

аргументувати, робити висновки. Його інтеграція в освітній процес дозволяє зробити уроки не лише пізнавальними, а й такими, що розвивають особистість, відповідно до освітньої концепції НУШ.

Список використаних джерел

1. Грабовська Т. С. Критичне мислення як ключова компетентність учня. Київ : Педагогічна думка, 2018. 234 с.
2. Пометун О. І., Пироженко Л. В. Інтерактивні технології навчання: теорія і практика. Київ : АСК, 2020. 252 с.
3. Тименко О. В. Сучасні технології розвитку критичного мислення на уроках мови. Харків : Основа, 2019. 211 с.

Владислав Мінський,

Тернопільський національний педагогічний університет
імені Володимира Гнатюка;
Науковий керівник – доктор філологічних наук,
професор Наталія Поплавська

КІБЕРБЕЗПЕКА ЯК ОСНОВА ЦИФРОВОЇ ГРАМОТНОСТІ

Розвиток інформаційного суспільства передбачає поступове впровадження цифрових технологій та сучасних інформаційних систем у всі аспекти людської діяльності, забезпечуючи ефективність, інноваційність і доступність у різних сферах нашого життя. Однак, одночасно з цими можливостями виникають нові виклики, пов'язані із загрозами для безпеки, що набувають особливого значення в епоху глобальної діджиталізації. Одним з найбільш актуальних і складних компонентів сучасної безпеки є кібербезпека, яка інтегрується у всі рівні як державних, так і приватних процесів. Кібербезпека – це цілісна система заходів, яка включає технічні рішення, соціальні механізми, стратегічні підходи та принципи для захисту громадян та суспільства від широкого спектру кіберзагроз. Основна мета цього напрямку – забезпечення конфіденційності, цілісності та стабільної доступності даних і інформаційних потоків під час їхньої передачі, зберігання та обробки. У сучасному світі вона виконує надзвичайно важливу функцію забезпечення безпеки суспільства перед потенційними небажаними наслідками, які можуть виникнути через вплив середовища інтернету та глобальних мереж передачі даних.

У нормативно-правовій базі України це поняття ґрунтовно розкрито в законі «Про основні засади здійснення кібербезпеки України», де кіберпростір проголошено віртуальним середовищем, яке формує умови для комунікації та реалізації соціальних відносин. Він створюється шляхом функціонування взаємопов'язаних комунікаційних систем і технологій електронного зв'язку за підтримки мережі Інтернет або інших глобальних платформ передачі даних. У цьому ж законі кібербезпека характеризується як процес забезпечення захисту основоположних інтересів індивіда,

суспільства та держави від ризиків у кіберпросторі. Вона покликана сприяти стабільному розвитку цифрових комунікаційних середовищ, швидкому реагуванню на загрози національній безпеці та мінімізації потенційних ризиків [1].

Одним із ключових аспектів ефективної роботи механізмів кібербезпеки є формування культури безпечної поведінки користувачів у цифровому середовищі. Закон виокремлює особливе значення підвищення рівня цифрової грамотності серед населення як стратегічний напрямок у розвитку безпечного та стабільного кіберпростору. Йдеться про комплекс знань, навичок і практичних умінь, що допомагають громадянам адаптуватися до нових умов і активно підтримувати ініціативи з удосконалення колективного захисту даних. У документі також наголошено на важливості державних і громадських проєктів, спрямованих на популяризацію обізнаності щодо кіберзагроз і відповідних заходів захисту, що є невід’ємними елементами сталого інформаційного суспільства [1].

Основи кібербезпеки є невід’ємною складовою сучасної цифрової грамотності, без якої неможливо повноцінно й безпечно взаємодіяти з цифровими технологіями. В умовах постійного розвитку технологій та поширення кібератак, знання з кібербезпеки допомагають захистити не лише персональні дані, а й пристрої, системи та онлайн-активності. Ця сфера охоплює широкий спектр практик, спрямованих на протидію таким загрозам, як шкідливе програмне забезпечення, фішинг і несанкціонований доступ до даних.

Цифрова грамотність включає знання, необхідні для виявлення потенційних загроз і уникнення ситуацій, що можуть призвести до витоку конфіденційних даних чи їх неправомірного використання. Для ефективного впровадження основних навичок потрібно дотримуватись кількох базових правил: використовувати надійні паролі та регулярно їх змінювати; створювати довжелезні комбінації з букв, цифр і спеціальних символів для кожного облікового запису, що суттєво ускладнить їх злам. Додатковий рівень захисту додасть активізація двофакторної автентифікації (2FA). Ця технологія додає захист шляхом підтвердження особи через SMS-повідомлення або зовнішній додаток. Необхідно уникати підозрілі посилання і вкладення. Не потрібно відкривати файли або веб-посилань із сумнівних джерел. Треба стежити за оновленнями програмного забезпечення, оскільки регулярне оновлення операційних систем і застосунків критично важливе для закриття відомих вразливостей, які можуть бути використані зловмисниками. Варто вчасно встановлювати антивіруси та інші засоби захисту. Використання антивірусного ПЗ, фаєрволів або антишпигунських програм дозволяє ефективніше виявляти та нейтралізувати потенційні загрози.

Вперше термін «цифрова грамотність» було визначено в роботі П. Гілстера, опублікованій у 1997 році. У своїй праці автор описав це поняття як здатність розуміти та використовувати інформацію, представлену в різних форматах і отриману з численних джерел за допомогою комп’ютерів [2]. З часом первісне трактування цифрової грамотності зазнало певних змін та оновлень. У 2015 році, в межах проєкту «Індекс цифрової грамотності», поняття було актуалізоване.

Відповідно до результатів проєкту, цифрова грамотність визначається як набір знань і навичок, необхідних для безпечного й ефективного використання цифрових технологій і ресурсів мережі Інтернет. Це включає цифрове споживання, компетенції та безпеку в цифровому середовищі [3].

Поняття цифрової грамотності зазвичай розглядається як сукупність знань і навичок, що дозволяють ефективно використовувати цифрові технології для особистих потреб користувача. Проте варто зауважити, що Інтернет від початку був створений як комунікаційний інструмент, і ця функція залишається ключовою до сьогодні. Тому аналіз цифрової грамотності потребує не тільки технічного підходу, а й комунікативного, враховуючи здатність користувачів ефективно взаємодіяти одне з одним у цифровому просторі.

Деякі дослідники вважають, що цифрова грамотність – це нова форма грамотності, що має на увазі пошук, оцінювання та використання різноманітних джерел інформації з метою формування комплексного змістовного уявлення про конкретне питання, тему або ситуацію [4, с. 435-438].

Отже, цифрова грамотність у поєднанні з кібербезпекою розширює можливості людей у різних аспектах їхньої діяльності. Це захист паролів та облікових записів, оскільки створення унікальних і складних паролів разом із застосуванням додаткового захисту унеможлиблюють крадіжку облікових даних.

Цифрова грамотність є ключовою передумовою для успішного функціонування людини в сучасному інформаційному суспільстві. Вона визначається як здатність ефективно використовувати цифрові технології для доступу до інформації, її оцінки, створення та обміну, що потребує оволодіння низкою важливих навичок. Цей термін охоплює п'ять основних компонентів, які дозволяють об'єктивно оцінити рівень її засвоєння: інформаційна грамотність, медійна грамотність, комп'ютерна грамотність, обчислювальна грамотність і комунікативна грамотність. Серед основних складових цифрової грамотності виділяють вміння працювати з інформацією, здійснювати її критичний аналіз, забезпечувати безпеку в Інтернеті, а також здатність до етичної взаємодії у цифровому середовищі. Це сприяє не лише ефективнішому використанню технологій, але й формуванню безпечної та відповідальної поведінки під час роботи з цифровими ресурсами. До цифрових компетенцій також входять навички програмування, обробки даних і використання цифрових інструментів у навчальній та професійній діяльності.

Важливим аспектом цифрової грамотності є кібербезпека, яка охоплює широкий спектр дій, технологій та методів для захисту інформаційних систем, мереж і ресурсів від несанкціонованого доступу, шкідливого втручання та кібератак. Основними компонентами кібербезпеки є захист даних, забезпечення безпеки мережевих комунікацій, обробка інформації, гарантування конфіденційності, цілісності та доступності даних. Ключовими завданнями в межах

кібербезпеки є оцінка ризиків, розробка політик і стандартів захисту, а також моніторинг і оперативне реагування на інциденти. Роль кібербезпеки у забезпеченні захисту цифрових ресурсів й охороні персональної та корпоративної інформації має стратегічне значення в умовах швидкого зростання використання Інтернету та інформаційно-комунікаційних технологій.

Список використаних джерел

1. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації від 3 березня 2021 р № 167-р Київ [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text>
2. Digital Education Action Plan (2021-2027). URL: <https://education.ec.europa.eu/focus-topics/digital-education/action-plan>
3. Gilster P. Digital Literacy. New York: Wiley. 8-th ed. 2019. 279 p.
4. Давиденко Г. Цифрова інклюзія та доступність: соціальна діджиталізація: монографія. Вінниця: ТВОРИ. 2023. 240 с. URL: <https://cutt.ly/meEwKWe4>

Соломія Оринчак,

solo17122or@gmail.com

Тернопільський національний педагогічний
університет імені Володимира Гнатюка;
Науковий керівник: доктор філологічних наук,
професор Любов Струганець

ЛЕКСИКО-ГРАМАТИЧНІ ОСОБЛИВОСТІ РЕКЛАМНОГО ДИСКУРСУ

Постановка проблеми. Сучасний рекламний дискурс в Україні є багатограним лінгвально-соціокультурним феноменом, що вийшов за межі суто комерційної комунікації і став активним інструментом формування суспільних цінностей, поведінкових моделей та підтримки національної ідентичності. Мова реклами, використовуючи маніпулятивний потенціал, має потужний вплив на свідомість реципієнтів, що вимагає її ґрунтовного наукового осмислення та класифікації мовних засобів за рівнями. На лексичному та граматичному рівнях відбувається постійна модернізація, що відображає динамічні зміни у лінгвосоціумі, особливо з огляду на необхідність вирішення нових прагматичних завдань: *спонукання до благодійності, підтримки військових та популяризації соціально потрібних ідей, таких як здоровий спосіб життя*. З огляду на це, детальний аналіз лексико-граматичної специфіки рекламного тексту є важливим складником формування медіаграмотності та наукового розуміння сучасних комунікативних процесів. Дослідження також є необхідним для методичної галузі, оскільки дозволяє оцінити наявність і якість аналізу рекламного тексту в шкільних та університетських підручниках.

Аналіз досліджень і публікацій. Теоретичним і практичним аспектам мови реклами, проблемам удосконалення тенденцій розвитку мовних технік