10,5%) визначили як високий рівень, 3 батьків (7,8%) визначили як низький і 2 батьків (5,2%) визнали неготовність дитини до користуванні цифровим середовищем у плані безпеки. Варто звернути увагу на те, що про найвищий рівень готовності дітей до убезпечення себе від ризиків під час користування інформаційним середовищем, ніхто із батьків не дав стверджувальну відповідь.

Отже, педагогічне дорадництво відіграє важливу роль в організації інформаційної безпеки в початковій школі, забезпечуючи комплексний підхід до захисту дітей у цифровому середовищі. Завдяки ефективному дорадництву школи можуть розробляти та впроваджувати стратегії, що враховують вікові та індивідуальні особливості учнів, сприяючи їх безпечному та усвідомленому користуванню інформаційними ресурсами.

Основними аспектами дорадництва є надання педагогам, батькам і учням необхідних знань та навичок для захисту від потенційних загроз, пов’язаних із використанням інтернету. Це включає навчання основам цифрової грамотності, правил безпечної поведінки в мережі та розпізнавання небезпек.

Крім того, дорадництво сприяє формуванню культури інформаційної безпеки, де кожен учасник освітнього процесу бере активну участь у підтримці безпечного інформаційного середовища, впроваджуючи превентивні заходи та швидко реагуючи на будь-які інциденти, пов’язані з інформаційною безпекою.

Важливим є те, що дорадництво допомагає створити систему захисту, що не лише забезпечує технічні заходи безпеки, але й сприяє усвідомленому ставленню до інформаційної безпеки як важливого аспекту навчального процесу та виховання в сучасному цифровому світі.

**2.5. Методичні поради вчителям початкової школи, батькам з організації інформаційної безпеки**

Проведена робота з організації інформаційної безпеки у початковій школі Гвардійського ліцею, аналіз науково-педагогічної літератури та нормативної бази, досвід Великобританій, Італії, США та інших країн світу з проблеми дослідження дозволили розробити методичні поради вчителям і батькам із забезпечення інформаційної безпеки здобувачів початкової освіти.

Забезпечення інформаційної безпеки в початковій школі, як ми зазначали у попередніх підрозділах нашого дослідження, є важливим завданням для вчителів, оскільки саме вони формують у дітей основи безпечного користування інформаційними технологіями та Інтернетом. Так, на нашу думку, члени педагогічного колективу початкової школи з метою впровадження і створення умов для інфомаційної безпеки можуть інтегрувати теми з проблеми дослідження у освітній процес. Це може бути реалізовано через уроки інформатики, а також під час занять з інших предметів. Важливо створити навчальні модулі, які б охоплювали основи безпеки в Інтернеті, вміння розпізнавати загрози, такі як кібербулінг, фішинг та інші ризики. Використання ігрових форм навчання, рольових ігор та інтерактивних вправ може значно підвищити інтерес учнів до цих тем.

Окрім того, вчителям слід активно залучати батьків до процесу навчання. Проведення батьківських зборів та семінарів, присвячених питанням інформаційної безпеки, можуть стати чудовою можливістю для обміну досвідом. Батьки повинні бути обізнані з актуальних загроз і методів захисту дітей, тому необхідними є підготовка інформаційних матеріалів, які допоможуть їм зрозуміти, як створити безпечне користування Інтернетом вдома.

Також важливо, щоб вчителі створювали безпечне навчальне середовище, де учні можуть вільно обговорювати свої переживання та проблеми, пов’язані з інформаційною безпекою. Організація анонімних опитувань або скриньок для скарг може допомогти дітям висловлювати свої побоювання без страху перед наслідками. Довірливе ставлення до учнів сприятиме відкритості та зменшенню стресу, пов’язаного з проблемами в онлайн-середовищі.

Оскільки учням початкової школи властиве наслідування значимих дорослих, вчителям необхідно бути прикладом для своїх учнів, дотримуючись правил інформаційної безпеки в своїй поведінці: розумне використання технологій, слідкування за конфіденційністю особистої інформації та безпечне спілкування в Інтернеті, зміст фото і текстів у соціальних сітках тощо.

Одним із ключових аспектів є співпраця з батьками. Організація зустрічей заходів щодо обговорення з батьками питання інформаційної безпеки, надання порада щодо безпечного використання Інтернету вдома сприяють узгодженню зусиль школи та сім’ї у забезпеченні безпеки дітей в онлайновому середовищі.

Не менш важливим є розвиток критичного мислення у дітей. Тобто створення середовища, ситуацій, для отримання навичок аналізу, оцінки інформації, яка отримується з Інтернету, розпізнання недостовірних джерел та формування навичок її аналізу. Критичність в отриманні інформації допоможе дітям бути більш обережними у цифровому середовищі. Пам’ятку для вчителів щодо забезпечення інформаційної безпеки у початковій школі подано у додатку З.

Співпраця із батьками щодо вирішення проблеми нашого дослідження є важливим ключовим компонентом у створенні цілісної системи у роботі з дітьми.

Проведена нами робота дозволяє рекомендувати батькам встановити відкритий діалог з дітьми про їхню онлайн-активність, через відверте спілкування отримати інформацію про сайти, додатки, ігри, коло спілкування дитини в Інтернеті вони відвідують. Заохочувати дітей ділитися будь-якими занепокоєннями або неприємними ситуаціями, з якими вони можуть зіткнутися онлайн.

Досить важливим, на нашу думку, є встановлення чітких правил користування Інтернетом: визначення разом з дітьми часу, який вони можуть проводити онлайн, місця користування гаджетами.

Контроль над контентом також є важливим аспектом: використання програм для батьківського контролю, які допомагають обмежити доступ до небажаних або небезпечних сайтів; встановлення фільтрів для блокування небажаного контенту, а також отримування звітів про онлайн-активність дитини.

Окрім того, необхідним є формування навички у дітей захисту своїх особистих даних. Діти, як активні користувачі Інтернету мають розуміти загрози, якщо вони діляться паролями, адресами або іншими конфіденційними даними в мережі. Важливим є створення паролей і регулярного їх замінення.

Важливо також навчити дітей розпізнавати потенційні загрози. Батькам необхідно пояснити, що таке фішингове повідомлення, як його уникнути, як перевірити підозріле посилання, як визначати неправдиву інформацію в Інтернеті. Діти мають знати і розуміти, що не вся інформація в Інтернеті є достовірною.

Досить важливою є поведінка самих батьків, які мають бути відповідальними користувачами Інтернету, адже діти часто наслідують поведінку дорослих, у тому числі, під час онлайн-активності.

Зрештою, важливо заохочувати дітей до активностей поза Інтернетом: підтримуючи їхні хобі та інтереси, організовуючи спільний час для сімейних заходів, які не пов’язані з технологіями.

Досить ефективним буде колективне створення і прийняття учнями початкової школи правил безпечного користування Інтернетом, які варто розмістити у класних куточках кожного класу. Такими правилами є:

1. Ніколи не ділися своїм ім’ям, адресою, номером телефону чи іншими особистими даними з незнайомими людьми в Інтернеті.
2. Не спілкуйся з людьми, яких ти не знаєш в реальному житті. Будь обережний(а), якщо хтось просить тебе про особисту інформацію, повідом про це вчителю або батькам.
3. Створюй посилені паролі, які складатимуться з літер, цифр і спеціальних символів. Не використовуй однакові паролі для різних акаунтів.
4. Отримавши електронний лист або повідомлення з незнайомими посиланнями, не відкривай його – це може бути шкідливий контент.
5. Не використовуй свої реальні фотографії або особисту інформацію в соціальних мережах, особливо якщо це загальнодоступно.
6. Будь ввічливим(ою) у спілкуванні з іншими користувачами, не використовуй образливих або агресивних коментарів – це може завдати шкоди іншим.
7. Перевіряй надійність джерела, з якого ти отримав(ла) інформацію.
8. Якщо ти відчуваєш, що хтось тебе турбує або ти почуваєшся незручно у спілкуванні онлайн, обов’язково розкажи про це дорослому.
9. Дотримуйся часу, дозволеного для користування Інтернетом. Не проводь занадто багато часу за комп’ютером чи планшетом.
10. Налаштуй параметри конфіденційності на своїх соціальних мережах так, щоб твої дані бачили лише ті, кому ти довіряєш.
11. Переконайся, що твій комп’ютер захищений антивірусом, і програмне забезпечення завжди оновлене.
12. Перед завантаженням будь-якої програми або гри обов’язково запитай дозволу у дорослих.
13. Ти завжди можете відмовитися від розмови або взаємодії, якщо тобі це некомфортно.

У сучасному світі, де Інтернет є невід’ємною частиною життя, забезпечення інформаційної безпеки дітей набуває особливої важливості. Діти дедалі більше часу проводять в онлайновому середовищі, і цей процес потребує особливої уваги з боку батьків та вчителів. Методичні поради для батьків і вчителів є важливим інструментом, який допомагає захистити дітей від потенційних загроз в Інтернеті. Дані поради надають чіткі рекомендації щодо створення безпечного середовища для дітей, допомагаючи батькам і вчителям встановлювати правила користування Інтернетом, розпізнавати загрози та діяти у випадку підозрілих ситуацій. У даному процесі навчання дітей основам цифрової грамотності є критично важливим для їхнього розвитку. Окрім того, методичні поради сприяють формуванню культури відповідального користування Інтернетом, заохочуючи молодших школярів до критичного мислення та відповідальності за власну онлайн-поведінку. Розвиток критичного мислення щодо отриманої інформації допомагає зменшити ризик того, що діти стануть жертвами онлайн-шахраїв або потраплять під вплив небезпечного контенту.

Дотримання правил користування Інтернетом є ключовим для захисту дітей від загроз, які існують в онлайновому середовищі. Такі правила допомагають дітям зрозуміти, як безпечно взаємодіяти з технологіями, а батькам і вчителям – ефективно контролювати їхню онлайн-активність.

Отже, методичні поради для батьків і вчителів, а також дотримання правил користування Інтернетом здобувачами початкової освіти, є необхідними елементами для забезпечення інформаційної безпеки у початковій школі. Саме вирішення проблеми інформаційної безпеки у початковій школі сприяє безпечному розвитку учнів в цифровому світі та формує основу для відповідального ставлення до технологій у майбутньому.

**ВИСНОВКИ**

У дипломному дослідженні розкрито теоретичний і практичний аспекти розв’язку актуальної проблеми у закладах загальної середньої освіти – організації інформаційної безпеки сучасної початкової школи.

Реалізовані мета і завдання дали підстави для формулювання таких висновків:

1. З метою визначення сутності поняття «інформаційна безпека» визначено зміст базових дефініцій проблеми дослідження: «безпека», «комп’ютерна безпека», «медіабезпека». Проаналізовано нормативні документи, які обумовлюють інформаційну безпеку держави, відповідно, закладів освіти, зокрема, початкової школи: Конституція України, Закон України «Про Концепцію Національної програми інформатизації», Закон України «Про інформацію», Рішення Ради з Національної безпеки. Досліджено, що інформаційна безпека розглядається на трьох рівнях: інформаційна безпека особи, інформаційна безпека суспільства, інформаційна безпека держави. Визначено, що поняття «інформаційна безпека» є досить складним та включає різні характеристики: конфіденційність та захист; цілісність; доступність користувачів до освітніх ресурсів; моніторинг і контроль з боку адміністрації та батьків. Виокремлено причини актуальності інформаційної безпеки у початковій школі.

Аналіз науково-педагогічної літератури дозволив виокремити принципи виховання здобувачів освіти в цифровому просторі, компоненти інформаційної безпеки здобувачів початкової освіти. Зроблено висновок про те, що сутність інформаційної безпеки в початковій школі полягає в захисті молодших школярів та їхньої персональної інформації під час користування цифровими технологіями та Інтернетом; забезпечується сукупністю заходів, впровадженням педагогічних умов, системою роботи, спрямованих на захист дітей молодшого шкільного віку від потенційних загроз у цифровому середовищі, розвиток у здобувачів початкової освіти навичок безпечної поведінки та відповідального користування інформаційними технологіями.

1. Виокремлено особливості організації інформаційної безпеки у початковій школі, серед яких: смислова пам’ять, словесно-логічне та вербально-дискурсивне мислення, обмежене розуміння абстрактних концепцій, довільна і короткотривала увага, ігрова діяльність, яка переходить у навчальну, потреба в руховій активності та отриманні вражень, емоційне сприйняття світу, недостатній моральний досвід, кліпове мислення, швидке сприймання картин і образів, підвищена емоційність, інтуітивність, асоціативність і візуальність у діяльності молодшого школяра, наслідування значимих дорослих, формування внутрішньої позиції, несформована здатність до самообмеження.
2. Вивчено досвід Великобританії, Іспанії, Італії, США щодо впровадження політики інформаційної безпеки. З метою недопущення доступу дітей до небезпечної інформації, небажаних сайтів, захисту ментального і фізичного здоров’я дітей проводиться активна державна політика щодо вирішення проблеми інформаційної безпеки дітей, залучення до цього процесу батьків та педагогів. Досліджено, що більшість країн світу ратифікують і послуговуються рядом документів для захисту дітей у цифровому середовищі: «Конвенція про права дитини», «Директива про захист дітей в онлайн-середовищі», «Директива про аудіовізуальні медіа-послуги», «План дій Європейського Союзу з безпеки дітей в інтернеті». Країни ЄС розробляють національні стратегії та плани дій для забезпечення безпеки дітей в Інтернеті, в свою чергу, заклади загальної середньої освіти розробляють власні стратегії організації інформаційної безпеки в Інтернеті, на основі яких проводять семінари та тренінги для батьків, щоб надати важливу інформацію, забезпечити основам цифрової грамотності та методам захисту дітей в Інтернеті, заохочуючи до обговорень з дітьми правил безпечного користування Інтернетом і встановлення сімейних правил щодо часу, проведеного в мережі.
3. З метою аналізу стану забезпечення інформаційної безпеки у початкових школах проаналізовано документи Міністерства освіти і науки України. Визначено, що політика інформаційної безпеки в початкових школах України значною мірою формується на основі державних нормативно-правових актів, які регулюють захист інформації та персональних даних. Так, Міністерство освіти і науки України розробляє законодавство, рекомендації та інструкції щодо забезпечення кібербезпеки в школах. Проте, рівень впровадження цих політик може варіюватися в залежності від конкретного закладу освіти, його фінансових можливостей та обізнаності керівництва.

Проведено дослідження фактичного стану забезпечення інформаційної безпеки у початковій школі Гвардійського ліцею Гвардійської сільської ради Хмельницького району Хмельницької області, у якому взяло участь 94 дитини, 14 педагогічних працівників, серед яких: 7 вчителів, 2 асистента вчителя, директор, 2 заступників директора з навчально-виховної роботи, заступник директора з виховної роботи, психолог/соціальний педагог. Проведено опитування серед здобувачів початкової освіти та пеедагогічних працівників початкової школи. Досліджено, що діти є активними користувачами мережі Інтернет, у більше 50% дітей є власні сторінки у соціальних мережах; досить частим, щоденним, неконтрольованим у часі є використання різної цифрової інформації, різних сайтів і мереж розважального контенту здобувачами початкової освіти; молодші школярі, практично, не обізнані і не усвідомлюють ризиків, шкідливості використання інформації різної за змістом, не знають послідовності дій, якщо стали жертвою кіберзлочинців; у початковій школі досить обмеженою є робота щодо забезпечення педагогічним колективом інформаційної безпеки.

Опитування членів педагогічного колективу дозволяє зазначити, що у початковій школі практично відсутня система роботи із забезпечення і організації інформаційної безпеки, більше того, адміністрація, вчителі недооцінюють важливість вирішення даної проблеми підготовки дітей і дорослих до життя в цифровому середовищі інформаційної безпеки. Серед проблем представники адміністрації визначили: нестачу коштів для придбання захисних систем, антивірусного програмного забезпечення та фаєрволів для захисту комп’ютерних систем, сайтів, регулярного оновлення програмного забезпечення та систем безпеки у школі; відсутність підготовлених до роботи в закладі освіти системних адміністраторів; відсутність можливості створення, придбання платформ для онлайн-навчання, дистанційного навчання, електронних ресурсів та їх захист від недоброчесного використання, зовнішнього втручання.

1. Визначено та обґрунтовано умови забезпечення інформаційної безпеки у початковій школі: підвищення цифрової освіти членів педагогічного колективу як умова інформаційної безпеки здобувачів початкової освіти; виховання культури поведінки молодших школярів під час використання цифрового середовища; інформаційно-консультативна підтримка в початковій школі через систему педагогічного дорадництва Розроблено методичні поради для батьків, вчителів, дітей щодо безпечного використання цифрових технологій.

Представлене дослідження не претендує на повноту та завершеність розв’язання проблеми забезпечення інформаційної безпеки у початковій школі. Подальшого вивчення потребують питання підготовки вчителя початкових класів до організації інформаційної безпеки молодших школярів; розробка відповідного інструментарію та ін.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Алєксєєнко Т. Формування безпечної поведінки підлітків в інтернет-мрежах: проблема і перспективи її розв’язання. URL: <https://lib.iitta.gov.ua/id/eprint/715632/2/01_19_%D0%90%D0%BB%D1%94%D0%BA%D1%81%D1%94%D1%94%D0%BD%D0%BA%D0%BE_%D0%A4%D0%BE%D1%80%D0%BC%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%BD%D0%BE%D1%97%20%D0%BF%D0%BE%D0%B2%D0%B5%D0%B4%D1%96%D0%BD%D0%BA%D0%B8%20%D0%BF%D1%96%D0%B4%D0%BB%D1%96%D1%82%D0%BA%D1%96%D0%B2%20%D0%B2%20%D1%96%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D0%BC%D1%80%D0%B5%D0%B6%D0%B0%D1%85%20-%20%D0%BF%D1%80%D0%BE%D0%B1%D0%BB%D0%B5%D0%BC%D0%B0%20%D1%96%20%D0%BF%D0%B5%D1%80%D1%81%D0%BF%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D0%B8%20%D1%97%D1%97%20%D1%80%D0%BE%D0%B7%D0%B2%D1%8F%D0%B7%D0%B0%D0%BD%D0%BD%D1%8F.pdf> (дата звернення: 01.11.2023)
2. Бех І. Особистість на шляху до духовних цінностей. Київ. Чернівці: Букрек, 2018, 296 с.
3. Бибик С. Нетикет, або мережевий етикет. Культура слова. 2015. № 85. С. 125-128
4. Виховання дітей та молоді у цифровому просторі: посібник / [Журба К. О., Канішевська Л. В., Малиношевський Р. В., Харченко Н. В., Федоренко С. В.]. Київ, 2022. 124 с.
5. Великий тлумачний словник сучасної української мови (з дод. і допов.) / Уклад. і голова. ред. В.Т. Бусел. К.; Ірпінь: ВТФ «Перун», 2005. 1728 с. ISBN 966-569-013-2. URL: <https://archive.org/details/velykyislovnyk/page/17/mode/1up> (дата звернення: 10.11.2023)
6. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою: навч. Посібник. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с.
7. Головко О. М. Медіабезпека людини: засади інформаційної правової політики: Монографія – Київ: Видавничий дім «АртЕк». 2019. 168 с. URL: <https://www.ippi.org.ua/mediabezpeka-lyudini-zasadi-informatsiino-pravovoi-politiki> (дата зверненння: 11.11.2023)
8. Державний стандарт початкової освіти. Постанова Кабінету Міністрів України від 21 лютого 2018 р. № 87 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/ laws/show/688-2019-%D0%BF#n8
9. Дізнайся про свої права в цифровому середовищі. Рекомендації Ради Європи щодо поваги, захисту та здійснення прав дитини в цифровому середовищі. Для дітей і молодих людей віком до 18 років. URL: <https://rescentre.org.ua/images/Uploads/Images/Internet-safety_blog/Learn_about_ your _ rights_in_a_digital_environment_UKR.pdf.pdf> (дата звернення: 10.10.2023)
10. Діти і соціум: Особливості соціалізації дітей дошкільного та молодшого шкільного віку: Монографія / А. М. Богуш, Л. О. Варяниця, Н. В. Гавриш, С. М. Курінна, І. П. Печенко; Наук. ред. А. М. Богуш; За заг. ред. Н. В. Гавриш. Луганськ: Альма-матер, 2006. 368 с.
11. Діти в Інтернеті: як навчити безпеці в віртуальному світі / І. В. Литовченко, С. Д. Максименко, С. І. Болтівець та ін. К.: Вид. ТОВ Видавничий будинок «Аванпост-Прим», 2010. 48 с. (Посібник для батьків).
12. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних». URL: <https://zakon.rada.gov.ua/laws/show/994_242#Text> (дата звернення: 10.10.2023).
13. Дьякова А. Світова практика. Як захищають дітей в інтернеті Велика Британія, США та ЄС. URL: https://life.nv.ua/ukr/blogs/zahist-ditey-v-interneti-svitova-praktika-50424714.html (дата звернення: 30.12.2024)
14. Забезпечення інформаційної безпеки у США. URL: https://pidru4niki.com/82888/politologiya/zabezpechennya\_informatsiynoyi\_bezpeki#621 (дата звернення: 26.12.2023).
15. Закон України №2297–VІ «Про захист персональних даних». URL: <https://www.president.gov.ua/documents/2297vi-11567> (дата звернення: 10.10.2023).
16. Закон України «Про загальну середню освіту». URL: <https://zakon.rada.gov.ua/laws/show/651-14#Text> (дата звернення: 10.10.2023).
17. Закон України «Про освіту». URL: <https://zakon.rada.gov.ua/laws/show/2145-19#Text> (дата звернення: 10.10.2023).
18. Закон України «Про Національну програму інформатизації» (Відомості Верховної Ради (ВВР), 2023, № 51, ст.127). URL: <https://zakon.rada.gov.ua/laws/show/2807-20#Text> (дата звернення: 04.11.2023)
19. Запорожець Олександр Володимирович / Н. В. Кудикіна // Енциклопедія Сучасної України [Електронний ресурс] / Редкол.: І. М. Дзюба, А. І. Жуковський, М. Г. Железняк [та ін.]; НАН України, НТШ. К.: Інститут енциклопедичних досліджень НАН України, 2010. URL: <https://esu.com.ua/article-15481> (дата звернення: 12.12.2023)
20. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 446 с.
21. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / О. Г. Додонов, В. П. Горбулін, Д. В. Ланде. К.: Інтертехнологія, 2009. 164 с.
22. Інформаційна безпека. Підручник В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с.
23. Кононко О. Л. Психологічні основи особистісного становлення дошкільника (Системний підхід). К.: Стилос, 2000. 336 с.
24. Конституція України. Офіційне інтернет-представництво. URL: https://www.president.gov.ua/documents/constitution (дата звернення: 29.10.2023)
25. Концепція Нової української школи. Концептуальні засади реформування середньої школи/ Упор. Л. Гриневич, О. Елькін, С. Калашнікова, І. Коберник, В. Ковтунець, О. Макаренко, О.Малахова, Т. Нанаєва, Г. Усатенко, П. Хобзей, Р. Шиян/ За заг.ред. М. Грищенко. URL[://mon.gov.ua/storage](https://mon.gov.ua/storage)/app /media/zagalna%20serednya/nova-ukrainska-shkola-compressed.pdf (дата звернення: 12.10.2021)
26. Конвенція про права дитини. URL: <https://zakon.rada.gov.ua/laws/show/995_021#Text> (дата звернення: 10.10.2023)
27. Концепція виховання дітей та молоді в цифровому просторі. Вісник Національної академії педагогічних наук України, 2022, Вип. 4. № 2, С. 1- 30. DOI: <https://doi.org/10.37472/v.naes.2022.4206> (дата звернення: 23.12.2023)
28. Концепції розвитку цифрових компетентностей. URL: <https://thedigital.gov.ua/storage/uploads/files/news_post/2021/3/kabmin-skhvaliv-kontseptsiyu-rozvitku-tsifrovikh-kompetentnostey-do-2025-roku/Dodatok-2.pdf> (дата звернення: 22.01.2024)
29. Кузнєцова О. та Удалова О. Формування культури безпечної поведінки особистості у мережі інтернет. Нові технології навчання, №92. 2019. С. 164-170.
30. Куницький В.В. Захист неповнолітніх в інформаційному просторі як об’єкт гуманітарної експертизи: український та зарубіжний досвід. Державне управління: теорія та практика. Київ. 2011. URL: http://www.academy.gov.ua/ej/ej14/txts/ Kunitskiy.pdf (дата звернення: 26.12.2023)
31. Кунченко-Харченко В., Огірко І., Костельнюк Д. Інформаційні технології прогнозування та моделювання кібербезпеки. URL: https://sites.google.com/view/blog-ua/%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D1%96-%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97-%D0%BF%D1%80%D0%BE%D0%B3%D0%BD%D0%BE%D0%B7%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F-%D1%82%D0%B0-%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F-%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8 (дата звернення: 11.11.2024)
32. Кутєлєва І. Уряд Іспанії пропонує закон про підвищення рівня безпеки дітей в Інтернеті. 2024. URL: <https://www.eurointegration.com.ua/news/2024/06/4/7187425/> (дата звернення: 17.04.2024)
33. Ліпій Я.О., Манжелей Н.М. Особливості впливу Інтернет-мережі на формування особистості молодшого школяра. [Електронний ресурс]. URL: <http://dspace.pnpu.edu.ua/bitstream/123456789/10463/1/> (дата звернення: 27.12.2023)
34. Ліпкан В.А., Сопілко І.М., Кір’ян В.О. Правові засади розвитку інформаційного суспільства в Україні: моногр. / за заг. ред. В.А. Ліпкана. Київ: ФОП О.С. Ліпкан, 2015. 718 с.
35. Лисенко О.М. Міжнародно-правове регулювання прав дитини в кіберпросторі. Соціологія права, 2016. № 3 (18). С. 25–30.
36. Методичні рекомендації з інформаційної безпеки навчального комп’ютерного комплексу / Укл. Дем’яненко В.М., Ковальчук В.Н. К.: ІІТЗН НАПН України, 2014. 39 с.
37. Морзе Н.В. Методика навчання інформатики: Навч. посібник: у 4 ч./ за ред. акад. М.І. Жалдака. К.: Навчальна книга, 2004. Ч. IV: Методика навчання алгоритмізації та програмування. 368 с.
38. Мужанова Т.М. Інформаційна безпека держави: навчальний посібник. К. : ДУТ. 131 с.
39. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.
40. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.
41. Ніколаєнко Н. О., Комарчук О. О. Засоби масової комунікації як детермінанти гібридної війни : монографія / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2021. 217 с.
42. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.
43. Огляд «Інтернет свободи». URL: <https://netfreedom.org.ua/article/u-velikobritaniyi-ta-yes-nabuli-chinnosti-novi-normi-shchodo-bezpeki-v-onlajni-yak-zakoni-mozhut-zminiti-socialni-media-ta-tehnologichni-kompaniyi-oglyad-internet-svobodi-za-lyutij-2024> (дата звернення: 22.12.2023)
44. Петрушко Г. В. Місце і роль інтернету у житті молодших школярів. Матеріали Всеукраїнської науково-практичної конференції «Інновації у роботі вчителя початкових класів: виклики і реалії НУШ». 14 квітня 2020 р., Львів. Центр Прогресивної освіти «Генезум», 2020. 203 с.
45. Про інформацію: закон України від 02.10.1992 р. URL: <https://zakon.rada.gov.ua/laws/main/2657-12#Tex> (дата 08.12.2023)
46. Про основні засади забезпечення кібербезпеки України: закон України від 05.10.2017 р. URL: https://zakon.rada.gov.ua/laws/show/2163- 19#Text (дата звернення: 08.12.2023)
47. Про рішення Ради національної безпеки і оборони України від 15.10.2021 р. «Про Стратегію інформаційної безпеки»: указ Президента України від 28.12.2021 р. URL: https://zakon.rada.gov.ua/laws/show/ 685/2021#n14 (дата звернення: 10.12.2023)
48. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України 15 травня 2013 р. № 386-р.
49. Радзивилюк Є. Особливості убезпечення інформаційного простору Італії в контексті розвитку інформаційно-комунікативних технологій. Міжнародні відносини, суспільні комунікації та регіональні студії. № 1 (7), 2020. URL: [file:///C:/Users/RM-Natali/Downloads/nazar,+%D0%9C%D0%92\_2020\_1\_ %D0%](file:///C:/Users/RM-Natali/Downloads/nazar,+%D0%9C%D0%92_2020_1_%20%D0%25)BE%D1%81%D1%82%D0%B0%D1%82%D0%BE%D1%87%D0%BD%D0%B8%D0%B9-112-122.pdf (дата звернення: 18.01.2024)
50. Саюк В. Зміст освітньо-професійної програми «Педагогічне дорадництво» підготовки магістрів спеціальності 011 «Освітні, педагогічні науки». *Проблеми сучасного підручника, №25*. 2020. 149-159. <https://doi.org/10.32405/2411-1309-2020-25-149-159>. URL: <https://ipvid.org.ua/> index.php/ psp/article/view/62 (дата звернення: 25.04.2024)
51. Сергєєнкова О. П., Столярчук О. А., Коханова О. П., Пасєка О. В. Вікова психологія. Навч. посіб. К.: Центр учбової літератури, 2012. 376 с.
52. 7 порад для вчителів, як навчити учнів безпечної поведінки в інтернеті. <https://nus.org.ua/articles/7-porad-dlya-vchyteliv-pro-onlajn-bezpeku-ditej/> (дата звернення: 22.01.2024)
53. Соціологія: словник термінів і понять. Упор.: Біленький Є.А., Дебой В.М., Козловець М.А., Котвицький А.А., Саух І.В., Федоренко В.О., Цибульський В.О., Жаловага В.О. / за заг. ред. Біленького Є.А. і Козловця М.А. К.: Кондор, 2006. 372 с.
54. Спірін О.М., Ковальчук В.Н. Методика забезпечення он-лайн безпеки старшокласників у навчально-виховному процесі школи. *Інформаційні технології і засоби навчання*. 2011. №1 (21). ISSN 2076-8184. Режим доступу до журналу: <http://www.journal.iitta.gov.ua> (дата звернення: 17.12.2023)
55. Столбов Д. В. Сутність і зміст поняття інтернет-безпеки сучасного школяра. Серія «Педагогіка, соціальна робота». Випуск 33. С. 187-189
56. Теорія розвитку Жана Піаже: стадії розвитку інтелекту. ALEXUS. URL: <https://alexus.com.ua/teoriya-zh-piazhe-prointelektualnij-rozvitok-ditini/#lwptoc> (дата звернення: 22.12.2023)
57. Топчій О. Педагогічні підходи до формування інформаційної безпеки дітей та юнацтва. [URL: https://www.pulib.sk/web/kniznica/elpub/dokument/](URL:%20https://www.pulib.sk/web/kniznica/elpub/dokument/) Bernatova9/subor/Topchij.pdf (дата звернення: 15.12.2023)
58. Якобчук А. Велика Британія впроваджує посилення захисту дітей у соціальних мережах, включаючи обов’язкову перевірку віку. 2024. URL: <https://slovoproslovo.info/velyka-brytaniya-vprovadzhue-posylennya-zahystu-ditey-u-sotsialnyh-merezhah-vklyuchayuchy-obov-yazkovu-perevirku-viku> (дата звернення: 15.12.2023)
59. Як у світі борються з кібербулінгом? Дієві практики. DOCUDAYS.ua. Всеукраїнська ініціатива. URL: <https://bullyingstop.org.ua/news/yak-u-sviti-boryut-sya-z-kiberbulingom-diyevi-praktiki> (дата звернення: 21.12.2023)
60. Як учителям підвищити цифрові компетентності? URL: <https://nus.org.ua/view/yak-uchytelyam-pidvyshhyty-tsyfrovi-kompetentnosti/> (з екрану) (дата звернення: 22.01.2024)
61. Шишкіна К.М. Особливості розвитку молодшого школяра як фактор ефективності формування інформаційної безпеки. *Гуманітарний вісник ДВНЗ* *«Переяслав-Хмельницький державний педагогічний університет імені Григорія Сковороди» – Додаток 2 до Вип. 35, Том I(13): Тематичний випуск «Міжнародні Челпанівські психолого-педагогічні читання»*. К.: Гнозис, 2015. 444 с. 425-431 URL: <https://chelpanov.eeipsy.org/index.php/eeip/issue/view/14/PDF13> (дата звернення: 15.12.2023)
62. Черних О. Формування безпечної поведінки дітей в інтернеті як актуальний напрям соціально-педагогічного супроводу. Інновації педагогічної освіти в умовах викликів сьогодення : монографія / за наук. ред. С. Я. Харченка. К. : Талком, 2019. 343 с. URL:
63. Що роблять діти в соціальних мережах [Електронний ресурс]. URL: <http://мордашки.com/shho-roblyat-diti-v-socialnix-merezhax/> (дата звернення: 27.12.2023)
64. Anderson Ross. Chat Control or Child Protection? arXiv:2210.08958 [cs.CY]. URL: <https://arxiv.org/abs/2210.08958> (<https://doi.org/10.48550/arXiv.2210.08958>)
65. Barker J., and Weller S. (2003). ‘Is it fun?’ Developing children-centred research methods. International Journal of Sociology and Social Policy, 23 (1), р. 33–58.
66. David Bamman, Jacob Eisenstein, and Tyler Schnoebelen. Gender identity and lexical variation in social media. Journal of Sociolinguistics, 2014, № 18(2), р. 135–160.
67. Children’s Internet Protection Act (1999–2000). URL: <https://www.congress.gov/bill/106th-congress/house-bill/4600> (дата звернення: 23.12.2023).
68. Schneier Bruce. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World, W. W. Norton & Company, 2015. ISBN 978-0-393-24481-6

**ДОДАТКИ**

**Додаток А**

**Тренінг з кібербезпеки для суб’єктів закладу освіти**

**Мета тренінгу:** підвищити обізнаність учнів, вчителів та персоналу щодо основ кібербезпеки та політики конфіденційності, навчити безпечному користуванню інформаційними технологіями та забезпечити захист особистих даних.

**Аудиторія:** Учні, вчителі, адміністративний та технічний персонал

**План тренінгу**

**Вступ (15 хвилин)**

Привітання та представлення тренера

Огляд тренінгу та його актуальність

Оголошення мети тренінгу

**Основи кібербезпеки (30 хвилин)**

* Що таке кібербезпека?

Визначення та значення

Основні загрози в Інтернеті

Основні правила кібербезпеки:

* використання складних паролів та двофакторної аутентифікації;
* безпечне користування електронною поштою (не відкривати підозрілі листи та вкладення);
* оновлення програмного забезпечення та систем;
* захист пристроїв;
* використання антивірусного програмного забезпечення;
* регулярне оновлення операційних систем та програм

Безпечний Інтернет:

Розпізнавання фішингових атак;

Безпечне користування соціальними мережами;

Захист приватної інформації.

**Конфіденційність та захист даних (30 хвилин)**

* Що таке конфіденційність?
* Визначення та значення
* Приклади конфіденційної інформації (особисті дані, академічні записи)

**Політика конфіденційності в закладі освіти**

* Збір, зберігання та використання особистої інформації
* Права учнів, вчителів та працівників щодо їхньої інформації
* Контроль доступу
* Використання паролів та аутентифікації
* Ролі та права доступу
* Фізична безпека даних
* Захист серверних кімнат та комп’ютерних класів
* Захист паперових документів
* Практичні завдання (30 хвилин)
* Створення та управління паролями
* Практичне завдання зі створення складних паролів
* Впровадження двофакторної аутентифікації
* Розпізнавання фішингових атак
* Приклади фішингових листів

Практичне завдання з розпізнавання підозрілих повідомлень

Захист приватної інформації

**Обговорення кейсів з порушення конфіденційності**

Вироблення рекомендацій для захисту даних

**Питання та відповіді (15 хвилин)**

Обговорення питань учасників

Пояснення складних моментів

**Підсумок тренінгу (15 хвилин)**

Основні висновки

Рекомендації для подальшого захисту інформації

Роздача інформаційних матеріалів та посібників

Завершення тренінгу

Матеріали для учасників:

Презентація тренінгу

Пам’ятка з основ кібербезпеки

Посібник з політик конфіденційності закладу освіти

Листок з вправами та завданнями

Додаткові ресурси:

Посилання на корисні веб-сайти та ресурси

Рекомендації щодо програмного забезпечення для кібербезпеки

Контактна інформація для додаткової підтримки та консультацій

Цей тренінг допоможе учасникам зрозуміти важливість кібербезпеки та конфіденційності, а також навчить їх практичним навичкам захисту своїх даних та інформації в закладі освіти.

**Додаток Б**

**Обов’язкові завдання з інформаційної безпеки у школах Великобританії:**

* підготовка та впровадження стратегій закладу з онлайн-безпеки, включаючи заходи з фільтрації та моніторингу інтернет-активності учнів на шкільних пристроях і мережах​ (NSPCC Learning)​;
* підготовка персоналу, тобто проходження навчань з питань інформаційної безпеки, з метою ознайомлення з загрозами для дітей в інтернеті та вивчення нових концепції, технологій, підходів з реагування та запобігання інцидентів, пов’язаних з онлайн-безпекою​ (NSPCC Learning)​​ (SWGfL)​;
* включення у навчальний план закладу освіти вивчення дисциплін з проблеми попередження інтернет-залежності, аналізу інформації, шахрайських схем, правил поведінки в соціальних мережах, месенджерах, платформах тощо;
* підготовка і ознайомлення з планом дій, алгоритмом протидії, звернення на випадок кіберінцидентів, включаючи контакти екстрених служб, логіни до ключових систем і процедури реагування на різні види атак, такі як атаки з використанням шкідливого програмного забезпечення або відключення інтернету​ (SWGfL)​;
* створення резервних копій важливих даних і перевірка їх дієвості; зберігання резервних копій у відокремленому місці, з метою уникнення вразливості до атак​ (SWGfL)​;
* партнерська взаємодія з батьками та громадою, з метою інформування батьків і опікунів про заходи з онлайн-безпеки та залучення їх до цього процесу, забезпечення відкритого діалогу та спільної роботи над захистом дітей від онлайн-загроз​ (NSPCC Learning)​.

Зазначені нами завдання убезпечують дітей, користувачів цифровим простором у школах Великобританії від потенційних загроз в Інтернеті, забезпечуючи безпеку здоров’я, добробут дітей.

**Додаток В**

Таблиця 1.3

**Законодавча база із забезпечення інформаційної безпеки дітей у країнах Європи та США**

****

**Додаток Д**

**Опитування для вчителів початкової школи щодо забезпечення інформаційної безпеки**

**Шановні вчителі!**

Дане опитування має на меті оцінити стан інформаційної безпеки в початкових школах, виявити потреби у навчанні та ресурсах. Ваша участь дуже важлива для покращення безпечного навчального середовища для учнів. Вся інформація буде використовуватися анонімно.

1.Як ви оцінюєте свою обізнаність про інформаційну безпеку (в шкалі від 1 до 3, де 1 – не обізнаний (а), 2 – щось мені відомо; 3 – добре обізнаний)?

• 1

• 2

• 3

2. Чи проходили ви навчання або курси з дотримання інформаційної безпеки в початковій школі?

• Так

• Ні

• Якщо так, будь ласка, вкажіть, які курси або тренінги ви проходили:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. Які технічні засоби ви використовуєте в освітньому процесі? (наприклад, комп’ютери, планшети, інтерактивні дошки тощо)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. Чи маєте ви доступ до програмних продуктів із забезпечення інформаційної безпеки?

• Так • Ні

5. Які ресурси ви вважаєте корисними для забезпечення інформаційної безпеки в класі? (наприклад, веб-сайти, книги, програми)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6. Як ви вважаєте, чи важливо залучати батьків до питань інформаційної безпеки?

• Так

• Ні

• Якщо так, які ініціативи ви б хотіли реалізувати для залучення батьків?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Дякуємо за вашу участь! Ваші відповіді допоможуть створити більш безпечне інформаційно-навчальне середовище для наших учнів

**Додаток Е**

План круглого столу

Тема: «Захист дітей у цифровому світі: актуальність проблеми і перспективи вирішення»

1. Вступне слово директора, запрошених гостей з сільської ради і заступників (10 хвилин)

Короткий огляд актуальності питання інформаційної безпеки для дітей молодшого шкільного віку.

2. Панельна дискусія (20 хвилин)

Проблеми інформаційної безпеки в сучасних школах

Обговорення основних викликів, з якими стикаються діти в Інтернеті (кібербулінг, небажаний контент, загрози приватності тощо).

Роль батьків і вчителів у забезпеченні безпеки дітей в Інтернеті

Огляд ролі батьків і вчителів у навчанні дітей безпечного користування інтернетом.

3. Презентація експертів (15 хвилин)

Знайомство запрошених експертів з кібербезпеки та представників правоохоронних органів з актуальними загрозами в Інтернеті та способи їх уникнення.

Практичні поради щодо налаштування безпечного інтернет-середовища вдома і в школі.

4. Обговорення кейсів (15 хвилин)

Аналіз реальних ситуацій та обговорення можливих рішень.

Висвітлення позитивного досвіду в забезпеченні інформаційної безпеки.

5. Групова робота та обговорення (20 хвилин)

Учасники розподіляються на групи (батьки, вчителі, адміністрація) для обговорення конкретних проблем та пропозицій щодо покращення інформаційної безпеки.

Представлення результатів групової роботи та обговорення пропозицій.

6. Підведення підсумків та узгодження рекомендацій (10 хвилин)

Висновки за результатами обговорень.

Узгодження спільних дій для покращення інформаційної безпеки дітей.

Планування наступних кроків і майбутніх зустрічей.

7. Заключне слово (5 хвилин)

Подяка учасникам за участь.

**Додаток Є**

Опитувальник здобувачів початкової освіти щодо обізнаності з поведінки у цифровому середовищі

1. Чи користуєшся ти комп’ютером або планшетом?

• Так • Ні

2. Як часто ти використовуєш Інтернет?

• Щодня

• Кілька разів на тиждень

• Рідко

3. Які сайти чи програми ти часто використовуєш? (наприклад, YouTube, ігри, навчальні платформи)

4. Чи знаєш ти, які сайти є небезпечні?

• Так • Ні

5. Чи спілкуєшся ти з незнайомими людьми в Інтернеті?

• Так • Ні

6.Чи говорили вам у школі про безпеку в Інтернеті?

• Так • Ні

7. Якщо так, що ти запам’ятав/запам’ятала з цих розмов? (можна вибрати кілька варіантів)

• Не ділитися особистою інформацією

• Не відкривати підозрілі посилання

• Повідомляти вчителя або батьків про небезпечні ситуації

• Інше (напишіть, будь ласка):

8. Якщо ти побачив/побачила щось небезпечне в Інтернеті, що ти зробиш?

• Скажу батькам

• Скажу вчителю

• Скажу другу

• Нічого не зроблю

**Додаток Ж**

**Опитування для батьків**

1. Як ви оцінюєте свою обізнаність з основ інформаційної безпеки до участі в дорадницькому пункті?

1 (дуже низька)

2

3

4

5 (висока)

1. На скільки ви оцінюєте свою обізнаність з основ інформаційної безпеки після участі в дорадницькому пункті?

1 (дуже низька)

2

3

4

5 (висока)

1. Які теми з інформаційної безпеки ви вважаєте найбільш корисними? (можна вибрати кілька варіантів):

Кібербулінг

Захист особистих даних

Безпечне спілкування в Інтернеті

Виявлення фейкових новин

Використання технологій безпечно

Інші (вкажіть):

1. Які навички ви отримали після участі в дорадницькому пункті? (можна вибрати кілька варіантів):

Розпізнавання загроз у цифровому середовищі

Реагування на інциденти інформаційної безпеки

Проведення бесід з дітьми про безпеку в Інтернеті

Інші (вкажіть):

1. Чи змінився ваш підхід до використання технологій після участі в дорадницькому пункті?

Так

Ні

1. Як ви оцінюєте готовність вашої дитини до безпечного користування Інтернетом після участі в дорадницькому пункті?

1 Дуже низька

2 Низька

3 Середня

4 Висока

5 Дуже висока

**Додаток З**

**Пам’ятка для вчителів щодо забезпечення інформаційної безпеки у початковій школі**

Дотримуйтеся цих правил самі й розкажіть учням:

1. **Переконайтеся, що всі пристрої надійно захищені (паролями) і заблоковані тоді, коли ви ними не користуєтесь.** Якщо вам потрібно вийти з класу, заблокуйте всі пристрої, які використовували, або завершіть сеанс роботи чи вийдіть з облікового запису. Встановіть на всіх пристроях ліцензійну антивірусну програму та стежте за тим, щоби вона регулярно оновлювалася.
2. **Встановіть правила в школі, де й коли можна користуватися мобільними пристроями.**А також правила, що учнів можна фотографувати лише після отримання згоди батьків / опікунів / самих учнів на це. Ці правила мають бути закріплені в шкільній політиці щодо онлайн-безпеки. Така політика має встановлювати ще й порядок реагування на інциденти, пов’язані з безпекою дітей, зокрема, у цифровому середовищі. Так, у школі може бути призначений спеціальний координатор для обліку та реєстрації порушень та інцидентів, пов’язаних з онлайн-безпекою, задля формування цілісного уявлення про наявні в школі проблеми та тенденції, що вимагають уваги.
3. **Забезпечте фільтрацію й моніторинг даних, які передаються через шкільну мережу, встановивши необхідні програми.**Допомогти їх встановити можуть інтернет-провайдери. Учні не повинні отримувати доступу до шкідливого або неприйнятного контенту через шкільну мережу. Такі системи фільтрації та контролю контенту допомагають звести до мінімуму передавання неприйнятного (наприклад, насильницького чи порнографічного) контенту в шкільній мережі. А системи фільтрації даних допомагають відстежувати, хто, що, коли й на якому пристрої завантажує. Такий механізм є одним зі способів запобігання кібербулінгу.
4. **Пам’ятайте, що ваші дії та слова в інтернеті можуть вплинути на вашу онлайн-репутацію, а також на репутацію навчального закладу.** Ви як користувач/-ка інтернету залишаєте свій цифровий слід – адже різні сайти, соціальні мережі, платформи, відповідно до своїх політик, збирають дані про вашу онлайн-активність. Перевіряйте інформацію, яку поширюєте в соціальних мережах. Перед тим як опублікувати інформацію, подумайте, хто може її побачити. Розповідайте дітям про важливість онлайн-репутації та як правильно її формувати.
5. **Слідкуйте за своєю професійною комунікацією**. Для будь-яких контактів між працівниками школи, учнями, батьками чи іншими зацікавленими сторонами завжди використовуйте шкільну електронну пошту замість особистої. У деяких випадках кодекс ділової етики, якщо він погоджений у школі, може передбачати заборону на контакти з учнями на платформах, які не мають стосунку до школи. Наприклад, у месенджерах чи соцмережах. Також рекомендується встановити в школі чіткі правила – як для працівників, так і для учнів – щодо проведення відеоконференцій чи занять у віддаленому режимі. Наприклад, правила, який вигляд має мати місце для проведення уроків, наявність фото профіля тощо.
6. **Сприяйте формуванню цифрових навичок та цифрової грамотності дітей.**Говоріть із ними про це на уроках. Намагайтеся включити до навчальних планів аспекти цифрової грамотності. Проводьте заходи в школі про онлайн-безпеку дітей. Водночас, показуйте високий рівень власної цифрової компетентності. І не забувайте проводити регулярну перевірку всіх заходів у школі на дотримання онлайн-безпеки дітей та її можливого удосконалення.
7. **Навчайтеся нового та постійно покращуйте навички цифрової грамотності**. Будьте в курсі того, які ризики на дітей можуть чекати в інтернеті, як діти проводять свій час у мережах. Це допоможе вам краще зрозуміти дітей та встановити з ними довірливі взаємини швидше й легше.

Пам’ятайте, що **інтернет – одночасно й ризик, і можливість для дітей**. Тому освітянам варто робити все можливе, щоби зробити цифрове освітнє середовище максимально безпечним для дітей.

