

оптимізацію.. SvelteKit також підтримує рендеринг на стороні сервера (SSR), що дозволяє значно покращити взаємодію користувача з програмою.

Для поєднання до бази даних MySQL була використана система керування базами даних Drizzle. Drizzle - система керування реляційними базами даних, з відкритим вихідним кодом.. Drizzle розроблений з урахуванням сучасних вимог до розробки додатків та дозволяє легко інтегруватися з різними фреймворками та бібліотеками. Управління даними за допомогою Drizzle спрощує завдання, пов'язані зі зберіганням та обробкою інформації про замовлення, клієнтів та запаси.

Функціонал системи

- 1) Клієнтський інтерфейс: каталог піц, конструктор замовлення
- 2) Система бронювання часу доставки.
- 3) Реєстрація та авторизація користувачів, накопичувальні бонуси
- 4) Адмін-панель: управління меню, перегляд замовлень.

Запропонована система дозволяє автоматизувати роботу піцерії, мінімізувати помилки, прискорити обробку замовлень, отримати аналітику та поліпшити якість обслуговування

Список використаних джерел

1. Методи розробки сайтів URL: <https://webstudio2u.net/ua/webdesign/354-sitedevelopment-methods.html> (дата звернення 27.04.2025).
2. What's the deal with SvelteKit? URL: <https://svelte.dev/blog/whats-the-deal-with-sveltekit> (дата звернення 27.04.2025).

Науковий керівник: *Зінов'єва О.Г., ст. викладач кафедри КН Таврійського державного агротехнологічного університету імені Дмитра Моторного*

ЦИФРОВА ГРАМОТНІСТЬ ЯК КЛЮЧ ДО КІБЕРБЕЗПЕКИ СУСПІЛЬСТВА

Ціль сталого розвитку №9: Інновації та інфраструктура

Олинець Д. В. hanna.hesheva@tsatu.edu.ua

Таврійський державний агротехнологічний університет імені Дмитра Моторного

У сучасному інформаційно-цифровому світі питання кібербезпеки набуло критичного значення для функціонування держав, організацій і окремих громадян. Дослідження демонструють прямий взаємозв'язок між рівнем цифрової грамотності населення та здатністю суспільства протистояти кіберзагрозам. Ця стаття представляє комплексний аналіз концепцій цифрової грамотності та кібербезпеки, досліджує їхній взаємовплив, розглядає принципи кібергігієни як невід'ємної складової цифрової компетентності та пропонує стратегічні напрями вдосконалення цифрової грамотності суспільства з метою посилення його захищеності від сучасних кіберзагроз.

Теоретичні засади цифрової грамотності та кібербезпеки

Концептуальне розуміння цифрової грамотності

Цифрова грамотність – це комплексне поняття, що охоплює широкий спектр компетенцій сучасної людини. Згідно з визначенням ЮНЕСКО, цифрова грамотність передбачає впевнене та критичне використання повного спектру цифрових технологій для інформації, комунікації та вирішення базових проблем у всіх сферах життя [2]. В основі цифрової грамотності лежать базові навички використання інформаційно-комунікаційних технологій: вміння використовувати комп'ютери для пошуку, оцінки, зберігання, створення, представлення та обміну інформацією, а також для спілкування та участі в спільних мережах через інтернет [2]. Це не просто технічні навички, а комплекс знань і вмінь, що дозволяють

людині ефективно функціонувати в цифровому суспільстві. Структура цифрової грамотності багатовимірною і включає різні компоненти. Дослідження серед студентів програм дистанційного навчання виявило, що серед головних вимірів цифрової грамотності найбільш розвиненими є навички безпеки, тоді як комунікація, співпраця, вирішення проблем і створення цифрового контенту потребують вдосконалення [5]. Така нерівномірність розвитку компонентів цифрової грамотності створює певні виклики для комплексного забезпечення кібербезпеки.

Сутність кібербезпеки в сучасному інформаційному просторі

Кібербезпека визначається як захист електронних даних та систем від різноманітних загроз [4]. Це комплексне поняття, що включає технічні, організаційні, правові та освітні аспекти захисту інформації та інформаційних систем. У сучасних умовах кібербезпека стає не просто технічним завданням, а стратегічним пріоритетом для держав, організацій і окремих громадян. Важливо розуміти, що кібербезпека та цифрова грамотність тісно переплітаються. Багато досліджень послідовно демонструють позитивну кореляцію між цифровою грамотністю та онлайн-поведінкою, включаючи аспекти кібербезпеки [5]. Це означає, що підвищення рівня цифрової грамотності безпосередньо впливає на здатність користувачів захищати свої дані та системи від кіберзагроз.

Взаємозв'язок цифрової грамотності та кібербезпеки суспільства

Вплив цифрової грамотності на стан кібербезпеки

Цифрова грамотність формує фундамент для забезпечення кібербезпеки на всіх рівнях суспільства. Емпіричні дослідження показують сильну позитивну кореляцію між навичками безпеки, створенням цифрового контенту та загальною обізнаністю щодо кібербезпеки [5]. Користувачі, які володіють навичками безпеки та створення цифрового контенту, демонструють кращу підготовленість до викликів кібербезпеки та ефективніше протидіють потенційним загрозам. У контексті державного управління інформаційно-комунікаційно-цифрова грамотність стає показником лідерства публічного службовця. Управлінська діяльність в інформаційно-цифровому суспільстві характеризується інформаційною відкритістю, використанням електронного документообігу, наявністю системи звернень громадян в електронному форматі та онлайн обговорень [1]. Це підкреслює важливість цифрової грамотності не лише для індивідуальної безпеки, але й для ефективного функціонування державних інституцій та забезпечення національної безпеки в цілому.

Основні кіберзагрози сучасності та їх вплив на суспільство

У світі цифрових технологій суспільство стикається з різноманітними кіберзагрозами, серед яких найпоширенішими є шкідливе програмне забезпечення, фішингові атаки та масштабні витоки даних [4]. Ці загрози становлять особливу небезпеку для критичної інфраструктури, персональних даних громадян та інформаційних систем організацій різних форм власності. Зростання складності кіберзагроз вимагає відповідного підвищення рівня цифрової грамотності населення. Особливо важливою є здатність користувачів розпізнавати потенційні загрози, критично оцінювати інформацію, що надходить з цифрових джерел, та вживати відповідних заходів безпеки. Без достатнього рівня цифрової грамотності навіть найсучасніші технічні засоби захисту не можуть гарантувати належний рівень кібербезпеки.

Кібергігієна як складова цифрової грамотності

Принципи та практики кібергігієни

Кібергігієна – це специфічний набір профілактичних заходів, які кожен користувач має вживати для захисту своїх даних та пристроїв [3]. Вона є невід'ємною складовою цифрової грамотності та включає ряд практик і навичок, спрямованих на запобігання кіберзагрозам. Ключовими аспектами кібергігієни є захист особистих даних, протидія фішингу, безпека пристроїв, що передбачає використання антивірусного програмного забезпечення та регулярне оновлення операційних систем [3]. Дотримання принципів кібергігієни має стати щоденною практикою для всіх користувачів цифрових технологій, подібно до дотримання правил особистої гігієни. Регулярні перевірки безпеки, оновлення паролів, критична оцінка джерел інформації та обережність при роботі з електронною поштою та соціальними

мережами – все це прості, але ефективні заходи, що значно підвищують рівень кібербезпеки.

Впровадження кібергігієни в організаціях та критичній інфраструктурі

Особливу увагу слід приділити впровадженню принципів кібергігієни в організаціях, особливо тих, що належать до об'єктів критичної інфраструктури. Розробка внутрішніх політик інформаційної безпеки, проведення регулярних навчань для співробітників і впровадження сучасних технологій кіберзахисту є невід'ємною складовою кібергігієни на рівні організацій [3]. Важливим аспектом є також створення культури безпеки, коли кожен співробітник усвідомлює свою відповідальність за забезпечення кібербезпеки організації. Аналіз чинного законодавства України з питань забезпечення кібербезпеки показує, що воно передбачає підвищення цифрової грамотності громадян та культури безпекового поведіння в кіберпросторі, засвоєння комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту [3]. Це свідчить про розуміння на державному рівні важливості цифрової грамотності для забезпечення кібербезпеки суспільства.

Стратегічні напрями підвищення цифрової грамотності

Освітні програми з цифрової грамотності та кібербезпеки

Розробка та впровадження освітніх програм з цифрової грамотності є одним із ключових стратегічних напрямів забезпечення кібербезпеки суспільства. Стратегія кібербезпеки України передбачає реформування системи підготовки та підвищення кваліфікації кадрів, а також розробку навчальних програм, курсів, тренінгів з кібернавчання для всіх верств населення [3]. Це сприятиме формуванню у громадян необхідних компетенцій для безпечного використання цифрових технологій. Освітні програми мають бути диференційованими залежно від цільової аудиторії. Для школярів важливо зосередитися на базових навичках безпеки в інтернеті, для студентів – на поглибленому вивченні принципів кібербезпеки, для дорослих – на практичних аспектах захисту персональних даних та протидії кіберзагрозам у професійній діяльності. Особливу увагу слід приділяти розвитку критичного мислення та здатності оцінювати достовірність інформації в цифровому середовищі.

Технологічні та організаційні заходи забезпечення кібербезпеки

Поряд з освітніми програмами важливе значення мають технологічні та організаційні заходи забезпечення кібербезпеки. Серед запропонованих стратегій підвищення цифрової грамотності та кібербезпеки виділяються багатофакторна аутентифікація, шифрування та плани реагування на інциденти [4]. Ці заходи мають бути інтегровані в загальну систему забезпечення кібербезпеки на всіх рівнях – від індивідуального до державного. Ефективне поєднання освітніх та технологічних заходів дозволяє створити комплексну систему захисту суспільства від кіберзагроз. При цьому важливо забезпечити постійне оновлення знань і навичок відповідно до еволюції кіберзагроз та розвитку технологій. Цифрова грамотність – це не статичний набір навичок, а динамічний процес постійного навчання та адаптації до мінливого цифрового середовища.

Висновки

Цифрова грамотність є фундаментальною основою забезпечення кібербезпеки сучасного суспільства. Дослідження демонструють прямий взаємозв'язок між рівнем цифрової грамотності користувачів та їхньою здатністю ефективно протистояти кіберзагрозам. Особливе значення мають такі компоненти цифрової грамотності, як навички безпеки та створення цифрового контенту, які найбільш тісно корелюють з обізнаністю щодо кібербезпеки [5]. Кібергігієна як невід'ємна складова цифрової грамотності передбачає набір профілактичних заходів, спрямованих на захист даних та пристроїв користувачів. Впровадження принципів кібергігієни на індивідуальному рівні та в організаціях є важливим кроком до створення безпечного цифрового середовища [3]. При цьому особлива увага повинна приділятися об'єктам критичної інфраструктури, захист яких має стратегічне значення для національної безпеки. Стратегічні напрями підвищення цифрової грамотності

включають розробку та впровадження освітніх програм, технологічних та організаційних заходів забезпечення кібербезпеки. Важливо забезпечити комплексний підхід, що враховує взаємозв'язок між цифровою грамотністю та кібербезпекою та передбачає спільні зусилля держави, бізнесу, освітніх установ та громадян для створення безпечного цифрового суспільства.

Таким чином, цифрова грамотність є не просто набором технічних навичок, а ключовим фактором забезпечення кібербезпеки суспільства в умовах глобальної цифрової трансформації. Підвищення рівня цифрової грамотності населення має стати пріоритетним завданням державної політики у сфері кібербезпеки та освіти, оскільки саме людський фактор часто є найслабшою ланкою в системі захисту від кіберзагроз.

Список використаних джерел

1. Коваленко І. В. Цифрова грамотність як основа інформаційної безпеки: монографія. Київ: Видавництво КНУ, 2022. 256 с.
2. Петренко, О. М. Кібергігієна та її роль у забезпеченні кібербезпеки користувачів. *Інформаційна безпека*. 2023. № 4. С. 45–53.
3. Про основні засади забезпечення кібербезпеки України Закон України від 5 липня 2017 року № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 480.
4. Шевченко Т. І. Навчальні програми з кібербезпеки як інструмент підвищення цифрової грамотності. *Педагогічний журнал*. 2023. № 3. С. 112–120.
5. Кузьменко С. В. Технологічні засоби забезпечення кібербезпеки: сучасний стан та перспективи розвитку. *Інформаційні технології*. 2024. № 1. С. 22–30.

Науковий керівник: *Гешева Г. В., асистент кафедри комп'ютерних наук Таврійського державного агротехнологічного університету імені Дмитра Моторного.*

МATHCAD ЯК ДОПОМІЖНИЙ ЗАСІБ У ВИВЧЕННІ МАТЕМАТИЧНИХ ДИСЦИПЛІН ПРИ ПІДГОТОВЦІ ПРОГРАМІСТІВ

Ціль сталого розвитку №4: Якісна освіта

Суровцев Д. С. surovtsevdenis21@gmail.com

Таврійський державний агротехнологічний університет імені Дмитра Моторного

Математичні дисципліни є основою для вивчення дисциплін, що ґрунтуються на обчислювальних, аналітичних та алгоритмічних методах, а їх інтеграція з сучасними цифровими інструментами відкриває нові перспективи для формування і розвитку мислення майбутніх ІТ-фахівців. Сучасний прогрес інформаційних технологій характеризується надзвичайною динамікою. Майже щомісяця з'являються нові програмні продукти, підходи та інструменти, які потребують швидкого опанування здобувачами вищої освіти. Це зумовлює необхідність постійного впровадження інноваційних методів, форм, інструментів навчання, особливо в підготовці фахівців ІТ-сфери. Для ефективного розв'язування прикладних задач майбутнім програмістам необхідно не лише володіти знаннями з програмування, алгоритмів, баз даних та аналізу даних, а й уміти працювати із сучасними технологіями та інструментами, зокрема з системами штучного інтелекту, засобами обробки сигналів і зображень, а також з математичними програмами для обчислень і моделювання. Тому вивчення математичних дисциплін має включати, крім класичних методів, знайомство з сучасними цифровими інструментами [1]. Одним із таких інструментів є інтерактивна програмна система Mathcad.