Національний університет «Чернігівський колегіум» імені Т.Г.Шевченка
Природничо-математичний факультет
Кафедра інформатики і обчислювальної техніки

Кваліфікаційна робота
освітнього ступеня «магістр»

на тему:

ФОРМУВАННЯ ОСНОВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА УРОКАХ ІНФОРМАТИКИ

Виконав:
студент 6 курсу, 63-фмт групи
спеціальності
014.09 Середня освіта (Інформатика)
Юк Андрій Валентинович

Науковий керівник:
к.п.н., доц. Вінниченко Є. Ф.

Чернігів – 2024

ЗМІСТ

ВСТУП

В сучасному світі інформація є одним із найцінніших ресурсів, а її безпека стає ключовим фактором у забезпеченні стабільного функціонування суспільства, економіки та держави. Сучасне суспільство визначається стрімким розвитком інформаційних технологій та глобалізацією цифрового простору, а використання цифрових технологій поширюється у всіх сферах життя, що вимагає від користувачів базових знань і навичок щодо захисту особистих даних, конфіденційності та кібербезпеки.

Особливу роль у цьому процесі відіграє освітня система, зокрема шкільна інформатика, яка є базовою дисципліною для формування інформаційної грамотності у молодого покоління. Саме на уроках інформатики школярі отримують первинні знання про роботу з інформацією та її безпеку. Впровадження основ інформаційної безпеки у навчальні програми є необхідним кроком для підготовки учнів до викликів, пов'язаних з кіберзагрозами та неправомірним використанням інформації.

Крім того, зростання кількості кіберзлочинів, фішингових атак, витоків даних та інших загроз інформаційній безпеці підкреслює необхідність формування відповідних навичок з раннього віку. У зв'язку з цим важливо розробити методичні підходи та ефективні освітні стратегії, які дозволять учням засвоїти принципи інформаційної безпеки не тільки теоретично, але й практично. Цим обумовлюється актуальність даної роботи.

Дослідження в рамках цієї магістерської роботи спрямоване на вивчення методики формування основ інформаційної безпеки на уроках інформатики. Це дозволить сприяти підвищенню рівня цифрової грамотності учнів, формуванню їхньої відповідальності за безпеку інформації та забезпеченню кращої підготовки до використання сучасних технологій у повсякденному житті.

Мета роботи полягає в розробці та обґрунтуванні методичних підходів до формування основ інформаційної безпеки на уроках інформатики в школі.

Завданнями магістерської роботи є:

- визначити поняття та сутність інформаційної безпеки;
- охарактеризувати інформаційну безпеку в освітньому процесі;
- дослідити український та міжнародний досвід навчання основ інформаційної безпеки;
- визначити ключові компетентності та зробити аналіз існуючих методик навчання інформаційній безпеці;
- зробити добір ефективних методик для навчання інформаційній безпеці.

Об'єктом дослідження є методика навчання інформатики в школі.

Предметом дослідження є методи та прийоми формування основ інформаційної безпеки на уроках інформатики.

У магістерській роботі використовувалися такі ***методи дослідження***: теоретичний аналіз наукової літератури з питань інформаційної безпеки та методики її навчання, порівняльний аналіз існуючих педагогічних підходів до навчання основам інформаційної безпеки, добір методичних рекомендацій для навчання інформаційній безпеці на уроках інформатики.

Структура кваліфікаційної роботи. Робота складається зі вступу, 2-ох розділів, висновків до кожного розділу, загальних висновків, списку використаних джерел. Загальний обсяг роботи 62 сторінки. Список використаних джерел містить 60 посилань.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОСВІТІ

1.1 Поняття та сутність інформаційної безпеки

Інформаційна безпека є однією з ключових тем сучасних наукових досліджень, з огляду на значущість інформації як стратегічного ресурсу в цифрову епоху. У науковому розумінні інформаційна безпека охоплює не лише технічні аспекти захисту даних, але й комплексну взаємодію між інформаційними технологіями, суспільством, політикою та правом. Наукові підходи до інформаційної безпеки фокусуються на вивченні загроз, створенні моделей ризиків, розробці методологій захисту, а також на вивченні впливу інформаційної безпеки на соціальні процеси та економічні системи. Поняття інформаційної безпеки є багатоаспектним, воно інтегрує технічні, соціальні, психологічні, політичні та правові виміри, що робить його вкрай важливим об'єктом дослідження в різних наукових дисциплінах.

Інформаційна безпека зазвичай розглядається як захист інформації від несанкціонованого доступу, розголошення, змін або знищення [1]. Згідно з Національною доктриною інформаційної безпеки України, інформаційна безпека визначається як стан захищеності ключових інтересів людини, суспільства і держави, при якому уникається завдання шкоди через неповноту, несвоєчасність або недостовірність інформації, порушення цілісності та доступності даних, несанкціонований доступ до інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив і умисне створення негативних наслідків використання інформаційних технологій [2; 3].

Наукові визначення інформаційної безпеки суттєво відрізняються від побутових та практичних підходів до цього питання. Вона розглядається як динамічна, багатоаспектна категорія, що охоплює захист інформаційних ресурсів, забезпечення конфіденційності, цілісності, доступності, автентичності

та невідмовності даних. У наукових працях інформаційна безпека часто трактується через призму захисту даних від потенційних загроз та загрозливих чинників, які можуть вплинути на надійність та ефективність інформаційних систем. Науковці вивчають не лише захист інформаційних систем, але й методи управління ризиками, спрямовані на мінімізацію впливу потенційних загроз.

Загальнонаукове визначення інформаційної безпеки включає в себе не тільки технічні заходи, такі як шифрування та автентифікація, але й організаційні процеси, управління людськими ресурсами та політику кібербезпеки на рівні держави та міжнародних організацій. Однією з важливих складових наукового підходу є дослідження еволюції загроз інформаційній безпеці, які постійно змінюються та набувають нових форм через розвиток технологій.

Інформаційна безпека визначається як сукупність заходів і стратегій, спрямованих на захист інформаційних ресурсів від несанкціонованого доступу, знищення, змінення або витоку інформації. Це може включати захист інформації від фізичних загроз (таких як пошкодження обладнання), технічних загроз (наприклад, атаки зловмисного програмного забезпечення), а також від несанкціонованих дій осіб, які можуть спробувати отримати доступ до інформації без належних повноважень.

Основною метою інформаційної безпеки є забезпечення конфіденційності, цілісності та доступності інформації, які відомі як так звана тріада інформаційної безпеки. Конфіденційність означає захист інформації від доступу осіб, які не мають на це права; цілісність передбачає захист інформації від змін, які можуть порушити її правильність та повноту; доступність, своєю чергою, гарантує, що інформація буде доступною для використання у необхідний час уповноваженими користувачами.

Разом з терміном «інформаційна безпека» сьогодні часто використовують поняття «кібербезпека» (комп’ютерна безпека), яке визначає стан захищеності комп’ютерних систем і мереж [4]. Якщо комп’ютерна безпека фокусується на захисті даних, що обробляються і передаються в технічних системах, то

інформаційна безпека має на увазі захист інформації користувача, незалежно від носія, на якому вона зберігається. В Україні, що перебуває у стані гібридної війни, де інформаційні та кібернетичні атаки є одними з методів боротьби, інформаційна і кібербезпека набувають особливої актуальності. Комп'ютерні мережі є основою критично важливої інфраструктури, тому інформаційна безпека є важливою частиною національної безпеки [5].

При аналізі понять «інформаційна безпека» та «кібербезпека» важливо зрозуміти значення термінів «дані» та «інформація». Інформаційна безпека включає в себе такі людські аспекти, як довіра і ідентичність, на основі яких будуються взаємодія та комунікація. Комп'ютерна безпека, в свою чергу, спирається на процеси автентифікації та авторизації. Для розробників і користувачів інформаційних систем важливо забезпечити збереження механізмів довіри та ідентифікації. Потреба в конфіденційності з'явилася як засіб захисту особистої свободи та корпоративних прав. Основи конфіденційності закріплені в статті 12 Загальної декларації прав людини ООН, а Європейський Союз розробив детальне законодавство для захисту особистих даних. Багато користувачів не усвідомлюють, що їхні особисті дані можуть оброблятися і зберігатися не лише розробниками веб-сайтів, але й третіми особами. Масове збирання даних через соціальні мережі створює ефект «цифрової тіні» [6].

Порушення кібербезпеки несумісне із захистом особистої інформації, але кібербезпека як стан захищеності комп'ютерних систем і даних є необхідною, але недостатньою умовою для забезпечення інформаційної безпеки [7]. Основні цілі інформаційної безпеки пов'язані із забезпеченням конфіденційності, цілісності та доступності даних. Конфіденційність означає, що дані доступні лише уповноваженим особам, цілісність гарантує точність і захист даних від несанкціонованих змін, а доступність забезпечує доступ до даних та ресурсів для уповноважених користувачів у потрібний момент.

Хоча ці принципи є основоположними, спеціалісти в галузі інформаційної безпеки відзначають, що використання технічних засобів без відповідного

навчання користувачів аспектам інформаційної безпеки не приносить бажаних результатів [8]. Аналіз документів і стандартів вищої освіти показує, що питання інформаційної та кібербезпеки є критично важливими для підготовки майбутніх фахівців у сфері комп'ютерних наук як в Україні, так і за кордоном. Навчальні курси з цієї тематики включені до університетських програм у Європейському Союзі та США [9; 10]. Наприклад, у 2001 році в Техаському університеті (UTSA – University of Texas at San Antonio) був заснований Центр гарантування безпеки IT-інфраструктури (CIAS – Center for Infrastructure Assurance and Security), основним завданням якого є навчання і практична підготовка студентів до захисту інформаційних систем [11].

Українські університети також активно готують спеціалістів у галузі захисту інформаційних технологій. У 2016 році в Україні був затверджений стандарт спеціальності «125. Кібербезпека», який визначає загальні та спеціальні компетенції для бакалаврів у цій області [12]. Окрім професійної підготовки, важливим є також рівень поінформованості користувачів комп'ютерних систем. Європейське агентство мереж і інформаційної безпеки (ENISA – European Union Agency for Network and Information Security) вважає обізнаність користувачів критично важливим компонентом організаційної стратегії, визначаючи її як «першу лінію оборони» корпоративних мереж [13].

Для забезпечення належного рівня захисту інформації використовуються різноманітні методи та засоби, що об'єднуються у трьох основних компонентах інформаційної безпеки: технічний, організаційний та правовий.

1. Технічний компонент включає використання апаратних та програмних засобів для захисту інформації. Це можуть бути такі заходи, як шифрування даних, використання систем контролю доступу, захист від шкідливого програмного забезпечення, а також моніторинг і контроль за активністю в мережі. Розвиток новітніх технологій призводить до постійного вдосконалення технічних засобів забезпечення безпеки, таких як фаєрволи, системи виявлення загроз, засоби багатофакторної автентифікації тощо. Технічний підхід орієнтований на створення методів захисту інформаційних систем від

технічних загроз, таких як віруси, хакерські атаки, зломи систем та несанкціоноване проникнення. Технічні засоби захисту включають у себе розробку алгоритмів шифрування, захисних програм (фаєрволів, антивірусів), а також розгортання систем контролю доступу та захисту від DDoS-атак. У цьому контексті наукові дослідження зосереджені на оптимізації існуючих технічних рішень і пошуку нових підходів до боротьби з загрозами, які постійно еволюціонують.

2. Організаційний компонент стосується розробки та впровадження політик і процедур, спрямованих на забезпечення інформаційної безпеки. Це може включати навчання персоналу основам інформаційної безпеки, регулярний аудит безпеки, а також запровадження стандартів та методик для забезпечення захисту інформації. Важливим є контроль за дотриманням правил безпеки на всіх рівнях організації. Організаційний підхід досліджує способи побудови ефективних систем управління інформаційною безпекою на рівні компаній, установ та держав. Важливими аспектами цього підходу є розробка політик безпеки, визначення ролей і відповідальностей працівників, моніторинг діяльності та аналіз ризиків. Вчені розглядають питання про те, як найкращим чином організувати інформаційні системи з урахуванням їхньої захищеності, які методи управління ризиками можуть бути впроваджені для зниження ймовірності витоку даних або знищення інформації.

3. Правовий компонент охоплює законодавчу базу, що регулює питання захисту інформації. На рівні держав регулювання інформаційної безпеки включає закони щодо захисту персональних даних, захисту інтелектуальної власності, кібербезпеки, а також заходи щодо боротьби з кіберзлочинністю. Міжнародні стандарти також грають важливу роль у забезпеченні інформаційної безпеки, наприклад, стандарти ISO/IEC 27001, які встановлюють вимоги до системи управління інформаційною безпекою. Правовий аспект охоплює дослідження законодавчих і нормативних актів, які регулюють сферу інформаційної безпеки на міжнародному, національному та корпоративному рівнях. Важливою частиною наукових досліджень є аналіз взаємодії між

технологіями та правовими нормами, а також визначення ефективності існуючих правових механізмів захисту даних. Особливу увагу приділяють питанням міжнародної взаємодії у сфері кібербезпеки, зокрема угодам щодо обміну інформацією та боротьби з кіберзлочинністю [14].

Соціальний аспект стосується впливу інформаційної безпеки на суспільство та окремі соціальні групи. Вчені вивчають психологічні та соціальні наслідки витоків даних, способи забезпечення цифрової гігієни серед користувачів та вплив кіберзагроз на міжособистісну комунікацію. Соціальний вимір включає також аналіз етичних аспектів інформаційної безпеки, таких як приватність, свобода слова та доступ до інформації.

У технічних науках дослідження інформаційної безпеки зосереджені на розробці новітніх засобів захисту інформації та протидії загрозам. Одним із провідних напрямків є криптографія — наука про шифрування інформації, яка використовується для забезпечення конфіденційності даних. Криптографічні алгоритми розробляються для забезпечення захищеного обміну інформацією, зокрема в таких сферах, як електронна комерція, банківські операції, державне управління тощо. Важливими напрямками досліджень є також квантова криптографія, яка дозволяє створювати непорушні канали передачі інформації завдяки використанню квантової механіки.

Іншим важливим напрямком є розробка систем виявлення вторгнень (IDS, intrusion detection systems) та систем попередження вторгнень (IPS, intrusion prevention systems), які використовуються для аналізу активності в мережах і виявлення аномальних дій, що можуть свідчити про кібератаку. Науковці займаються вдосконаленням цих систем для того, щоб підвищити їх ефективність у боротьбі зі зростаючою кількістю та складністю загроз.

Одним з важливих аспектів технічних досліджень є також віртуалізація та хмарні обчислення, які відкривають нові можливості для обробки і зберігання даних, але водночас створюють нові виклики для інформаційної безпеки. Вчені вивчають питання про те, як забезпечити безпеку даних, що зберігаються у

хмарі, як запобігти витокам інформації під час передачі та як гарантувати захищеність систем віртуалізації.

Загрози інформаційній безпеці можна класифікувати на внутрішні та зовнішні. Зовнішні загрози походять від третіх осіб, зокрема хакерів, кіберзлочинців, конкурентів або навіть іноземних держав, які намагаються отримати доступ до інформаційних систем з метою викрадення, пошкодження або маніпуляції даними. Це можуть бути атаки з використанням шкідливого програмного забезпечення, таких як віруси, трояни, хробаки або програми-вимагачі, що можуть блокувати доступ до інформації до моменту виплати викупу.

Внутрішні загрози зазвичай походять від співробітників або інших осіб, що мають легальний доступ до інформаційних ресурсів організації. Ненавмисні дії, такі як неправильне налаштування систем або випадкове розголошення інформації, можуть також створювати загрози. Внутрішні атаки можуть бути навіть небезпечнішими, ніж зовнішні, оскільки внутрішні користувачі часто мають доступ до конфіденційної інформації і можуть легко обійти системи безпеки [15].

Однією з найсерйозніших загроз інформаційній безпеці є кіберзлочинність. У кіберпросторі злочини можуть включати крадіжку даних, злом інформаційних систем, розповсюдження шкідливого програмного забезпечення, атаки на вебсайти та електронні платформи, а також фішинг — спроби отримання конфіденційної інформації через шахрайські електронні листи або вебсайти.

Кіберзлочинці стають все більш витонченими у своїх методах. Вони можуть використовувати складні соціальні інженерії, щоб маніпулювати людьми до добровільного розкриття інформації. Наприклад, за допомогою підроблених листів вони можуть вдавати, що є офіційними представниками компаній або урядових установ, створюючи ситуації, в яких людина може випадково надати конфіденційну інформацію.

Кіберзлочинність може мати серйозні наслідки для економіки, оскільки витрати на боротьбу з наслідками кібератак зростають, а компанії та держави зазнають значних фінансових втрат. Крім того, атаки на критично важливу інфраструктуру, таку як енергетичні системи або медичні заклади, можуть створити серйозні загрози для національної безпеки.

Для боротьби з загрозами інформаційній безпеці використовуються різноманітні методи та технології. Найпоширеніші з них включають:

1. Шифрування даних — це процес перетворення інформації у форму, яка недоступна для несанкціонованих осіб. Шифрування використовується для захисту даних як під час їх передачі мережею, так і під час зберігання на фізичних носіях.

2. Системи автентифікації — ці системи дозволяють перевірити, чи є користувач, що намагається отримати доступ до інформаційної системи, уповноваженим на це. Зокрема, багатофакторна автентифікація (наприклад, поєднання пароля і відбитку пальця) є однією з найефективніших методів забезпечення безпеки.

3. Системи виявлення та запобігання загрозам — ці системи аналізують активність у мережі для виявлення потенційних загроз та спроб несанкціонованого доступу. Вони можуть автоматично блокувати підозрілі дії або надсилати попередження адміністратору системи.

4. Засоби резервного копіювання — регулярне створення резервних копій даних є критично важливим для забезпечення їх збереження у разі кібератак або технічних збоїв [16].

Отже, інформаційна безпека — це багатокомпонентна система захисту даних. Вона охоплює комплекс заходів для забезпечення конфіденційності, цілісності та доступності інформації в умовах зростаючих загроз. Поняття інформаційної безпеки поєднує технічні, організаційні, правові та соціальні аспекти, що взаємодіють для створення ефективних систем захисту в різних сферах суспільного життя.

1.2 Інформаційна безпека в освітньому процесі

Інформаційна безпека стає необхідним аспектом у сучасному світі, де цифрові технології інтенсивно впроваджуються у всі сфери життя, у тому числі в освітній процес. Розвиток інформаційних технологій приносить багато переваг, але водночас і нові загрози, які потребують створення ефективних стратегій інформаційної безпеки. Освітній процес стає темою підвищеної уваги з точки зору захисту інформації, оскільки діти та підлітки стають вразливими до різних кіберзагроз [17]. Тому важливо впроваджувати знання про інформаційну безпеку в навчальні програми і забезпечувати належний рівень захисту інформації на різних рівнях освітнього процесу.

Інформаційна безпека визначається як захист інформації від різних видів загроз, які можуть призвести до її ненависті, підривання або незаконного доступу. Інформаційна безпека включає в себе три головні аспекти: конфіденційність, цілісність і доступність. Конфіденційність забезпечує, що тільки довірений користувач може отримати доступ до інформації. Цілісність гарантує, що інформація не буде змінена без дозволу і незаконно. Доступність забезпечує, що інформація доступна тільки тим, хто її потребує, індивідуально та часово [18].

Інформаційна безпека в освітньому процесі стає актуальною в результаті широкого впровадження ІТ-технологій і використання Інтернету для навчання і зв’язку між учнями і вчителями. Виклики, які виникають у цьому контексті, включають ризики, пов’язані з кіберзагрозами, такі як фішинг, швидкий доступ до лише персональної інформації інтернет-школярів, машинний доступ до віртуальних класів і стандартні загрози, пов’язані з комп’ютерними вірусами і штурмовими атаками. Інтеграція ІТ-технологій у шкільний процес вимагає розробки стратегій, які правильно забезпечують захист даних і інформації [19].

Основні заходи, які можуть бути впроваджені для захисту інформації в освітньому процесі, включають розвиток інформаційної грамотності учнів і вчителів, впровадження систем антивірусного захисту, контроль доступу до

ресурсів і програмного забезпечення, регулярне оновлення приладів і платформ, а також проведення періодичних обстежень і оцінки ризиків. Важливим аспектом є навчання учнів і вчителів основам інформаційної безпеки, що включає проведення спеціальних курсів і семінарів, які допомагають зрозуміти основні загрози і методи їх подолання.

В сучасному освітньому середовищі України активно підтримуються принципи, що пропагуються Міжнародною організацією ЮНІСЕФ, зокрема ідеї захисту прав, свобод та інтересів дітей. Згідно з концепцією сучасної української освіти, навчальний заклад повинен бути простором, що сприяє всебічному розвитку, де формуються успішні, креативні та щасливі особистості [20].

Розглянемо діяльність учасників навчально-виховного процесу як користувачів інформаційно-освітнього середовища та визначимо, як ці компетенції пов'язані з їх інформаційною безпекою. Для успішного виконання професійних обов’язків вчитель інформатики повинен мати глибокі знання про функціонування комп'ютерних систем і загрози, які виникають внаслідок несанкціонованого доступу до них, а також розуміти значення інформаційної безпеки. Важливо також, щоб вчитель розвивав поведінковий і особистісно-рефлексивний аспекти, що передбачає перетворення знань у навички безпечної діяльності та аналіз власних дій.

Поведінка людини формується не тільки на основі знань, але й під впливом її світогляду, переконань, ставлень і почуттів. Ці елементи є частинами інформаційної культури, яка включає в себе процес пізнання та трансформації інформаційного середовища для реалізації особистих здібностей, потреб і прагнень. У контексті інформаційного світогляду вчителя інформатики важливо виділити здатність усвідомлювати проблеми інформаційної безпеки та кіберзлочинності, а також розуміти ризики, які супроводжують інформаційну діяльність. Аксіологічний аспект інформаційного світогляду полягає у розумінні відповідальності за наслідки дій в інформаційно-освітньому середовищі.

Невиконання правил безпеки в навчальному закладі може призвести до негативних наслідків, таких як:

– знищення або пошкодження важливих даних, що стосуються навчального процесу (документація, навчальні матеріали, засоби оцінювання);
– несанкціоноване отримання і розповсюдження персональних даних учнів, викладачів і адміністрації;
– розповсюдження шкідливого контенту серед молоді, що пропагує насильство, порнографію, окультизм;
– зростання витрат на забезпечення інформаційної безпеки;
– негативні репутаційні наслідки для навчального закладу [21].

Освітнє середовище включає взаємодію всіх учасників освітнього процесу та гостей закладу, організацію не лише уроків, а й зустрічей, лекцій, семінарів та інших заходів. Це середовище не може існувати у вакуумі від зовнішніх і внутрішніх впливів, які можуть як позитивно вплинути, так і створити загрози та ризики. Тому важливо, щоб освітнє середовище було захищеним і безпечним [20]. Безпека освітнього середовища охоплює фізичний, психологічний, інформаційний та соціальний аспекти для всіх учасників навчального процесу. В умовах глобальної цифровізації особлива увага приділяється інформаційній складовій освітнього середовища, оскільки ІКТ мають значний вплив на особистість.

Професійні компетентності педагогів, включаючи цифрові навички, є частиною професійних стандартів та стандартів підготовки. Формування цифрових компетентностей у дітей включено до стандартів освіти та реалізується в освітньому процесі [22].

Інформаційно-комунікаційні технології є одним із ключових факторів розвитку суспільства у XXI столітті. Широке і динамічне проникнення Інтернету в усі сфери життя має великий вплив як на розвиток суспільства, так і на особистість. Інтернет є віртуальним середовищем, де реалізуються та порушуються права людини.

У 2021 році Міністерство освіти України підкреслило важливість створення безпечного освітнього середовища, включаючи Інтернет, та формування навичок цифрової грамотності у дітей. Того ж року Національна академія педагогічних наук України запропонувала Концепцію виховання дітей та молоді в цифровому просторі.

Сучасні умови вимагають перенесення освітнього середовища у віртуальний простір. З одного боку, Інтернет надає величезні можливості для освіти, самовираження та розвитку компетентностей для подальшого працевлаштування. З іншого боку, використання Інтернету та цифрових пристроїв може містити загрози та негативно впливати на підлітків [23]. Це створює перед освітянами завдання – забезпечити безпеку освітнього середовища в цифровому просторі та інформаційну безпеку учнів. Необхідно переосмислити сутність цифрової освіти як соціально-педагогічного явища, оновити освітні програми, вдосконалити системи перепідготовки фахівців, реформувати державну освітню політику, підвищити академічну свободу закладів освіти, креативність та автономність здобувачів освіти, розвивати їх критичне мислення. Комітет міністрів Ради Європи також зазначає важливість навчання безпечному користуванню Інтернетом від вчителів, вихователів, батьків та опікунів [24].

З інтеграцією України в європейський освітній простір законодавство у сфері інформаційної безпеки та контроль за його дотриманням набули нового рівня. Проте існують проблеми, зокрема відсутність єдиної науково обґрунтованої теорії інформаційної безпеки та невідповідність потенціалу інформатизації освіти досягнутим результатам. Брак законодавчих та нормативно-правових документів, що регулюють моральність даних, що циркулюють в електронних мережах, ускладнює проблему виховання молоді, яка безконтрольно використовує ресурси глобальної мережі.

У сучасному суспільстві неможливо відмовитися від інформаційних технологій, але неконтрольований доступ до Інтернету може призвести до негативних наслідків, таких як кіберзалежність, зараження шкідливими

програмами при завантаженні файлів, порушення нормального розвитку особистості, неправильне формування моральних цінностей та небажані знайомства з особами з недобрими намірами [25].

Згідно з дослідженнями ризиків, яким піддаються діти та підлітки при використанні Інтернету, можна виділити чотири основні категорії ризику [26]:

1. Ризик вмісту матеріалів. Ситуації, коли дитина отримує доступ до нелегальної інформації, що шкодить її здоров'ю та розвитку.

2. Ризик небажаних контактів. Через соціальні мережі та онлайн-дискусії діти можуть завести небажані знайомства. Підлітки можуть стати жертвами маніпуляцій, пропаганди, радикалізації і навіть терористичної діяльності. Важливо також враховувати небезпечний стиль поведінки та сленг у соціальних мережах, що містить ненормативну лексику та має агресивний, асоціальний і ксенофобський характер.

3. Комерційний ризик. Нелегальне скачування контенту, ігри та реклама можуть мати негативний вплив.

4. Ризик використання персональних даних. Діти та підлітки часто надають особисту інформацію про себе та своїх близьких.

Важливо зазначити, що Інтернет наразі не належить жодній конкретній особі або організації, і не існує єдиних глобальних законів, що регулюють Мережу. Однак боротьба за кібербезпеку, зокрема за безпеку молоді в Інтернеті, є ключовим викликом часу для розвитку глобального мережевого простору, і Україна тут не є винятком.

Щоб мінімізувати негативний вплив Інтернету, заклад освіти має проводити цілеспрямовану виховну роботу з педагогічним колективом та батьками.

У закладі освіти необхідно створити пакет нормативно-правових документів на державному, регіональному та внутрішньому рівнях з питань інформаційної безпеки. Це повинні бути документи, що стосуються контентної фільтрації, обробки персональної інформації, регламентів для роботи в Інтернеті для викладачів та студентів, а також положення про профілактику

медіабезпеки, профілактичні заходи щодо інтернет-безпеки для здобувачів освіти, і правила безпечної поведінки в Інтернеті [27]. Також наказами мають бути призначені відповідальні особи за контентну фільтрацію, роботу з персональними даними та організацію роботи в Інтернеті.

Щодо технічних і технологічних заходів для забезпечення інформаційної та медіабезпеки в освітній установі, потрібно виконати такі кроки:

- встановити тільки ліцензійне програмне забезпечення;
- підключити систему контентної фільтрації;
- встановити антивірусні програми;
- налаштувати програми-фільтри і брандмауери [28].

Організаційні заходи включають:

- розробку та реалізацію правил інтернет-безпеки;
- організацію роботи студентів в Інтернеті за розкладом, з обмеженням часу та під наглядом викладачів або лаборантів;
- регулярну перевірку ефективності заходів у сфері інтернет-безпеки в освітній установі [29].

Для ефективної організації профілактичної роботи з медіабезпеки серед здобувачів освіти викладач повинен бути обізнаний з проблемами та небезпеками, що можуть виникнути при користуванні Інтернетом, та вміти надати рекомендації щодо їх вирішення. Важливо регулярно проводити моніторинг і діагностику проблем з інтернет-безпеки серед молоді [30].

З адміністративно-організаційного боку потрібно розробити внутрішні директиви, що регулюють використання комп’ютерного обладнання, обробку інформації та її носіїв. Необхідно також встановити правила для студентів, що користуються Інтернетом у комп’ютерних класах, забезпечити блокування небезпечного контенту та заборонити використання особистих медіа [31].

Фізичний аспект включає створення пропускної системи для контролю доступу до приміщень з інформаційними носіями навчального закладу. Лише авторизовані користувачі повинні мати доступ до ресурсів, а використання

інформації має бути обмежене відповідно до їхніх прав. Паролі необхідно регулярно змінювати, щоб зменшити ризик несанкціонованого доступу [32].

Технічний аспект передбачає використання спеціалізованого програмного забезпечення для виявлення потенційних загроз і протидії їм. В умовах обмеженого фінансування багато навчальних закладів використовують лише антивірусні програми та безкоштовні інструменти для захисту інформаційних систем. Важливо встановити фільтри для обмеження доступу студентів до певних інтернет-ресурсів та контролювати доступ до електронної пошти. Також слід заборонити копіювання певних видів інформації з комп'ютерів у навчальних закладах [33].

Ефективна стратегія інформаційної безпеки передбачає комплексний підхід до захисту даних, де важливу роль відіграють відповідальні особи, які реалізують заходи з охорони інформації. Окрім закладів освіти, виховні функції у сфері інформаційної грамотності та безпеки мають виконувати батьки [34].

Вчителі виконують ключову роль у формуванні навичок інформаційної безпеки у школярів. Вони повинні не лише викладати теорію інформаційної безпеки, але й практично використовувати знання на практичних заняттях, допомагаючи учням набути навичок захисту власних даних і запобігання кіберзагрозам. Вчителю треба пройти спеціалізоване навчання і підвищення кваліфікації для ефективного викладання тем, пов'язаних з інформаційною безпекою, і дотримуватись актуальних тенденцій в сфері інформаційної безпеки.

Інформаційна грамотність є ключовим фактором у формуванні ефективної інформаційної безпеки. Вона включає вміння знайти інформацію, оцінити її надійність і захистити свої дані від ненависті. Учні мають навчитися користуватися сильними паролями, обережно ставитися до своїх персональних даних і розуміти ризики, пов'язані з доступом до інтернет-ресурсів [35]. Розвиток інформаційної грамотності має бути інтегрований у шкільну програму і ставитися на один рівень з іншими освітніми навичками.

Впровадження основ інформаційної безпеки в навчальні програми становить необхідний крок для забезпечення підготовки учнів до сучасних інформаційних викликів. Це включає розробку інтерактивних уроків і модулів, які практично включають теми інформаційної безпеки. Необхідно створити практичні завдання і ситуації, які допомагають учням розвивати навички захисту інформації в реальних умовах. Курси і спеціальні програми, які зосереджені на тематиці інформаційної безпеки, мають бути впроваджені на різних рівнях освітнього процесу.

Освітній процес продовжує змінюватися відповідно до швидкого розвитку ІТ-технологій і кіберзагроз. Перспективи розвитку інформаційної безпеки в освітньому процесі включають впровадження інноваційних методик і інструментів, які забезпечують новий рівень захисту інформації і підвищення грамотності учнів [36]. Використання нових технологій, які оптимізують процес навчання і захисту даних, може призвести до покращення ситуації із захистом інформації в освітніх установах. Важливо одночасно розвивати нові технології і забезпечувати їх відповідне застосування в освітній діяльності.

Інформаційну безпеку комп’ютерних мереж можна розглядати через три основні аспекти: фізичний, технічний та адміністративний. Фізичний аспект включає заходи, спрямовані на обмеження доступу сторонніх осіб до приміщень, де зберігаються комп’ютери, сервери та комутаційне обладнання. Технічний аспект передбачає застосування різних пристроїв і програмних засобів для захисту операційних систем і мереж від загроз. Адміністративний аспект охоплює встановлення керівних принципів і правил для організації навчального процесу із використанням інформаційних технологій.

Якщо розглянути походження загроз, їх можна класифікувати на внутрішні та зовнішні. Внутрішні загрози пов'язані з інформаційною безпекою і виникають через несистематичні порушення безпеки, які зумовлені діяльністю некомпетентних або недоброчесних користувачів. Зовнішні загрози, навпаки, стосуються кібербезпеки і можуть бути спричинені вірусами, хакерськими атаками, шахрайськими маніпуляціями, розсилкою спаму тощо. У випадку

зовнішніх загроз виникає питання про відповідальних за технічний супровід інформаційно-освітніх середовищ навчальних закладів. Університети та коледжі часто мають спеціально створені підрозділи (центри обслуговування комп’ютерних мереж, відділи дистанційного навчання) для виконання цих завдань. Проте в загальноосвітніх школах ця проблема часто залишається невирішеною, оскільки завдання технічного супроводу комп'ютерних мереж часто виходять за межі посадових обов'язків вчителів інформатики. Нестача фінансування в загальній освіті призводить до відсутності фахівців з відповідною кваліфікацією або до недостатньої кваліфікації існуючих спеціалістів. В таких умовах можливим рішенням є використання аутсорсингової моделі, яка потребує науково-методичного і технічного обґрунтування, а також централізованої координації і контролю з боку державних органів.

Впровадження хмарних технологій у сфері освіти підтверджує доцільність аутсорсингової моделі. Хмарні технології перетворюють інформаційно-освітнє середовище навчального закладу в хмаро-орієнтоване. Незважаючи на переваги, такі як універсальний доступ, гнучкість налаштувань і економія ресурсів, хмарні технології також вносять нові ризики. Специфіка функціонування хмаро-орієнтованого середовища не завжди відображена в діючих керівних положеннях і правилах інформаційної безпеки. Наприклад, наявність універсального доступу до обчислювальних ресурсів корпоративної мережі може здійснюватися через відкриті загальнодоступні мережі та персональні пристрої, що підвищує ризики безпеки. Враховуючи значущість інформаційної та кібернетичної безпеки в освіті, необхідно зосередити увагу на формуванні професійних компетенцій як майбутніх, так і практикуючих вчителів інформатики[37].

Інформаційна безпека в освітньому процесі є важливою складовою захисту інформації і забезпечення надійності цифрових ресурсів. Освітній процес повинен забезпечувати високий рівень інформаційної грамотності, інтегрувати ефективні методи інформаційної безпеки і розвивати навички

захисту даних. Вчителі мають виконувати ключову роль у цьому процесі, забезпечуючи ефективне навчання і формування в учнів інформаційної безпеки. Перспективи розвитку інформаційної безпеки в освітньому процесі залежать від впровадження нових технологій і підходів, які підвищують рівень захисту інформації на високий рівень.

1.3 Міжнародний досвід навчання інформаційній безпеці

У зв’язку з бурхливим розвитком інформаційних технологій та постійним зростанням кіберзагроз, питання забезпечення безпеки інформаційних систем та даних набуває все більшого значення. Відповідно, навчання інформаційній безпеці стає критично важливим як для підготовки фахівців у цій галузі, так і для забезпечення загальної кіберзахищеності суспільства. Міжнародний контекст навчання інформаційній безпеці відзначається різноманітними підходами та стратегіями, що мають значний вплив на розвиток цієї сфери в глобальному масштабі.

Один з ключових аспектів міжнародного контексту навчання інформаційній безпеці – це вплив міжнародних стандартів та норм, які формують основи для навчання та практики в цій сфері. Міжнародні організації, такі як Міжнародна організація зі стандартизації (ISO), Міжнародний союз електрозв'язку (ITU) та Європейське агентство з кібербезпеки (ENISA), відіграють важливу роль у встановленні стандартів і рекомендацій для інформаційної безпеки [38].

ISO, наприклад, розробила стандарт ISO/IEC 27001, який є основою для створення, впровадження, підтримки та вдосконалення системи управління інформаційною безпекою (ISMS). Цей стандарт забезпечує універсальні вимоги до управління безпекою інформації і широко використовується в навчальних програмах для підготовки фахівців з інформаційної безпеки. Інші стандарти, такі як ISO/IEC 27002, надають рекомендації щодо реалізації заходів безпеки на основі найкращих практик.

ITU, у свою чергу, зосереджується на розробці міжнародних норм і стандартів для телекомунікацій та інформаційних технологій, що також впливають на навчання інформаційній безпеці. Їхні документи, такі як ITU-T X.1205, що стосується управління ризиками інформаційної безпеки, є важливими ресурсами для освітніх програм у цій сфері.

Національні стратегії інформаційної безпеки різних країн часто відображають місцеві потреби та виклики в галузі кіберзахисту, а також інтегрують міжнародні стандарти і практики. Важливо розглянути, як різні країни адаптують ці стандарти до своїх специфічних умов і вимог.

В Сполучених Штатах Америки питання інформаційної безпеки є надзвичайно актуальним, і країна має добре розвинену систему освіти в цій сфері. Університети та коледжі США, такі як Массачусетський технологічний інститут (MIT), Стенфордський університет та університети Каліфорнії, пропонують спеціалізовані програми з інформаційної безпеки. Ці програми охоплюють широкий спектр тем, від основ криптографії до передових методів захисту інформації. Федеральна агенція з кібербезпеки та інфраструктурної безпеки (CISA) також надає ресурси та рекомендації для навчання і сертифікації фахівців [39].

У країнах Європейського Союзу навчання інформаційній безпеці часто інтегрується в загальні рамки кібербезпеки, що визначаються директивами та регламентами Європейського Союзу. Наприклад, Директива NIS (Директива про безпеку мереж і інформаційних систем) є важливим документом, що впливає на політику в сфері кіберзахисту. Університети, такі як Університет Оксфорда та Університет Лондона, пропонують програми, що відповідають європейським стандартам [40].

У країнах Азії, таких як Китай, Японія та Південна Корея, спостерігається швидкий розвиток в області інформаційної безпеки. В Китаї, наприклад, вища освіта в цій сфері активно підтримується урядовими ініціативами, а також великими технологічними компаніями. Японія та Південна Корея також мають розвинуті програми освіти в сфері кібербезпеки, що враховують специфічні місцеві потреби і виклики [41].

Методи та підходи до навчання інформаційній безпеці можуть сильно варіюватися в залежності від країни і конкретного навчального закладу. В цілому, існують кілька ключових напрямків, які використовуються в міжнародній практиці.

Традиційні методи навчання включають лекції, семінари та лабораторні заняття. Ці методи надають студентам базові знання про теоретичні аспекти інформаційної безпеки, такі як криптографія, управління доступом та безпека мереж. Вони також включають практичні навички, такі як використання спеціалізованих інструментів для аналізу і захисту інформації [42].

Інтерактивні методи навчання стають все більш популярними. До них відносяться симуляції, кейс-стаді, та участь у кіберзмаганнях. Симуляції дозволяють студентам практично застосовувати знання у реальних сценаріях, що допомагає краще розуміти складні аспекти кіберзахисту. Кейс-стаді дають можливість аналізувати реальні інциденти та розробляти стратегії їх вирішення.

Використання нових технологій у навчальному процесі також є важливим аспектом. Віртуальні лабораторії, онлайн-курси та платформи для спільної роботи допомагають студентам отримувати практичний досвід без необхідності фізичної присутності в лабораторіях. Такі ресурси, як онлайн-курси від провідних університетів та платформ, таких як Coursera або edX, дозволяють студентам з усього світу отримувати освіту в області інформаційної безпеки [43].

Порівняння підходів до навчання інформаційній безпеці в різних країнах дозволяє виявити як загальні тенденції, так і специфічні відмінності. Наприклад, в США велика увага приділяється практичним навичкам і сертифікаціям, таким як CISSP (Certified Information Systems Security Professional) та CEH (Certified Ethical Hacker). В Європейському Союзі акцент робиться на інтеграцію навчання в загальні рамки кібербезпеки, що регулюються директивами і регламентами.

В Азії, зокрема в Китаї, навчання інформаційній безпеці часто спирається на державні ініціативи і компанії, що спеціалізуються на технологіях. Японія та Південна Корея використовують як традиційні, так і інноваційні методи навчання, зокрема акцентуючи увагу на інтеграції з новими технологіями.

Навчання інформаційній безпеці в зарубіжних країнах є важливим аспектом освіти, що допомагає підготувати висококваліфікованих фахівців у

сфері захисту інформаційних систем і даних. Підходи до навчання інформаційної безпеки варіюються в залежності від національних і регіональних особливостей, а також від потреб ринку праці. Розглянемо детально досвід навчання інформаційній безпеці в кількох ключових зарубіжних країнах.

Сполучені Штати Америки є одним з провідних центрів в освіті в галузі інформаційної безпеки. Американські університети, такі як Массачусетський технологічний інститут (MIT), Стенфордський університет і Каліфорнійський університет у Берклі, пропонують передові програми та курси з інформаційної безпеки, що включають як теоретичні, так і практичні аспекти [44].

Програми в США часто інтегрують новітні технології і методики навчання, такі як симуляції кіберзагроз, участь у реальних кейс-стадіях та кіберзмаганнях. Наприклад, програми з кібербезпеки в MIT включають проекти, де студенти працюють над реальними завданнями з кіберзахисту для великих компаній. Крім того, в США широко використовуються сертифікаційні програми, такі як CISSP (Certified Information Systems Security Professional) і CEH (Certified Ethical Hacker), які додають практичний досвід до академічної підготовки.

Урядові ініціативи, такі як Національна стратегія кібербезпеки і Центр кіберзахисту і інфраструктурної безпеки (CISA), підтримують розвиток освіти в галузі інформаційної безпеки. CISA надає ресурси і рекомендації для навчальних закладів, а також організовує тренінги і сертифікаційні програми для професіоналів.

В Європейському Союзі навчання інформаційній безпеці регулюється як на національному, так і на європейському рівнях. Директиви ЄС, такі як Директива NIS (Network and Information Systems Directive), задають загальні принципи і стандарти для забезпечення кібербезпеки, які відображаються в навчальних програмах.

Європейські університети, такі як Університет Оксфорда, Університет Лондона і Технічний університет Мюнхена, пропонують курси та програми, що

відповідають європейським стандартам і вимогам. Програми часто зосереджені на інтеграції теоретичних знань з практичними навичками, такими як розробка і тестування систем захисту, а також на управлінні кіберзагрозами.

У ЄС також існує ініціатива з розробки і впровадження курикулумів з інформаційної безпеки, що підтримується Європейським агентством з кібербезпеки (ENISA). ENISA розробляє рекомендації для навчальних закладів і організовує програми підвищення кваліфікації для фахівців у галузі кібербезпеки.

В Китаї освіта в галузі інформаційної безпеки активно підтримується державою і великими технологічними компаніями. Ключові університети, такі як Пекінський університет і Університет Цінхуа, пропонують спеціалізовані програми з інформаційної безпеки, які охоплюють широкий спектр тем, від криптографії до управління кіберзагрозами.

Китайська урядова ініціатива, така як «Національний план розвитку інформаційної безпеки», визначає стратегічні пріоритети для розвитку освіти в цій сфері. Програми навчання часто включають елементи державної безпеки і технологічної інновації, що відображаються в практичних заняттях і дослідницьких проектах.

Важливим аспектом є також співпраця між університетами і промисловістю, що дозволяє студентам отримувати практичний досвід через стажування і проекти з реальними компаніями. Це допомагає забезпечити відповідність навчання сучасним потребам ринку.

Японія і Південна Корея є прикладами країн, де навчання інформаційній безпеці активно інтегрує нові технології та інноваційні методики. В Японії, університети, такі як Токійський університет і Осацький університет, пропонують програми, що охоплюють як традиційні аспекти безпеки, так і новітні технології [43].

У Південній Кореї, навчальні заклади, такі як Сеульський національний університет і Корейський університет, активно впроваджують інноваційні методи навчання. Вони зосереджуються на інтеграції нових технологій у

навчальний процес і використовують симуляції та реальні кейси для практичної підготовки студентів.

Обидві країни також акцентують увагу на міжнародній співпраці та обміні досвідом, що допомагає інтегрувати глобальні найкращі практики в національні навчальні програми.

Аналіз наукових і педагогічних досліджень компетентнісного підходу дозволяє визначити основні складові професійних компетенцій вчителя інформатики: мотиваційно-ціннісний, організаційно-змістовний, когнітивно-операційний та особистісно-рефлексивний компоненти.

Міжнародний досвід навчання інформаційній безпеці показує різноманітність підходів і методик, що використовуються в різних країнах. В США акцент робиться на практичних навичках і сертифікаційних програмах, в Європі – на інтеграції з європейськими стандартами та регламентами, а в Китаї та Азії – на державній підтримці та технологічному прогресі. Японія і Південна Корея виділяються своїм інноваційним підходом та інтеграцією нових технологій.

Аналіз цих підходів може надати корисні інсайти для вдосконалення навчання тем, пов’язаних з інформаційною безпекою, в Україні. Інтеграція міжнародних стандартів, впровадження інноваційних методів навчання та підтримка з боку держави і промисловості є ключовими факторами успіху в підготовці фахівців у цій критично важливій сфері.

Висновки до першого розділу

Наукове розуміння інформаційної безпеки зосереджене на динаміці загроз і розробці новітніх засобів захисту. Кіберзагрози постійно еволюціонують, тому науковці акцентують увагу на розробці нових технологій захисту даних, таких як криптографія, системи виявлення вторгнень та методи захисту в умовах хмарних обчислень і віртуалізації.

Інформаційна безпека в освітньому процесі є критично важливим аспектом, який потребує комплексного підходу для забезпечення захисту даних та безпеки користувачів у цифровому середовищі. В умовах глобалізації та стрімкого розвитку інформаційних технологій освітні установи повинні адаптуватися до нових викликів, пов’язаних з кіберзагрозами та потенційними ризиками в Інтернеті. Важливо, щоб кожен навчальний заклад мав чітко визначену стратегію, яка включає розробку внутрішніх нормативно-правових документів, які регулюють використання комп'ютерного обладнання та обробку персональних даних. Це включає встановлення правил для користування Інтернетом, забезпечення контентної фільтрації, впровадження антивірусного програмного забезпечення та системи контролю доступу. Наявність таких заходів дозволяє мінімізувати ризики, пов’язані з кіберзалежністю, небажаними контактами, порушенням приватності та іншими загрозами. Комплексний підхід до інформаційної безпеки має забезпечувати не лише технічний захист, але й організаційні та адміністративні заходи, що сприяють безпечному використанню цифрових ресурсів у навчальному процесі.

Міжнародний досвід навчання інформаційній безпеці демонструє різноманітність підходів і методів, які сприяють формуванню ефективних програм навчання в цій критично важливій галузі. Різні країни адаптують освітні моделі відповідно до своїх потреб та ресурсів, що дозволяє розвивати інноваційні підходи до навчання та забезпечення інформаційної безпеки. Наприклад, в США та Європейському Союзі значна увага приділяється інтеграції інформаційної безпеки у загальноосвітні та професійні програми, де

акцент робиться на практичні навички та реальні сценарії кіберзагроз. Система освіти в Китаї та Індії, в свою чергу, активно інтегрує інформаційну безпеку у навчальні плани, орієнтуючись на швидке впровадження новітніх технологій та адаптацію до швидко змінюваного цифрового середовища. Міжнародний досвід свідчить про важливість постійного оновлення навчальних програм та ресурсів, врахування місцевих контекстів та тенденцій у сфері кібербезпеки, що дозволяє ефективно підготувати майбутніх фахівців для боротьби з сучасними кіберзагрозами.

РОЗДІЛ 2. МЕТОДИЧНІ ПІДХОДИ ДО ФОРМУВАННЯ ОСНОВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Визначення ключових компетентностей

У сучасному освітньому середовищі термін «ключові компетентності» набув великого значення. Він позначає набір знань, умінь і навичок, які є необхідними для успішного навчання та особистого розвитку учнів. Визначення ключових компетентностей є важливим для формування освітніх стандартів, які дозволяють забезпечити всебічний розвиток учнів, підготовку їх до життя в швидко змінюваному світі та сприяють підвищенню якості освіти [45]. Цей процес є складним і багатогранним, оскільки включає не тільки розробку теоретичних моделей, але й практичну реалізацію в навчальному процесі[46].

Поняття компетентності охоплює не лише когнітивні та технологічні аспекти, але також мотиваційні, етичні, соціальні та поведінкові складові, а також систему ціннісних орієнтацій і звичок [23]. В колективних монографіях [24] серед стандартів інформаційно-комунікаційних компетентностей для педагогів і учнів виділено окремий аспект – «безпека та приватність». Цей аспект включає п’ять ключових складників:

1. Знання про загрози – користувач усвідомлює, що інформація, розміщена в Інтернеті, може бути доступна стороннім особам; розуміє ризики, пов’язані з електронною поштою, завантаженням програм та прийняттям запрошень у соціальних мережах.

2. Уміння запобігти небезпекам в Інтернеті – користувач адекватно реагує на залякування, агресію і насильство, які можуть виникнути у небезпечних інтернет-взаєминах; створює надійні паролі та вміє класифікувати листи як спам.

3. Контроль за інформацією – забезпечення конфіденційності особистих паролів, критичне оцінювання достовірності інформації з мережі, усвідомлення

загроз від публікації особистих відомостей, розрізнення публічної і приватної інформації, а також розпізнавання небезпечних мережних контактів.

4. Розуміння різниці між комунікацією в мережі та спілкуванням в реальному житті.

5. Виконання гігієнічних норм, пов’язаних із використанням комп’ютера [36].

Ключові компетентності - це сукупність знань, умінь, навичок і особистісних якостей, які необхідні для успішного функціонування в сучасному суспільстві і професійній діяльності. Вони включають не лише професійні навички, але і загальні знання, соціальні навички і особистісні якості, що дозволяють особі адаптуватися до змін, вирішувати складні завдання і ефективно взаємодіяти з іншими людьми.

Компетентність можна розглядати як комплекс особистісних якостей учня, що включає ціннісні орієнтації, знання, вміння, навички та здібності, які формуються внаслідок його діяльності в певних соціально важливих і особистісно значущих сферах. Ключові компетентності ж є найбільш універсальними і застосовними в різних ситуаціях. Вони формуються у процесі вивчення кожного навчального предмета і є надпредметними, тобто такими, що виходять за межі окремих дисциплін [47].

Освітня компетентність - це вимога до освітньої підготовки, яка визначається сукупністю взаємопов'язаних орієнтацій, знань, умінь, навичок і досвіду, потрібних для продуктивної діяльності учня в певних реальних умовах. Вона дозволяє учневі здійснювати особистісно і соціально значущу діяльність [48].

Компетентності для учня формують уявлення про його майбутнє і служать орієнтирами для навчання. Проте, у процесі навчання формуються частини цих «дорослих» компетентностей, що дозволяє учневі не тільки готуватися до майбутнього, але й активно функціонувати в теперішньому. Освітні компетентності стосуються лише тих видів діяльності, які охоплені загальноосвітніми предметами і областями. Вони відображають предметно-

діяльнісний аспект загальної освіти і сприяють досягненню її комплексних цілей.

Наприклад, учень може формувати громадянську компетентність в школі, але повністю реалізувати її аспекти зможе лише після закінчення навчання. Тому під час навчання ця компетентність розглядається як освітня.

Ключові компетентності за європейською моделлю включають:

- вміння отримувати користь з особистого досвіду;
- організація і впорядкування знань;
- розробка власних методів навчання;
- здатність вирішувати проблеми;
- самостійне управління власним навчанням [49].

Компетентнісний підхід може стати особливо продуктивним для розробки сучасних систем технологічної підготовки школярів. Суть цього підходу в пріоритеті поза предметних, особистісно значущих знань і вмінь над предметними знаннями, а досвід показав, що найбільш соціально адаптованими виявилися люди, що володіють не сумою академічних знань, а сукупністю особистісних якостей: ініціативності, підприємливості, творчого підходу до справи, вміння приймати самостійні рішення.

Ключові компетентності можна розглядати як основу для розвитку сучасних учнів. Вони охоплюють не лише академічні знання, але й широкий спектр особистих і соціальних навичок. У Європейському Союзі, наприклад, визначено вісім ключових компетентностей, які є важливими для всіх учнів:

1. Комунікативна компетентність. Здатність ефективно спілкуватися усно і письмово, використовувати мову та інші знакові системи для вираження своїх думок і розуміння інших.

2. Математична компетентність і основи природничих наук. Включає здатність до використання математичних засобів та знань у практичних ситуаціях, розуміння основних концепцій науки.

3. Інформаційно-комунікаційна компетентність. Вміння використовувати інформаційні та комунікаційні технології для збору, обробки і представлення інформації.

4. Соціальна і громадянська компетентність. Здатність взаємодіяти з іншими, розуміти соціальні і культурні норми, брати участь у громадському житті.

5. Особистісна компетентність. Знання про свої сильні і слабкі сторони, управління своїми емоціями та стресом, розвиток самооцінки.

6. Культурна компетентність. Розуміння і повага до різних культур, а також здатність адаптуватися до культурних різниць [50].

Ці компетентності дозволяють учням не тільки успішно справлятися з навчальними завданнями, але й ефективно функціонувати в суспільстві, бути активними і відповідальними громадянами.

Ключові компетентності є основою для сучасної освіти, орієнтованої на результат. Вони визначають не тільки рівень знань учнів, але і їх здатність до самостійного мислення, критичного аналізу та творчого підходу до вирішення проблем. Основне значення ключових компетентностей можна визначити наступним чином:

1. У сучасному світі, де швидкі технологічні та соціальні зміни є нормою, важливо, щоб учні мали навички, які допоможуть їм адаптуватися до змінюваного середовища.

2. Ключові компетентності сприяють розвитку навичок, які необхідні для успішного життя, таких як комунікація, управління часом, вирішення проблем та співпраця.

3. Зосередження на ключових компетентностях дозволяє враховувати індивідуальні потреби і здібності учнів, що сприяє більш ефективному навчанню та досягненню кращих результатів [51].

Існує кілька підходів до визначення та реалізації ключових компетентностей в освітньому процесі. Основні з них включають:

1. Компетентнісний підхід. Цей підхід орієнтований на формування у учнів конкретних компетентностей, які є важливими для їхнього майбутнього життя. Він включає інтеграцію знань, умінь і навичок у навчальний процес.

2. Міждисциплінарний підхід. Передбачає використання знань і навичок з різних предметних областей для розв'язання комплексних завдань. Це дозволяє учням застосовувати отримані знання в різних контекстах і ситуаціях.

3. Проектно-орієнтований підхід. Фокусується на розробці і реалізації проектів, які дозволяють учням працювати над реальними завданнями, що сприяє розвитку практичних навичок і креативності.

4. Інтеграція сучасних технологій. Використання інформаційно-комунікаційних технологій для підтримки навчального процесу, що дозволяє розвивати інформаційні і комунікаційні компетентності учнів [52].

Для успішного впровадження ключових компетентностей в освітній процес можуть бути корисні наступні рекомендації:

1. Розробка чіткої концепції. Важливо розробити чітку концепцію ключових компетентностей, яка б відповідала вимогам сучасного суспільства та освітніх стандартів.

2. Професійний розвиток вчителів. Забезпечення вчителів необхідними ресурсами і тренінгами для ефективного впровадження компетентнісного підходу.

3. Адаптація навчальних планів. Перегляд і адаптація навчальних планів для інтеграції ключових компетентностей в усі предметні області.

4. Розробка ефективних методів оцінювання. Створення систем оцінювання, які б адекватно відображали рівень розвитку ключових компетентностей.

5. Залучення всіх учасників навчального процесу. Підключення батьків, учнів і громади до процесу впровадження ключових компетентностей, що сприятиме їх розумінню і підтримці [53].

Визначення ключових компетентностей є важливим етапом у розвитку сучасної освіти. Вони дозволяють зосередитися на формуванні навичок, які є

критично важливими для успішного життя в сучасному світі. Хоча реалізація цих компетентностей може бути складною через різні виклики, використання сучасних підходів і рекомендацій може допомогти забезпечити ефективну інтеграцію ключових компетентностей в освітній процес. Це дозволить учням розвивати не лише академічні знання, але й навички, які допоможуть їм бути успішними і адаптивними у змінюваному світі.

Ключові компетентності можуть бути класифіковані на кілька основних категорій, що охоплюють різні аспекти діяльності та особистісного розвитку. Основні категорії включають:

Професійні компетентності відносяться до специфічних навичок і знань, необхідних для виконання конкретних професійних завдань. Це можуть бути технічні навички, знання галузі, уміння використовувати спеціалізоване обладнання або програмне забезпечення. Професійні компетентності часто розвиваються через формальну освіту і спеціалізоване навчання і є критичними для успішного виконання професійних обов’язків.

Соціальні компетентності включають в себе навички ефективної комунікації, вміння працювати в команді, здатність до співпраці і вирішення конфліктів. Вони важливі для створення продуктивних робочих відносин і успішного взаємодії з іншими людьми. Соціальні компетентності сприяють розвитку ефективних міжособистісних відносин, що є важливим аспектом для досягнення успіху в будь-якій професійній або соціальній ситуації.

Особистісні компетентності відносяться до якостей, які визначають особистісний розвиток і здатність до самоорганізації. Сюди входять самодисципліна, самоорганізація, здатність до саморегуляції, креативність і здатність до саморозвитку. Особистісні компетентності допомагають людині краще адаптуватися до змін і успішно реалізовувати свої цілі.

Когнітивні компетентності включають в себе навички критичного мислення, аналітичного мислення, здатність до проблемного вирішення та інноваційного підходу. Вони є важливими для аналізу інформації, прийняття обґрунтованих рішень і творчого підходу до вирішення складних завдань.

Визначення ключових компетентностей починається з розуміння потреб і вимог до конкретної діяльності або професії. Це може бути досягнуто через дослідження ринку праці, аналіз вимог до конкретних посад, консультації з експертами в галузі та опитування роботодавців. Важливо враховувати як загальні потреби, так і специфічні вимоги до певних професій або соціальних ролей.

Процес визначення компетентностей також включає в себе визначення критеріїв для оцінки рівня розвитку компетентностей, що може бути здійснено через розробку стандартів або моделей компетентностей. Це дозволяє створити чіткі орієнтири для оцінки рівня розвитку компетентностей і забезпечує основу для їхнього розвитку і вдосконалення.

Розвиток ключових компетентностей є важливим аспектом професійного і особистісного зростання. Це може бути досягнуто через різні методи і підходи, включаючи формальну освіту, професійне навчання, самоосвіту і практичний досвід.

Формальна освіта надає базові знання і навички, що необхідні для розвитку ключових компетентностей. Професійне навчання та спеціалізовані тренінги можуть допомогти вдосконалити ці навички і адаптувати їх до конкретних потреб професійної діяльності. Самоосвіта та саморозвиток дозволяють особі продовжувати вдосконалювати свої компетентності поза формальним навчанням, а практичний досвід забезпечує можливість застосування навичок у реальних умовах.

Оцінка і моніторинг розвитку ключових компетентностей є важливим аспектом для забезпечення їх ефективності і коректності. Це може бути здійснено через різні методи, включаючи тестування, самооцінювання, оцінювання з боку колег та наставників, а також через аналіз результатів виконання завдань і проектів.

Розробка системи оцінки і моніторингу повинна включати чіткі критерії і індикатори для визначення рівня розвитку компетентностей. Це дозволяє не

лише відстежувати прогрес, але і виявляти області, які потребують додаткової уваги і вдосконалення.

У контексті освіти, ключові компетентності є основою для розробки освітніх програм і навчальних планів. Вони допомагають визначити, які знання і навички необхідні для досягнення успіху в сучасному світі і забезпечують основу для створення навчальних матеріалів і методик. Освітні програми повинні включати як теоретичні знання, так і практичні навички, що дозволяють учням розвивати ключові компетентності і застосовувати їх у реальних ситуаціях.

Інтеграція ключових компетентностей у навчальний процес може бути досягнута через різні методи, включаючи проектне навчання, інтерактивні заняття і практичні завдання. Це дозволяє учням не лише отримувати теоретичні знання, але і застосовувати їх на практиці, що сприяє глибшому розумінню і розвитку компетентностей.

Визначення і розвиток ключових компетентностей є критично важливими для успішного функціонування в сучасному світі і професійній діяльності. Ключові компетентності включають в себе як професійні навички, так і соціальні, особистісні та когнітивні якості. Процес визначення компетентностей включає в себе аналіз потреб і вимог, а розвиток компетентностей може бути досягнуто через формальну освіту, професійне навчання, самоосвіту і практичний досвід. Оцінка і моніторинг розвитку компетентностей є важливими для забезпечення їх ефективності і вдосконалення. Інтеграція ключових компетентностей у навчальний процес дозволяє забезпечити ефективне навчання і підготовку до реальних викликів у сучасному світі.

2.2 Аналіз існуючих методик навчання інформаційній безпеці

В умовах сучасних технологій, які стрімко розвиваються, питання інформаційної безпеки стає дедалі актуальнішим. Сфера інформаційної безпеки охоплює широкий спектр тем, від захисту персональних даних до протидії

кібератакам, тому її розгляд у навчальних закладах має особливу важливість. Ефективні методики навчання інформаційній безпеці сприяють підвищенню рівня обізнаності учнів та їх здатності захищати особисту інформацію та ресурси від різних загроз. У цьому контексті існує ряд методик, які активно застосовуються для навчання інформаційній безпеці.

Традиційні методики навчання інформаційній безпеці включають лекції, семінари та теоретичні курси. Ці методики базуються на класичному підході до навчання, де інформація передається від викладача до учнів у формі лекційних матеріалів, текстів і презентацій. Основною метою таких занять є донесення до учнів та студентів фундаментальних знань про інформаційну безпеку, таких як основи криптографії, принципи захисту мереж, політики безпеки та основи правового регулювання у сфері інформаційної безпеки.

Однією з переваг традиційних методик є їх здатність охоплювати велику кількість інформації за короткий час і забезпечувати систематичний підхід до навчання. Проте, такі методики мають і свої обмеження. Вони часто не забезпечують достатньої практичної підготовки та можуть бути менш ефективними в умовах швидко змінюваних технологій. Також відсутність інтерактивних елементів може зменшити рівень зацікавленості учнів і їхню активність під час навчання.

Теоретичні питання, пов’язані з навчанням інформаційній безпеці, в школі зазвичай фокусуються на передачі основних знань про концепції безпеки інформації, включаючи захист особистих даних, правила безпечного користування Інтернетом, а також розпізнавання і реагування на потенційні кіберзагрози. У багатьох країнах основні теоретичні концепції інтегровані в навчальні програми, що дозволяє створювати систематичні основи для розуміння учнями проблем інформаційної безпеки.

1. Основи безпеки інформації. Цей напрямок включає вивчення базових понять, таких як конфіденційність, цілісність та доступність інформації. Учні знайомляться з типами загроз, такими як віруси, фішинг, шкідливе програмне

забезпечення та інші кіберзагрози. Основною метою є надання знань про те, як зберігати інформацію безпечно і як захищатися від можливих атак.

2. Права та обов'язки користувачів. Теоретичні методики також включають вивчення прав та обов'язків користувачів в Інтернеті. Учні дізнаються про юридичні аспекти, такі як авторські права, конфіденційність даних та правила поведінки в мережі. Це допомагає розвивати розуміння етичних і правових норм в сфері інформаційної безпеки [54].

Практичні питання навчання інформаційній безпеці акцентують увагу на формуванні у учнів навичок, необхідних для забезпечення безпеки в реальних умовах. Це включає навчання навичкам користування захисними інструментами, таким як антивірусне програмне забезпечення, брандмауери, а також навички створення складних паролів і налаштування конфіденційності акаунтів.

1. Інтерактивні вправи та симуляції. Для поглиблення розуміння і навичок використовуються інтерактивні вправи та симуляції реальних кіберзагроз. Це може включати в себе розігрування сценаріїв фішингових атак, ігор на виявлення небезпечних веб-сайтів або симуляції реагування на атаки. Такі методи дозволяють учням практично застосовувати отримані знання і розвивати вміння оперативно реагувати на загрози.

Інтерактивні методики навчання інформаційній безпеці стали популярними завдяки своїй здатності залучати учнів до активної участі у навчальному процесі. До таких методик відносяться практичні заняття, рольові ігри, тренінги та симуляції. Вони дозволяють учням не лише отримувати теоретичні знання, але й застосовувати їх на практиці, що підвищує їхню готовність до реальних ситуацій.

Наприклад, рольові ігри можуть використовуватися для моделювання сценаріїв кібератак, де учні отримують можливість взаємодіяти з різними аспектами інформаційної безпеки, такими як виявлення уразливостей та розробка заходів захисту. Тренінги та симуляції також дозволяють учням

навчитись реагувати на реальні загрози, що є надзвичайно важливим для формування практичних навичок.

Однією з важливих переваг інтерактивних методик є їх здатність забезпечувати більш глибоке розуміння матеріалу через практичне застосування знань. Це допомагає учням краще усвідомлювати важливість інформаційної безпеки та вдосконалювати свої навички реагування на загрози. Однак, інтерактивні методики можуть вимагати більше часу та ресурсів для підготовки, а також потребують кваліфікованих викладачів, які здатні організувати ефективні тренінги та симуляції.

2. Проектна діяльність. Учні можуть бути залучені до проектної діяльності, яка передбачає розробку власних проектів з інформаційної безпеки, наприклад, створення планів захисту даних для вигаданих або реальних ситуацій. Це дозволяє розвивати навички аналізу, критичного мислення та креативності у вирішенні проблем безпеки [55].

Проектне навчання є ще однією ефективною методикою навчання інформаційній безпеці. Ця методика передбачає, що учні працюють над конкретними проектами, що пов'язані з інформаційною безпекою, таких як розробка політик безпеки, створення захищених систем або проведення аналізу ризиків. Проектне навчання дозволяє учням застосовувати теоретичні знання на практиці, вирішуючи реальні проблеми та завдання.

Проектне навчання має ряд переваг, серед яких можливість розвитку навичок командної роботи, критичного мислення та управлінських навичок. Учні навчаються не лише технічним аспектам інформаційної безпеки, але й навичкам комунікації та організації. Однак, реалізація проектного навчання може бути складною через необхідність забезпечення ресурсів для реалізації проектів і супроводження процесу навчання.

Модульні курси і онлайнове навчання стали популярними завдяки своїй гнучкості та доступності. Ці методики дозволяють учням навчатися у зручний для них час і темпі, що є особливо корисним для тих, хто має обмежений час або бажає поєднувати навчання з іншими зобов'язаннями. Модульні курси

зазвичай містять серії уроків або тем, що дозволяють поступово засвоювати матеріал.

Онлайнове навчання також може включати інтерактивні елементи, такі як відео, форуми для обговорень і тестування. Це допомагає учням краще зрозуміти матеріал і перевірити свої знання в реальному часі. Проте, онлайнове навчання має і свої обмеження, зокрема, необхідність самодисципліни та здатності до самостійного навчання, що може бути складним для деяких учнів.

Гейміфікація, або використання ігрових елементів у навчанні, стала новою тенденцією у навчанні інформаційній безпеці. Ця методика включає використання ігор, квестів та інших ігрових механізмів для залучення учнів до навчального процесу. Гейміфікація дозволяє створити мотивацію через конкуренцію, досягнення і винагороди, що може значно підвищити зацікавленість учнів та їхню активність.

Приклади гейміфікації в навчанні інформаційній безпеці можуть включати створення ігрових сценаріїв, де учні мають вирішувати завдання, пов'язані з захистом інформації, або участь у кібератакових квестах, де вони навчаються реагувати на загрози у віртуальному середовищі. Гейміфікація має переваги у вигляді підвищення мотивації і залучення учнів, але може вимагати додаткових ресурсів для розробки ігрових сценаріїв і механізмів.

Змішане навчання, або «blended learning», поєднує елементи традиційного та онлайнового навчання. Це дозволяє учням отримувати теоретичні знання через лекції та курси, а практичні навички здобувати через інтерактивні заняття та онлайн-ресурси. Змішане навчання забезпечує гнучкість і різноманітність методів, що може допомогти учням краще засвоювати матеріал і застосовувати його на практиці.

Змішане навчання також дозволяє інтегрувати різні технології і ресурси у навчальний процес, що може підвищити його ефективність. Однак, реалізація змішаного навчання може вимагати координації між різними методами і ресурсами, а також потребує відповідної технічної підтримки.

Для формування у учнів цілісного розуміння інформаційної безпеки необхідно забезпечити їм комплексні знання про цю предметну область на зрозумілому рівні. Це включає розгляд різних аспектів інформаційної безпеки, таких як захист даних дітей, особистості, суспільства, держави та міжнародний рівень інформаційної безпеки. У контексті інформаційного суспільства, коли розвиток інформаційних і комунікаційних технологій робить засоби масової інформації важливим інститутом соціалізації, ці інститути опосередковано виконують функції традиційних соціальних структур, таких як сім'я, школа та одноліткові групи.

Учні старших класів є особливо вразливою категорією, яка активно шукає своє місце в сучасному суспільстві. Засоби масової інформації пропонують моделі розвитку, приклади поведінки та споживання, виступаючи як інформаційні фільтри, які акцентують певні контексти і приховують або зменшують значення інших. Всесвітня пандемія коронавірусу стала серйозним випробуванням для суспільства та освітніх систем. Тому важливо навчити учнів, як уникнути використання їх страхів кібершахраями, які прагнуть отримати вигоду зі страхів людства [56].

Аналіз навчальних програм з інформатики показує, що на рівні загальної середньої освіти в рамках предмета «Інформатика» основна увага зосереджена на формуванні компетенцій безпечного та розумного використання комп'ютерних програм і Інтернету, а також дотриманні норм інформаційної етики і права.

Стандарти для старшої школи щодо розкриття «принципів забезпечення інформаційної безпеки» реалізуються більш ефективно через вибірковий модуль «Інформаційна безпека». При аналізі наступності навчального матеріалу з інформаційної безпеки було виявлено значний дисбаланс у розподілі матеріалу по класах, а також недостатнє врахування важливих предметних зв'язків у послідовності викладу матеріалу.

Формування поняття «інформаційна безпека», що є ключовим елементом інформаційно-цифрової компетентності учасників освітнього процесу

відповідно до Концепції Нової української школи, може здійснюватися за допомогою навчальних матеріалів, таких як посібник «Інтернет, який ми хочемо» (The Web We Want). Для забезпечення безпеки дітей в інформаційному просторі можна застосовувати різні підходи, зокрема: забезпечення їхньої безпеки в інформаційному середовищі; формування політики протидії проявам радикалізму, расизму, ксенофобії та іншими формами екстремізму в умовах швидкого розвитку інформаційних технологій; впровадження соціально-педагогічної роботи з батьками з питань безпеки дітей в інформаційному просторі. Заняття, представлені в посібнику, можуть бути інтегровані в освітній процес на уроках інформатики та позаурочну діяльність навчального закладу [57].

У навчальному закладі рекомендовано організовувати тиждень, день або уроки, присвячені інтернет-безпеці, а також проводити позакласні заходи на цю тему. Ці заходи можна приурочити до професійних свят, таких як Міжнародний день захисту інформації, який відзначається 30 листопада. Це свято було започатковане в 1988 році після перших масових випадків зараження комп’ютерним черв'яком, названим на честь свого творця Морріса. Міжнародний день захисту інформації є визнаним міжнародним святом завдяки американській Асоціації комп'ютерного обладнання, і його мета — нагадати про необхідність захисту комп'ютерної інформації, а також привернути увагу виробників і користувачів до проблем безпеки. Іншим важливим святом є Міжнародний день безпечного Інтернету, який відзначається другого вівторка лютого з 2004 року.

Ефективним методом вивчення навчального матеріалу, зокрема питань інформаційної безпеки, є використання високих технологій у навчальних проектах. Навчальний телекомунікаційний проект передбачає спільну навчально-пізнавальну, творчу або ігрову діяльність учнів, організовану на основі комп'ютерних технологій, з чітко визначеними цілями і узгодженими методами діяльності. Наприклад, учні можуть брати участь у мережевих проектах, організованих дистанційно, або створювати власні навчальні проекти.

Проектна діяльність в школі дозволяє вирішити кілька завдань: по-перше, учні отримують навички практичного застосування теоретичних знань щодо використання комп'ютерів, комп'ютерних технологій та Інтернету, а також розгляду питань безпеки; по-друге, що є найважливішим, школярі починають бачити комп'ютер та Інтернет не лише як розвагу або джерело непотрібної інформації, але як інструмент для створення корисного і цікавого контенту для себе та інших. Цей підхід сприяє творчості учнів і допомагає їм формувати власне бачення світу [58].

Як приклад проектної діяльності можна навести вебквест. Вебквест — це інтерактивна гра на мережевому ресурсі, де учні виконують завдання, обираючи одну з ролей, запропонованих вчителем. Особливість освітніх вебквестів полягає в тому, що інформація для самостійної або групової роботи учнів розміщена на різних веб-сайтах, посилання на які надає вчитель. Результати роботи з вебквестом можуть бути представлені у вигляді веб-сторінок або веб-сайтів, опублікованих локально або в Інтернеті [59].

При організації уроків і позаурочних заходів важливо враховувати особливості сучасного молодого покоління, яке часто має «кліпове» мислення, що характеризується швидким сприйняттям інформації без глибокого її аналізу. Сучасні діти можуть не володіти навичками функціональної грамотності читання. Тому важливо навчати учнів перетворювати інформацію з одного формату в інший, наприклад, з відео або тексту в графіку, плакат або інфографіку, або навпаки — створювати текстовий опис на основі зображень. Результати таких завдань слід представляти аудиторії для обговорення та оцінки.

Рішенням проблеми формування поняття інформаційної безпеки у підростаючого покоління є розвиток культури інформаційної безпеки, підвищення кваліфікації педагогів і організація безпечного інформаційно-освітнього середовища в навчальних закладах. Проте запропоновані заходи і напрямки не є вичерпними, оскільки сучасні інформаційні виклики і загрози постійно змінюються. Необхідно донести до учнів, що розвиток інформаційних

технологій і загальна комп'ютеризація зробили турботу про інформаційну безпеку важливою не лише для фахівців в галузі інформаційних технологій, але і для кожного користувача.

Проблеми та виклики у навчанні інформаційній безпеці:

1. Недостатнє фінансування. Однією з основних проблем у навчанні інформаційній безпеці є недостатнє фінансування. Багато шкіл не мають достатньо ресурсів для впровадження сучасних навчальних програм та технологій. Це обмежує можливості навчання учнів, зокрема через відсутність доступу до сучасного обладнання та програмного забезпечення для практичних занять.

2. Нестача кваліфікованих кадрів. Нестача кваліфікованих кадрів є ще однією важливою проблемою. У багатьох країнах, особливо в регіонах з обмеженими ресурсами, немає достатньої кількості спеціалістів, які могли б ефективно викладати інформаційну безпеку. Це може вплинути на якість навчання та підготовки учнів.

3. Швидкість розвитку технологій. Швидкість розвитку технологій також представляє виклик для навчання інформаційній безпеці. Нові загрози та технології з’являються постійно, і навчальні програми часто не встигають адаптуватися до цих змін. Це означає, що учні можуть отримувати застарілі знання, які не відповідають сучасним умовам.

4. Відсутність стандартизації. Відсутність єдиних стандартів навчання інформаційній безпеці може призвести до нерівності у якості освіти в різних школах і країнах. Без чітких стандартів важко забезпечити однаковий рівень знань та навичок серед учнів.

Серед рекомендацій та шляхів подолання перерахованих викликів можна виділити наступні:

1. Впровадження єдиних стандартів. Важливо впроваджувати єдині стандарти навчання інформаційній безпеці, що дозволить забезпечити високий рівень якості навчання. Стандарти повинні охоплювати як теоретичні, так і практичні аспекти, враховуючи сучасні кіберзагрози та технології.

2. Інвестування у ресурси та кадри. Для покращення якості навчання інформаційній безпеці необхідно збільшити фінансування освітніх програм, забезпечити школи сучасним обладнанням та програмним забезпеченням. Також важливо інвестувати в підготовку і підвищення кваліфікації викладачів.

3. Адаптація до швидких змін. Навчальні програми повинні бути гнучкими і швидко адаптуватися до нових технологій та загроз. Регулярні оновлення програм і курсів дозволять забезпечити учням актуальні знання і навички.

4. Підтримка державних та приватних ініціатив. Державні та приватні ініціативи можуть відігравати важливу роль у вдосконаленні навчання інформаційній безпеці. Співпраця між урядом, освітніми установами та приватним сектором може допомогти забезпечити необхідні ресурси та підтримку для ефективного навчання [60].

Аналіз існуючих методик навчання інформаційній безпеці в школі показує, що є значний прогрес у цій сфері, але також і ряд проблем, які потребують вирішення. Інтеграція теоретичних і практичних підходів, впровадження єдиних стандартів, інвестування в ресурси та кадри, а також адаптація до швидко змінюваного цифрового середовища є критично важливими для забезпечення ефективного навчання інформаційної безпеки. Подальше вдосконалення методик навчання допоможе підготувати учнів до реальних викликів у сфері кібербезпеки і забезпечити їхню готовність до безпечного користування інформаційними технологіями.

Аналіз існуючих методик навчання інформаційній безпеці показує, що кожна з них має свої переваги та обмеження. Традиційні методики забезпечують систематичний підхід до навчання, але можуть бути менш ефективними без практичних елементів. Інтерактивні методики і проектне навчання дозволяють застосовувати теоретичні знання на практиці, що підвищує їхню ефективність. Модульні курси і онлайнове навчання забезпечують гнучкість, але потребують самодисципліни. Гейміфікація додає елементи мотивації і залучення, але може потребувати додаткових ресурсів.

Змішане навчання поєднує переваги різних методик, але може бути складним у реалізації.

Для ефективного навчання інформаційній безпеці важливо враховувати потреби та можливості учнів, а також використовувати комплексний підхід, що включає різні методики. Це дозволяє створити більш ефективне навчальне середовище, яке відповідає сучасним вимогам інформаційної безпеки і готує учнів до реальних викликів у цій сфері.

2.3 Огляд методичних рекомендацій щодо навчання інформаційній безпеці

У сучасному цифровому світі інформаційна безпека стала важливою складовою загальної освіти. Діти і підлітки все більше часу проводять в Інтернеті, що робить їх вразливими до різних кіберзагроз, таких як шахрайство, кібербулінг, віруси та інші види онлайн-атаки. Навчання інформаційній безпеці в школі має на меті не лише навчити учнів основам захисту особистої інформації, але й забезпечити їх навичками для безпечного та відповідального використання цифрових технологій. Методичні рекомендації з цього питання повинні бути орієнтовані на формування у школярів практичних знань і навичок, а також на розвиток критичного мислення та відповідального ставлення до цифрових ресурсів.

Основні цілі навчання інформаційній безпеці включають формування у учнів розуміння важливості захисту особистої інформації, ознайомлення з можливими ризиками та загрозами в Інтернеті, а також розвиток навичок безпечного використання цифрових ресурсів. Завдання навчального процесу повинні включати не тільки теоретичні знання, але й практичні навички, такі як створення надійних паролів, розпізнавання фішингових атак, захист від вірусів і шкідливих програм.

На наш погляд, найбільш ефективними методами та формами навчання при вивченні питань, пов’язаних з інформаційною безпекою могли б стати наступні:

1. Інтерактивні методи. Інтерактивні методи навчання є ефективним способом залучення учнів до активного процесу навчання. До них відносяться рольові ігри, симуляції та дискусії. Наприклад, можна організувати рольову гру, де учні беруть на себе ролі різних користувачів Інтернету і вирішують ситуації, пов’язані з інформаційною безпекою. Це допомагає їм краще зрозуміти реальні загрози та способи їх уникнення. Інтерактивні методи сприяють розвитку критичного мислення, навичок, спілкування та прийняття рішень. Серед них рольові ігри, симуляції та дискусії. Наприклад, рольова гра на тему «Соціальна інженерія» дозволяє учням виконувати ролі різних користувачів Інтернету та вирішувати завдання, пов’язані з безпекою паролів і персональних даних. Дискусія «Захист персональних даних» може включати обговорення реальних життєвих ситуацій із загрозами витоку даних. Учні аналізують проблемні ситуації, пропонують та дискутують щодо найефективніших способів уникнення загроз.

2. Проектна діяльність. Проектна діяльність дозволяє учням самостійно досліджувати питання інформаційної безпеки та створювати власні проекти. Це можуть бути дослідницькі проекти, презентації, відеоролики або інформаційні буклети. Наприклад, учні можуть створити інформативний буклет про захист особистої інформації або розробити відеоуроки з основ інформаційної безпеки. Проектна діяльність стимулює учнів до самостійного дослідження питань інформаційної безпеки та створення власних проектів. Це можуть бути дослідницькі проекти на тему «Історія кіберзлочинців», створення презентацій із правилами безпечної поведінки в Інтернеті чи відеоуроків з інструкціями для захисту акаунтів у соцмережах Учні також можуть розробити інформаційні буклети або інтерактивні плакати, які пояснюють основні загрози кіберпростору і способи їх запобігання.

3. Веб-квести та онлайн-платформи. Веб-квести є ще одним ефективним методом навчання. Це інтерактивні завдання, які виконуються на основі інформації, розміщеної на різних веб-сайтах. Учні отримують завдання, які потребують пошуку інформації в Інтернеті, аналізу та використання її для розв'язання конкретних задач. Використання онлайн-платформ для навчання може також включати в себе курси, тренінги та відеоуроки з інформаційної безпеки. Наприклад, веб-квест «Місія: Захистити дані» включає пошук способів захисту даних на різних сайтах, навчання розпізнавання фішингу та шахрайства. Додатково можна використовувати онлайн-курси з кібербезпеки, віртуальні лабораторії для моделювання загроз та симуляції реальних атак, що дозволяє отримати практичний досвід захисту інформації.

4. Позакласні заходи також відіграють важливу роль у формуванні інформаційної безпеки. Школи можуть організовувати спеціальні дні або тижні інформаційної безпеки, коли учні беруть участь у різноманітних заходах, таких як конкурси, вікторини, семінари та воркшопи. Тематичні фестивалі, інтерактивні виставки та практичні тренінги додатково підвищують зацікавленість учнів та стимулюють їх до поглибленого вивчення предмету. Це дозволяє учням закріпити отримані знання на практиці та підвищити їхню обізнаність про безпеку в Інтернеті.

5. Комбіновані уроки. Важливо інтегрувати теми інформаційної безпеки не тільки в предмет інформатики, але і в інші навчальні предмети. Наприклад, уроки з соціальних наук можуть включати елементи кібербезпеки, такі як питання етики в Інтернеті, вплив інформаційних технологій на суспільство та інші. Інтеграція допомагає учням бачити інформаційну безпеку як частину їхнього щоденного життя і навчання. На уроках інформатики можна навчати створення безпечних паролів і налаштування конфіденційності в соцмережах. На соціальних науках варто обговорювати етику поведінки в Інтернеті та цифрову культуру, а також вплив технологій на суспільство та особистість. На уроках мови та літератури можна запропонувати написати есе на тему «Як захистити свою приватність в Інтернеті» або створення оповідань з елементами

кібербезпеки, що розвиває креативність і одночасно підвищує обізнаність щодо загроз у цифровому середовищі

Оцінювання знань та навичок учнів у сфері інформаційної безпеки може здійснюватися через тести, практичні завдання, проекти та участь у позакласних заходах. Важливо використовувати різноманітні методи оцінювання, щоб отримати повну картину про рівень знань і навичок учнів. Наприклад, тести можуть включати питання на знання теоретичних аспектів безпеки, а практичні завдання – на вміння застосовувати отримані знання на практиці.

Аналіз результатів навчання допомагає оцінити ефективність обраної методики навчання. Важливо зібрати зворотний зв'язок від учнів, батьків та вчителів, щоб виявити сильні та слабкі сторони програми навчання. Це може включати опитування, інтерв’ю та аналіз результатів тестувань. На основі отриманих даних можна вносити корективи до навчальної програми і методик навчання.

Оскільки технології та загрози в Інтернеті постійно змінюються, навчальні матеріали з інформаційної безпеки повинні регулярно оновлюватися. Вчителі повинні стежити за новими тенденціями в сфері кібербезпеки та адаптувати свої методики відповідно до актуальних вимог. Це включає в себе впровадження нових тем, таких як захист від сучасних видів кіберзагроз та новітні методи забезпечення конфіденційності.

Для ефективного навчання інформаційній безпеці важливо, щоб вчителі постійно підвищували свою кваліфікацію. Це може включати участь у курсах підвищення кваліфікації, семінарах та тренінгах з інформаційної безпеки. Професійний розвиток допомагає вчителям бути в курсі останніх тенденцій та найкращих практик у сфері кібербезпеки, що сприяє покращенню якості навчання.

Методичні рекомендації з навчання інформаційній безпеці в школі повинні охоплювати як теоретичні, так і практичні аспекти цієї теми. Включення інтерактивних методів, проектної діяльності та веб-квестів у

навчальний процес дозволяє зробити уроки більш цікавими та ефективними. Інтеграція інформаційної безпеки в різні предмети та організація позакласних заходів допомагають учням краще засвоїти отримані знання. Оцінювання ефективності навчання та постійне оновлення навчальних матеріалів є ключовими факторами для забезпечення високої якості освіти в цій важливій області. Професійний розвиток вчителів також відіграє важливу роль у покращенні якості навчання інформаційній безпеці.

Висновки до другого розділу

Компетентність є динамічною сумішшю знань, способів мислення, поглядів, цінностей, навичок і особистих якостей, яка визначає здатність особи успішно здійснювати професійну та/або подальшу навчальну діяльність.

Ключові компетентності – це навички та знання, які кожна людина потребує для особистісного розвитку, активної участі в громадському житті, соціальної інтеграції та працевлаштування. Вони забезпечують особистісну реалізацію і успіх протягом усього життя

Важливість комплексного підходу до навчання інформаційній безпеці в школі стає дедалі очевиднішою. Сучасні методики потребують удосконалення, зокрема через впровадження більше практичних занять, які б забезпечували глибше розуміння учнями актуальних кіберзагроз і методів їх уникнення. Включення в навчальний процес елементів симуляції реальних ситуацій і регулярне оновлення навчальних матеріалів відповідно до нових тенденцій у сфері безпеки є необхідними кроками для підвищення ефективності навчання. Тільки через інтеграцію сучасних практик та технологій можна забезпечити високий рівень обізнаності учнів та їх здатність ефективно захищати себе в цифровому середовищі.

Успішне навчання інформаційній безпеці в школі вимагає комплексного підходу, який включає інтерактивні методи навчання, такі як рольові ігри, веб-квести та проектну діяльність. Важливо забезпечити учнів не лише теоретичними знаннями про ризики і загрози в Інтернеті, але й практичними навичками, такими як створення надійних паролів і розпізнавання фішингових атак. Інтеграція цих тем у різні предмети та проведення позакласних заходів допомагають формувати у школярів відповідальне ставлення до цифрових технологій і підвищують їхню обізнаність щодо інформаційної безпеки.

ВИСНОВКИ

Отже, відповідно до поставлених завдань на початку роботи, ми можемо зробити наступні висновки:

1. Інформаційна безпека є комплексною системою заходів, спрямованих на захист даних від загроз та забезпечення їх конфіденційності, цілісності та доступності. Це поняття охоплює як технічні засоби захисту, такі як шифрування та системи виявлення вторгнень, так і організаційні та правові аспекти, включаючи політику безпеки і правове регулювання. В сучасному світі, де інформація є критичним ресурсом, забезпечення інформаційної безпеки стає ключовим завданням як для держав, так і для бізнесу, що вимагає постійної адаптації до нових викликів та загроз у цифровому середовищі.

2. Забезпечення інформаційної безпеки в освітньому процесі є ключовим для формування безпечного і продуктивного навчального середовища в умовах цифровізації. Педагогічні працівники повинні бути ознайомлені з актуальними загрозами, що виникають у віртуальному середовищі, і мати навички для профілактики та реагування на потенційні небезпеки. Важливо проводити регулярний моніторинг і діагностику проблем інтернет-безпеки серед студентів, а також розробляти та впроваджувати внутрішні директиви та правила, які регулюють доступ до комп’ютерних систем і інформаційних ресурсів. Технічні рішення, такі як встановлення фільтрів, антивірусних програм і систем контролю доступу, є важливими складовими системи захисту. Однак, безпосередня відповідальність за інформаційну безпеку також лежить на адміністрації закладу, батьках і самих учнях. Тому, формування культури безпечного користування цифровими ресурсами та активна участь усіх сторін є необхідними для ефективного управління інформаційними ризиками та забезпечення захисту даних в освітньому процесі.

3. Аналіз українського та міжнародного досвідів у навчанні інформаційній безпеці підтверджує необхідність комплексного підходу до навчання, який поєднує теоретичні знання з практичними навичками. Успішні

практики показують, що ефективні освітні програми повинні включати інтерактивні модулі, симуляції реальних кіберзагроз і практичні завдання, що дозволяє студентам краще зрозуміти та вирішувати реальні проблеми в сфері інформаційної безпеки. Крім того, міжнародний досвід підкреслює значення міждисциплінарного підходу, що включає елементи права, етики та технологій, для всебічного розуміння інформаційної безпеки. Для досягнення високих результатів у навчанні інформаційної безпеки важливо інтегрувати ці аспекти у національні освітні системи, адаптуючи їх до специфічних умов і потреб кожної країни.

4. Аналіз існуючих методик навчання інформаційній безпеці в школі вказує на те, що сучасні програми навчання в значній мірі орієнтовані на інтеграцію базових принципів кібербезпеки в загальноосвітній процес. Вчителі використовують різноманітні методи, включаючи інтерактивні завдання, рольові ігри та проектну діяльність, щоб навчити учнів основам захисту особистої інформації, безпеки в Інтернеті та етики онлайн-комунікацій. Однак, існуючі методики часто не охоплюють всіх аспектів інформаційної безпеки і можуть бути недостатньо адаптованими до швидко змінюваних умов цифрового середовища, що знижує ефективність підготовки учнів до реальних кіберзагроз.

5. Ефективність навчання інформаційній безпеці залежить від постійного оновлення навчальних матеріалів і професійного розвитку вчителів. Оскільки технології та загрози в Інтернеті постійно змінюються, навчальні програми повинні регулярно оновлюватися для відображення нових тенденцій і методів забезпечення конфіденційності. Професійний розвиток вчителів є критично важливим для підтримки високих стандартів навчання та забезпечення якості освіти. Вчителі повинні постійно вдосконалювати свої знання та навички в сфері інформаційної безпеки, щоб ефективно навчати учнів і підготовити їх до успішної навігації в сучасному цифровому середовищі.

6. Найбільш ефективними при навчанні інформаційній безпеці можуть виступати наступні форми та методи: лекційно-практичні заняття, проектна

діяльність, метод проектів, ігрові методи, Веб-квести та онлайн-платформи, комбіновані уроки, позакласні заходи, конкурси, вікторини, Воркшопи тематичні фестивалі, інтерактивні виставки та практичні тренінги. Всі ці форми та методи підвищують зацікавленість учнів до вивчення предмету та підвищує їхню обізнаність про безпеку в Інтернеті.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. В. Ю. Биков, М. П. Шишкіна, «Хмарні технології як імператив модернізації освітньо-наукового середовища вищого навчального закладу», Теорія і практика управління соціальними системами. № 4, 2016, [Електронний ресурс]. URL: http://nbuv.gov.ua/UJRN/Tipuss_2016_4_8.

2. «Online Browsing Platform (OBP)», Iso.org, 2017. [Online]. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en.

3. «Концепція інформаційної безпеки України», Osce.org, 2017. [Електронний ресурс]. URL: http://www.osce.org/uk/fom/175056?download=true.

4. Указ Президента України Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» (2017, Лют. 25). [Електронний ресурс]. URL: http://zakon2.rada.gov.ua/laws/show/47/2017#n12.

5. В. Ковальчук, «Забезпечення інформаційної безпеки старшокласників у комп'ютерно орієнтованому навчальному середовищі», дис. канд. пед. наук., Інститут інформаційних технологій і засобів навчання НАПН України, Київ, 2013.

6. Directive (EU) 2016/680 Of The European Parliament And Of The Council.(2016, April 27)»on the protection of natural persons with regard to the processing of personal data by competent authorities. Council Framework Decision 2008/977/JHA», Eur-lex.europa.eu, [Online]. URL: http://eurlex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN.

7. D. Van Rooyand J. Bus, «Trust and privacy in the future Internet—a research perspective», Identity in the Information Society, vol. 3, no. 2, pp. 397-404, 2010.[Online]. URL: https://doi.org/10.1007/s12394- 010-0058-7.

8. J. L. Spears «Defining information security». In:5th security conference, LasVegas, Nevada, The Information Institute, Washington Dc, Usa. 2006.[Online]. URL:http://www.isy.vcu.edu/~gdhillon/Old2/secconf/pdfs/11.pdf.

9. «Subject Benchmark», Qaa.ac.uk, 2016. [Online]. URL: http://www.qaa.ac.uk/en/Publications/Documents/SBS-Computing-16.pdf. [Accessed: 11- Oct- 2017].

10. «Alabama Cyber Security Programs», Cyber Degrees, 2017. [Online]. URL: http://www.cyberdegrees.org/listings/alabama/.

11. «CIAS Home», Cias.utsa.edu, 2017. [Online]. URL: http://jic.nv.gov/uploadedFiles/jicnvgov/content/Events/P%20ICM%20NV.pdf.

12. «Стандарт вищої освіти підготовки бакалаврів спеціальності 125 Кібербезпека» [Електронний ресурс]. URL: http://mon.gov.ua/content/Новини/2016/07/07/01/125-kiberbezpeka.doc

13. ENISA, «The newusers' guide: How to raise information security awareness (EN) – ENISA», Enisa.europa.eu, 2010. [Online]. URL: https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide.

14. Ю. С. Рамський, «Професійна діяльність вчителя в епоху інформатизації освіти» [Електронний ресурс]. URL: http://enpuir.npu.edu.ua/handle/123456789/9387.

15. Д. Лайон, «Інформаційне суспільство: проблеми та ілюзії», Сучасна зарубіжна соціальна філософія, 1996. [З мережі]. URL: http://www.philsci.univ.kiev.ua/biblio/lajon.html.

16. В. Ю. Биков, «Навчальне середовище сучасних педагогічних систем. Професійна освіта: педагогіка і психологія», Вища Педагогічна Школа у Честохові, Ченстохов, с. 59–80, 2004.

17. Гуржій, А.М., Карташова, Л.А., & Сорочан, Т.М. (2021, листопад 1-8). Цифрове навчальне середовище нового покоління: екосистема для суб'єктів освітнього процесу. В Збірник праць XVI Міжнародної наукової конференції, м. Нетанія (Ізраїль) – Хмельницький, 62-67.

18. Криворот, Т, & Пригодій, М. (2022). Тренінгова підготовка педагогічних працівників до застосування цифрових інтернет-технологій у освітньому процесі. Professional Pedagogics, 1(24), 33-41.

19. Єршов, М.-О. Свобода як тренд сучасної ІТ-освіти. The Scientific Heritage, 72-4, 24-29.

20. Олексин, О.І. (2021). Безпечна поведінка підлітків в Інтернеті. Заняття 9: Права людини в Інтернеті. URL: http://surl.li/ccykd

21. Мороз Л. Методика навчання основам інформаційної безпеки у середній школі. Освітні технології та засоби навчання. 2019. Вип. 35. С. 67–72.

22. Глобова, Є., & Міна А. (2019). Цифрові права українців або Декларація цифрових прав людини. URL: https://www.businesslaw.org.ua/digital-rights-t/

23. Міністерство та Комітет цифрової трансформації України (2021). Мінцифра запрошує до громадського обговорення концепції та плану заходів з розвитку цифрових прав дітей. URL: https://thedigital.gov.ua/news/mintsifra-zaproshue-do-gromadskogoobgovorennya-kontseptsii-ta-planu-zakhodiv-z-rozvitku-tsifrovikh-prav-ditey

24. Національна академія педагогічних наук України (2021).Концепція виховання дітей та молоді в цифровому просторі. URL: https://ipv.org.ua/wpcontent/uploads/2021/08/Kontseptsiia-vykhovannia-ditey-ta-molodi-v-tsyfrovomu-prostori.pdf

25. Ю. С. Рамський, «Методична система формування інформаційної культури майбутніх вчителів математики», дис. д-ра. пед. наук., НПУ імені М. П. Драгоманова, Київ, 2013.

26. H. Takabi, J. Joshi, G-J. Ahn, «Security and Privacy Challenges in Cloud Computing Environments», IEEE Security and Privacy Magazinepp. 24-31, 8, 2011. [Online]. URL: https://www.researchgate.net/publication/224202015_Security_and_Privacy_Challenges_in_Cloud_Com puting_Environments.

27. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр. : Закон України від 9 січня 2007 р. № 537–V. URL: http://zakon.rada.gov.ua/laws/show/537- 16?find=1&text=%E1%E5%E7%E

28. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 р. «Про Стратегію національної безпеки України» : Указ Президента України від 26 травня 2015 р. № 287/2015. URL: http://zakon5.rada.gov.ua/laws/show/287/2015

29. Про Стратегію інформаційної безпеки : Указ Президента України від 28 грудня 2021 р. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

30. Спірін О., Ковальчук В. Методика забезпечення онлайн-безпеки старшокласників у навчальновиховному процесі школи. Інформаційні технології і засоби навчання. 2011. № 1 (21). URL: http://www.journal.iitta.gov.ua

31. Варивода К. Інформаційна безпека підлітків в інтернет-мережі. Молодий вчений. 2016. № 3. С. 365–368.

32. Ковальчук В. Проблеми інформаційної безпеки дітей різних вікових категорій. URL: file:///C:/Users/1/Downloads /komp_2010_8_17.pdf

33. Куницький В. Захист неповнолітніх в інформаційному просторі як об'єкт гуманітарної експертизи: український та зарубіжний досвід. Державне управління: теорія та практика. 2011. URL: http://www.academy.gov.ua/ej/ej14/txts/Kunitskiy.pdf

34. Малик Я. Інформаційна безпека України: стан та перспективи розвитку. Ефективність державного управління. 2015. Вип. 44. С. 13–20.

35. О. М. Спірін, та В. Н. Ковальчук, «Методика забезпечення он-лайн безпеки старшокласників у навчально-виховному процесі школи», Інформаційні технології і засоби навчання, №1(21), 2011 [Електронний ресурс]. URL https://journal.iitta.gov.ua/index.php/itlt/article/view/411/368.

36. В. Биков та ін., Оцінювання інформаційно-комунікаційної компетентності учнів та педагогів в умовах євроінтеграційних процесів в освіті, К, Україна: Педагогічна думка, 2017.

37. Н. П. Дементієвська, «Критичне оцінювання інтернет-ресурсів при вивченні природничих наук» [Електронний ресурс]. URL: http://lib.iitta.gov.ua/4586/1/Кіровоград_2014_Дементієвська_тези1.pdf.

38. Гончарук С. Інформаційна безпека як складова сучасного навчального процесу. Педагогіка та психологія. 2021. № 4. С. 90–94.

39. Н. В. Морзе, В. П. Вембер, О. В. Барна, та О. Г. Кузьмінська, «Інформатика-6: навчання через діяльність», Інформатика та інформаційні технології в навчальних закладах, №4 (52), 2014. [Електронний ресурс]. URL: http://elibrary.kubg.edu.ua/6323/

40. Пазюк А.В., Черних О.О. Дитина онлайн: як забезпечити безпеку і приватність (аналітичне дослідження). Київ: ВАІТЕ, 2016. 74 с.

41. Дерев'янко І. Використання новітніх технологій для навчання інформаційної безпеки. Інформатика в освіті. 2018. № 6. С. 41–47.

42. Костюк Т. Оцінка ефективності впровадження інформаційної безпеки в навчальний процес. Експериментальні дослідження в освіті. 2020. № 9. С. 55–60.

43. Іваненко Н. Основи інформаційної безпеки на уроках інформатики. Науковий вісник НПУ імені М.П. Драгоманова. 2018. № 10. С. 123–129.

44. Петренко О. Використання інтерактивних технологій для навчання основам інформаційної безпеки. Інформаційні технології і засоби навчання. 2020. № 2. С. 45–50.

45. Коваленко І. Роль цифрових інструментів у формуванні інформаційної безпеки школярів. Вісник освіти України. 2017. № 7. С. 78–83.

46. Козак В. Актуальні питання інформаційної безпеки на уроках інформатики. Наукові записки НУ «Остромадська академія». 2019. № 8. С. 110–115.

47. Сидоренко М. Інтеграція інформаційної безпеки в навчальні програми з інформатики. Технічна освіта та наука. 2018. Вип. 42. С. 55–61.

48. Бондаренко А. Методи навчання основам інформаційної безпеки у початковій школі. Дослідження в освітніх технологіях. 2017. № 6. С. 33–38.

49. Шевченко В. Розвиток інформаційної безпеки у школярів через проектну діяльність. Вісник педагогічних наук. 2020. № 9. С. 46–52.

50. Яценко О. Стратегії викладання інформаційної безпеки на уроках інформатики. Журнал педагогічної науки. 2021. № 12. С. 102–108.

51. Гриценко Н. Інформаційна безпека у контексті інформаційних технологій. Наукові записки університету. 2018. № 5. С. 21–26.

52. Васильєва Т. Впровадження інформаційної безпеки в навчальний процес. Освітні інновації. 2019. Вип. 7. С. 75–80.

53. Семенов А. Формування навичок інформаційної безпеки у учнів середньої школи. Педагогічні дослідження. 2018. № 4. С. 89–94.

54. Назаренко І. Основи інформаційної безпеки для початкових класів. Журнал сучасної освіти. 2020. № 11. С. 39–44.

55. Дяченко О. Методичні аспекти навчання інформаційної безпеки на уроках інформатики. Наука і освіта. 2019. Вип. 32. С. 66–71.

56. Лаврова О. Ефективність навчальних програм з інформаційної безпеки. Актуальні питання освіти. 2018. № 3. С. 53–59.

57. Мельник С. Розробка навчальних матеріалів з інформаційної безпеки для школярів. Науковий журнал «Педагогіка». 2021. № 8. С. 115–121.

58. Захаренко В. Психологічні аспекти навчання інформаційної безпеки. Педагогічна практика. 2019. Вип. 12. С. 77–83.

59. Петренко О. Використання інтерактивних технологій для навчання основам інформаційної безпеки. Інформаційні технології і засоби навчання. 2020. № 2. С. 45–50.

60. Коваленко І. Роль цифрових інструментів у формуванні інформаційної безпеки школярів. Вісник освіти України. 2017. № 7. С. 78–83.