R2:
Всі значення відповідають умовам середнього ризику.
Рівень істинності: =
R3:
ПК (низький ризик) активується частково з належністю 0.0.
ФБ (високий ризик) має належність 0.0.
МД (низький ризик) має належність 0.2.
АМТ (високий ризик) має належність 0.6.
ЗЗ (високий ризик) має належність 0.0.
Рівень істинності: =

Агрегування виходів - дозволяє сформувати узагальнений набір значень для нечіткої множини, що описує кінцевий рівень загрози для організації [6].
Агреговано результати для кожного правила:
B1: Високий рівень загрози з належністю 0.4.
B2: Середній рівень загрози з належністю 0.19.
B3: Високий рівень загрози з належністю 0.0.
Об'єднання результату: =

Дефазифікація виходу - перетворення нечіткої множини у чітке значення [7].

$$y = \frac{(0 \times 0.4) + (0.5 \times 0.19) + (1 \times 0)}{1 + 1 + 1} = \frac{0 + 0.2 + 0}{3} = 0.095$$

Таким чином, рівень загрози для заданих умов є низьким і становить 9.5% - це означає, що рівень безпеки функціонування достатній.

Висновок. Запропонована система дозволяє розширити можливості аналізу й захисту даних, автоматизуючи процеси прийняття рішень. Використання нечітких множин дає змогу швидко адаптуватися до нових умов і реагувати на зміни в поведінці користувачів, зменшуючи ризики.

Список використаних джерел

1. Why training is the best defence against cybersecurity and data threats. URL: https://thomasmurray.com/training-employees-cyber-security (Last accessed: 10.11.2024).
2. Mamdani, Ebrahim H . "Application of fuzzy algorithms for control of simple dynamic plant". Proceedings of the Institution of Electrical Engineers. 121 (12): 1585–1588. doi:10.1049/piee.1974.0328.
3. User Behavior Analysis for Detecting Compromised User Accounts. URL: https://www.researchgate.net/publication/374277004 (Last accessed: 10.11.2024).
4. 14 Cybersecurity Metrics + KPIs You Must Track in 2024. URL: https://www.upguard.com/blog/cybersecurity-metrics (Last accessed: 10.11.2024).
5. Survey on Network Security Traffic Analysis and Anomaly Detection Techniques. URL: https://www.researchgate.net/publication/380903277 (Last accessed: 10.11.2024).
6. Fuzzy Inference Process URL: https://la.mathworks.com/help/fuzzy/fuzzy-inference-process.html (Last accessed: 10.11.2024).
7. Defuzzification Methods. URL: https://la.mathworks.com/help/fuzzy/defuzzification-methods.html (Last accessed: 10.11.2024).

ПОЙДА С.А.,
к.пенд.н., доцент кафедри управління та адімінстрування
ГРАБОВИЙ Р.В.,
студент спеціальності «Публічне управління та адміністрування»,
ступеня вищої освіти «Магістр»,
КЗВО «Вінницька академія безперервної освіти»

МЕДІАГРАМОТНІСТЬ ТА КІБЕРБЕЗПЕКА ЯК КЛЮЧОВІ КОМПЕТЕНТНОСТІ СУЧАСНОГО ФАХІВЦЯ З ПУБЛІЧНОГО УПРАВЛІННЯ

Стрімкий розвиток цифрових технологій та зростання обсягів інформації вимагає від сучасного фахівця з публічного управління навиків медіаграмотності та розуміння основ кібербезпеки. Інформаційні загрози стають загрозою для органів управлінняя та соціуму загалом. Здатність критично оцінювати інформацію, розпізнавати фейки та маніпуляції, забезпечення захисту

персональних даних, розуміння, яка інформація є критично важливою та навики щодо її захисту є ключовими компетенціями сучасного управлінця.

Окрім необхідності в базовій медіаграмотності, фахівці з публічного управління повинні усвідомлювати роль інформації в прийнятті рішень та її вплив на суспільні процеси. Вони мають бути здатні не лише орієнтуватися в інформаційному середовищі, а й активно протидіяти кіберзагрозам, що стають дедалі складнішими та витонченішими.

Звісно, від фахівця з публічного управління, ніхто не вимагає ґрунтовних технічних знань. Однак, оскільки часто кібератаки пов'язані із соціальною інженерією, то це вимагає від фахівця з публічного управління, переважно розуміння соціальних і психологічних аспектів кібербезпеки, що дозволяє ефективно захищати як державні установи, так і громадян від шкідливих впливів.

Соціальна інженерія — це метод маніпуляції людьми з метою отримання конфіденційної інформації або доступу до захищених систем без застосування технічних засобів злому. Замість того, щоб атакувати програмні або апаратні компоненти системи, зловмисники використовують психологічний вплив, експлуатуючи людські слабкості, такі як довірливість, страх або бажання допомогти. На науковців «зловмисники використовують методи соціальної інженерії, щоб приховати свої справжні особистості і мотиви і видати себе за довірену людину або джерело інформації. Мета атаки полягає в тому, щоб маніпуляцією або обманним шляхом змусити користувача надати конфіденційну інформацію або доступ зловмиснику в межах організації. Багато вдалих атак в області соціальної інженерії просто покладаються на готовність людей бути корисними. Наприклад, зловмисник може претендувати на роль співробітника, у якого є якась термінова проблема, що вимагає доступу до додаткових мережевих ресурсів"[1].

Розуміння принципів соціальної інженерії дає можливість осягнути критичні для інфраструктури точки впливу - осіб, на яких цей вплив буде здійснюватись зловмисниками в першу чергу. Цю думку підтримують дослідники, які зауважують, що "першим кроком в більшості атак соціальної інженерії є проведення дослідження або своєрідна розвідка, з метою дізнатися про об'єкт атаки якомога більше. Серед зловмисників, що використовують соціальну інженерію, популярна тактика, яка полягає в тому, щоб зосередитися на поведінці співробітників з невисоким рівнем повноважень, але з початковим доступом, наприклад, охоронцем або людиною, яка сидить на стійці реєстрації. Злочинці можуть переглядати профілі в соціальних мережах цих співробітників, з метою отримання інформації, і, таким чином, вивчати їх поведінку як у онлайн так і звичайному житті особисто. На основі зібраної інформації, злочинець може розробити план нападу, скориставшись вразливостями, виявленими в ході етапу розвідки"[1].

Таке явище, як соціальна інженерія появилось ще задовго до появи мережі Інтернет і, переважно, використовувалось для отримання доступу до конфіденційної інформації у військовій розвідці та промисловому шпіонажі, адже найвищу вартість у постіндустріальному суспільстві має саме інформація. Зокрема, М. Говда зауважує, що "соціальну інженерію, як зброю почали використовувати вже давно для особистого збагачення, шантажу, розваги, залякування тощо. Соціальна інженерія не вимагає знання програмування чи інших технічних знань, тобто агресором може бути навіть самий неосвічений злодій. Існують різні методи та форми соціальної інженерії, найважливіші хочу відмітити: фішинг, вішинг та смішинг, видавання себе за іншу особу та, звичайно, кібершахрайство"[2]. Водночас варто зауважити, що неосвічений у технічних питаннях зловмисник може мати ґрунтовні знання у галузі психології, що дає йому суттєві сподівання на успіх. Такі дії зловмисників можуть мати катастрофічні наслідки у період війни, оскільки можуть передбачати отримання ворогом важливої інформації, пов'язаної з військовою та державною таємницею, критичною інфраструктурою, фінансовими та особистими даними.

О.Бохонько та С.Лисенко стверджують, що "масштабні кібератаки із застосуванням соціальної інженерії можуть мати далекосяжні наслідки, що виходять за межі окремих жертв або організацій. Наприклад, кібератаки на об'єкти критичної інфраструктури, державні системи або комунальні підприємства можуть порушити надання основних послуг, поставити під загрозу громадську безпеку або підірвати довіру в суспільстві. Жертвами таких атак стали багато транснаціональних корпорацій і компаній, інформаційних агентств і навіть урядові установи цілих держав. Зловмисники отримують доступ до інформації, націлюючись на окремих осіб, але в більшості випадків їхньою основною метою є організації з якими такі особи мають певні зв'язки"[3].

Поширеними методами соціальної інженерії є:

- Фішинг – відправлення електронних листів або повідомлень, які виглядають як офіційні запити від відомих організацій. Метою фішингу є змусити жертву передати логіни, паролі або іншу конфіденційну інформацію.
- Вішинг (голосовий фішинг) – використання телефонних дзвінків для отримання конфіденційних даних під виглядом працівників банку, служби підтримки або державних органів.
- Смішинг (SMS-фішинг) – використання текстових повідомлень для того, щоб переконати жертву перейти за шкідливим посиланням або завантажити шкідливе програмне забезпечення.
- Претекстинг – створення вигаданої історії або ситуації, яка змушує жертву розкрити конфіденційну інформацію. Наприклад, зловмисник може видавати себе за представника служби безпеки або колегу.
- Бейтинг – використання привабливих пропозицій або приманок, наприклад, заражених USB-накопичувачів, які залишаються у громадських місцях, сподіваючись, що хтось підключить їх до комп'ютера.

Розглянемо приклади цих атак та їх наслідки більш докладно. Почнемо з фішингової атаки на інформаційну інфраструктуру компанії Sony Pictures 24 листопада 2014 року. Зловмисник надіслали фішингові листи за допомогою яких отримали доступ до локальної мережі компанії, в наслідок чого були викрадені й опубліковані конфіденційні дані, що стало причиною фінансових та репутаційних втрат [4].

Відповідальність за атаку взяла на себе хакерська група «Guardians of Peace» («GOP»), опублікувавши конфіденційну переписку адміністрації щодо Дженніфер Лоуренс, Бреда Пітта, Джорджа Клуні, а також оприлюднивши авторську версію матеріалів фільму «Зоряні війни: Пробудження Сили». Розвідка США звинуватила у цьому злочині уряд Північної Кореї, як організаторів атаки та керівників хакерського угрупування. Керівництво Північної Кореї відкидає звинувачення, оскільки особистості хакерів та їх спільників у Sony Pictures досі невідомі [4].

На думку О.Акменко, "цей інцидент сильно пошкодив репутацію компанії, спричинив значні фінансові втрати та порушив конфіденційність клієнтів та співробітників. Крім того, він викликав серйозні проблеми з кібербезпекою та викликав глобальну обуреність. Цей приклад підкреслює важливість захисту конфіденційної інформації та необхідність використання сучасних технологій і стратегій для попередження кібератак та забезпечення економічної безпеки компанії"[5].

Одним із прикладів фішингових атак також є дія шкідливого програмного забезпечення WannaCry - "вимагальник" (ransomware), яке стало широко відомим після масової кібератаки у травні 2017 року. Вірус швидко поширювався по всьому світу, вражаючи сотні тисяч комп'ютерів у понад 150 країнах. Основний механізм роботи WannaCry полягає в тому, що він шифрує файли на інфікованому комп'ютері та вимагає викуп, зазвичай у криптовалюті Bitcoin, для їхнього розблокування. Зловмисники встановлювали крайній термін, після якого сума викупу збільшувалася або дані ставали недоступними назавжди. Як зазначає О. Зосимчук "атака WannaCry була серією кібератак, здійснених глобальним кіберзлочинним угрупованням, яке використовувало ботнет для розповсюдження шкідливого програмного забезпечення шифровальника WannaCry. WannaCry використовував уразливість у програмному забезпеченні Microsoft Windows, щоб отримати доступ до комп'ютерів і шифрувати їхні файли, а потім вимагати викуп у розмірі 300 доларів США у біткойнах "[6].

Українська цифрова інфораструктура ткож постраждала від поідбного шкідливого програмного забезпечення. "Я-петя" (або Petya, також відомий як NotPetya) — це шкідливе програмне забезпечення типу WannaCry, яке стало відомим через масштабну кібератаку, що вразила низку організацій, переважно в Україні. Хоча цей вірус був спрямований на вимагання викупу за розблокування зашифрованих файлів, згодом стало зрозуміло, що його основна мета — знищення даних, а не просто отримання грошей. Цей вірус поширювався через вразливість у протоколі SMB, так само як і WannaCry, але також використовував оновлення програмного забезпечення бухгалтерської системи M.E.Doc, широко поширеної в Україні. Серед постраждалих опинилися банки, енергетичні компанії, аеропорти, урядові установи, що призвело до значних фінансових втрат та збоїв в роботі критичної інфраструктури.

На думку В. Кривошеїна, "атаки вірусу Petya підтверджують небезпеки глобальної кібервійни і неготовність, а інколи і безпорадність державної влади у боротьбі із загрозами такого рівня. Виникає побоювання щодо нездатності провідних міжнародних акторів мінімізувати наслідки кібератак як спеціальних операцій в умовах глобальної кібервійни [7] ".

Саме медіаграмотність, розуміння того, що не варто бездумно відкривати файли-вкладення до електронних листів, могло б значно знизити ризики кібератак на державні установи, зберігши конфіденційність і безпеку державних даних. Обробка величезних обсягів чутливої інформації, включно з персональними даними громадян і стратегічно важливими державними документами вимагають від сучасного фахівця з публічного управління навиків медіаграмотності та відповідального ставлення до інформаційної безпеки. Належна обізнаність з правилами кібергігієни та запровадження політики безпечної роботи з електронними листами — це необхідні кроки для захисту інформаційної інфраструктури держави та підтримки її стабільної роботи в умовах цифрової трансформації.

Нерідко в Україні останнім часом стається злам електронної пошти, облікових записів у соціальних мережах та месенджерах. Результатом цього є втрата персональних даних, доступ зловмисників до критично-важливої інформації та коштів потерпілих. Якщо фішингові атаки стаються, переважно, через електронну пошту, то у вказаних випадках зловмисники частіше вдаються до вішингу та смішингу.

Для цього шахраї представляються працівниками банків або правоохоронних органів і повідомляють жертві про "проблеми" з рахунком або підозрілі транзакції. Під приводом необхідності перевірки інформації вони просять надати особисті дані, такі як номери банківських карток, CVC-коди або паролі до облікових записів. Аналогічні атаки можуть бути здійснення через SMS, або повідомлення у месенджерах, що виглядають як повідомлення від офіційних організацій, наприклад, від банків чи поштових служб. У цих повідомленнях містяться посилання на фальшиві вебсайти, де користувачів просять ввести особисті дані, або ж пропонується завантажити шкідливе програмне забезпечення. Наприклад, під виглядом банківського документа у PDF-файлі може міститись шкідливе програмне забезпечення. У випадку менеджерів зловмисники стараються отримати коди безпеки, які месенджери надсилають у випадку зміни номеру телефону чи паролю домесенджерів. Часто такі повідомлення мають характерні елементи терміновості, наприклад, попередження про необхідність підтвердження фінансової операції або доставлення посилки, що може змусити людину діяти швидко і необачно.

У випадку байтингу зловмисники пропонують щось, що виглядає вигідним або привабливим для потенційної жертви. Це може бути фізичний предмет (наприклад, USB-накопичувач), який навмисно залишають у громадському місці, або віртуальна пропозиція, така як безкоштовне програмне забезпечення, музика, фільми чи інші цифрові матеріали, але разом із цією інформацією завантажується шкідливе програмне забезпечення, що відкриває зловмиснику доступ до даних, які зберігаються на пристрої. Як тільки жертва підключає знайдений пристрій або завантажує запропоновані файли, шкідливе програмне забезпечення починає інфікувати її комп'ютер або мережу, що може призвести до викрадення даних, контролю над системою або розповсюдження вірусу в корпоративній мережі.

Якщо попередні види атак шкодять, перш за все самим користувачам, то претекстинг у сфері публічного управління є надзвичайно небезпечним. Це характерний приклад соціальної інженерії та може бути використаний для отримання доступу до конфіденційної державної інформації або критичних інфраструктур. Наприклад, зловмисник може представитися представником іншої державної установи або високопосадовцем і вимагати доступ до документів чи баз даних, посилаючись на нагальні службові потреби. У таких ситуаціях жертви, зважаючи на авторитет або начебто офіційний характер запиту, можуть передати інформацію, не замислюючись про справжність запиту.

Розглянемо тепер шляхи реагування на описані виклики. Важливим аспектом подолання загроз, пов’язаних із кібератаками є запровадження установами чітких правил безпеки, які регулюють використання зовнішніх пристроїв і обробку інформації. Наприклад, можна заборонити використання невідомих USB-накопичувачів або встановлення програмного забезпечення з неперевірених джерел. Крім того, важливо використовувати ліцензійне програмне забезпечення, регулярно його оновлювати та використовувати сучасні антивірусні системи, щоб мінімізувати ризики інфікування шкідливим ПЗ. Прийняті організацією політики безпеки мають бути зрозумілими й обов’язковими для всіх працівників.

Ще одним важливим кроком створення культури кібербезпеки в організаціях є формування у кожного працівника розуміння своєї відповідальності за збереження даних, що мають критичне значення, або становлять державну таємницю. Це включає не лише дотримання правил, але й активне обговорення та навчання щодо запобігання кіберзагрозам на всіх рівнях. Важливо

заохочувати працівників звертатися за допомогою або повідомляти про підозрілі інциденти, навіть якщо вони не впевнені в їх небезпеці.

Подолання загроз для організацій та суспільства, пов'язаних з кібератаками, можна лише шляхом підвищення обізнаності та навчання. Фахівці з публічного управління повинні постійно навчатись, щоб розуміти, як діяти у випадку кібератаки. Чим краще вони розумітимуть ці загрози, тим більше шансів, що вони зможуть вчасно їх розпізнати і не стати жертвою кіберзагроз. Це включає навчання розпізнаванню підозрілих повідомлень і дзвінків, а також розуміння, що не можна передавати конфіденційну інформацію без підтвердження достовірності запиту.

Розглядаючи форми навчання фахівців з публічного управління варто зупинитись на такому виді самонавчання через мережу Інтернет, як МООС - (Massive Open Online Courses) курси — це масові відкриті онлайн-курси, які стають все популярнішими серед фахівців з публічного управління. Цей формат навчання дозволяє кожному самостійно отримувати якісні знання з різних галузей, включаючи публічне управління, кібербезпеку, цифрові технології, управління проєктами та інші важливі темиу зручному для них місці та у зручний час. МООС курси надають можливість доступу до навчальних програм провідних університетів та інституцій світу, таких як Гарвард, MIT, Стенфорд, що робить їх ідеальними для тих, хто хоче підвищувати свою кваліфікацію за новітніми стандартами. Серед українських сервісів МООС варто відзначити такі:

- https://apps.prometheus.org.ua/
- https://vumonline.ua/
- https://ed-era.com/
- https://osvita.diia.gov.ua/

Важливим шляхом розвитку компетентності, пов'язаної з медіаграмотністю та кібербезпекою є онлайн-курси та вебінари, які дозволяють навчатися без відриву від основної роботи, оскільки переважну більшість таких занять можна переглядати у записі. Цей формат особливо корисний у контексті постійного вдосконалення, оскільки публічні службовці можуть отримувати нові знання у зручний для себе час. Онлайн-курси часто пропонують сертифікацію, що підтверджує рівень знань і додає ваги професійному розвитку. Крім того, сучасні освітні платформи дають можливість доступу до матеріалів, підготованих провідними експертами з усього світу, що допомагає підвищувати рівень компетенцій у глобальному контексті.

Ефективною формою розвитку компетентності, пов'язаної з медіаграмотністю та кібербезпекою є періодичні офлайн семінари та тренінги, де працівники можуть безпосередньо взаємодіяти з експертами, обговорювати конкретні проблеми та практично відпрацьовувати навички. Такі заходи можуть бути присвячені темам, як-от медіаграмотність, кібербезпека або управління інформацією, що дозволить фахівцям удосконалити свої професійні компетенції.

Таким чином, медіаграмотність та кібербезпека в сучасних умовах отримали ключове значення для ефективного виконання обов'язків сучасного фахівця з публічного управління. Важливість цих навичок полягає не тільки у вмінні орієнтуватися в інформаційному середовищі, але й у здатності протидіяти різноманітним кіберзагрозам. Використання методів соціальної інженерії, та інші види кіберзагроз вимагають від фахівців з публічного управління уміння реагування на них.

Успішна протидія кібератакам реалізується через впровадження чітких політик безпеки в державних установах та регулярне навчання працівників. Формування культури відповідальності за інформаційну безпеку в організаціях, використання ліцензійного програмного забезпечення та розробка внутрішніх протоколів безпеки - важливі кроки для мінімізації ризиків.

Важливо також постійно вдосконалювати свої навички, беручи участь у тренінгах, семінарах, вебінарах та використовуючи сучасні форми навчання. Це дозволяє не лише підвищувати рівень професійної компетентності, але й розуміти новітні технології та протидіяти загрозам у сфері кібербезпеки, забезпечуючи тим самим надійний захист.

Використана література

1. Войтко Б. С., Марченко М. М., Антонов Ю. С., к.ф.-м.н., Соціальна інженерія як інструмент для проникнення у інформаційну систему підприємства. 2020р. С.198-199. -URL: https://jait.donnu.edu.ua/article/view/9023
2. Говда М. Соціальна інженерія як інформаціна зброя в ході російсько-української війни. 2023р. С. 150. -URL: http://surl.li/ezjfmg
3. Бохонько О., Лисенко С., Методи виявлення кібератак соціальної інженерії 2023р. С. 231 -URL: http://surl.li/nromvv

4. Wikipedia. Хакерська_атака_на_сервери_Sony_Pictures_Entertainment [Електронний ресурс] / Wikipedia. – 2014. -URL: http://surl.li/zmdoor
5. Акименко О. Ю., Інформаційно-аналітичне забезпечення управління економічною безпекою підприємства 2023р. С. 312. -URL: http://surl.li/eqifwg
6. Зосимчук О. Р., Методика та програмний застосунок для запобігання кібератакам 2023р. С. 12. -URL: http://surl.li/rekdmc
7. Кривошеїн В. В. Ментальні ризики в ракурсі «Ми» – «Вони» . 2017р. С. 271. -URL: https://ipiend.gov.ua/wp-content/uploads/2018/07/zn_88_90.pdf

ПОЙДА С.А.,
к.пед.н., доцент кафедри управління та адміністрування
КЗВО «Вінницька академія безперервної освіти»

ФОРМУВАННЯ НАВИЧОК ВИКОРИСТАННЯ НЕЙРОМЕРЕЖ У ПРОЦЕСІ ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ ПЕДАГОГІЧНИХ ПРАЦІВНИКІВ

Анотація. У статті розглядаються актуальні аспекти підготовки педагогічних працівників до використання генеративного штучного інтелекту у їх професійній діяльності

Загальнодоступні та дружні до користувачів системи генеративного штучного інтелекту (ГШІ), що з'явились зовсім недавно, активно почали використовуватись фахівцями в різних галузях науки та суспільного життя. Питання використання систем генеративних штучного інтелекту не обійшло і освітян. Водночас варто зазначити що педагогічні працівники ще недостатньо використовують системи генеративного штучного інтелекту у своїй професійній діяльності. Це пов'язано з кількома факторами, серед яких найістотнішими є відсутність якісного підключення до мережі інтернет та нерозуміння принципів побудови запитів до таких сервісів.

Генеративний штучний інтелект працює на основі великих мовних моделей (LLM), які по суті є нейромережами, спеціально навченими на величезних обсягах даних. Такі сервіси використовують архітектуру нейромереж, щоб генерувати текст, зображення, аудіо та відео. ГШІ застосовує принципи нейромереж для створення нового контенту на основі запитів, або промптів. Опрацьовуючи запит користувача нейромережа аналізує слова та фрази, визначає їх зв’язки у тексті з урахуванням бази даних, на якій була навчена та генерує відповідь, яка виглядає осмисленою та творчою.

Серед переваг використання нейромереж для педагогів варто відзначити автоматизацію рутинних процесів, допомогу в підготовці методичних та дидактичних матеріалів (планів-конспектів, практичних завдань, інструментів оцінювання тощо), надають можливість побудови індивідуальної траєкторії навчання з урахуванням потреб кожного учня.

При цьому можна визначити низку недоліків стосовно використання генеративного штучного інтелекту вчителями, серед яких: помилки або некоректна інформація у генерованому контенті (так звані, цифрові галюцинації), зниження здатності вчителів до креативної діяльності, надмірні очікування від результатів діяльності нейромереж тощо. Також використання нейромереж викликає етичні питання, адже його безконтрольне застосування може суперечити принципам академічної доброчесності.

Водночас, існує ряд факторів, які визначають потребу в підготовці вчителів до використання нейромереж у власній професійній діяльності. Перш за все, це те, що учні вже активно використовують нейромережі для виконання навчальних завдань і вчителю просто необхідно вміти за стилем отриманого матеріалу розрізняти генерований текст. З цієї проблеми випливає й наступна – вчителю необхідно розуміти як працюють нейромережі та як будуються до них запити для того, щоб перебудувати навчальний процес так, щоб учень не використовував ГШІ там, де він повинен думати самостійно. Третім фактором є потреба у створенні якісного яскравого навчального контенту, який зміг би привернути увагу, зацікавити сучасного учня, адже саме цікавість, в першу чергу, дає можливість формувати мотивацію здобувачів освіти.

У КЗВО «Вінницька академія безперервної освіти» вже понад рік проводяться курси підвищення кваліфікації для педагогічних працівників, що допомагають вчителям опановувати ці інструменти. На курсах особливу увагу приділяють навчанню побудови якісних запитів (промптів) для роботи з великими текстовими моделями, розглядаються питання генерації зображень, презентацій,