УДК 378.147:004.056.5

М.Г. Коляда, Луганський національний університет імені Тараса Шевченка

ПРОДУКТИВНІ МЕТОДИ НАВЧАННЯ МАЙБУТНІХ ФАХІВЦІВ ІЗ ЗАХИСТУ ІНФОРМАЦІЇ ТА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Коляда М.Г.

Продуктивні методи навчання майбутніх фахівців із захисту інформації та управління інформаційною безпекою

У статті розглядаються продуктивні методи навчання майбутніх фахівців із захисту інформації та управління інформаційною безпекою. Автор наводить когнітивні методи навчання, такі як метод: евристичних запитань, порівнянь, фактів, досліджень, конструювання понять, конструювання правил, прогнозування, помилок, метод «Що буде, якщо...?».

Ключові слова: методи навчання, продуктивні методи, когнітивні методи.

Коляда М.Г.

Продуктивные методы обучения будущих специалистов по защите информации и управлению информационной безопасностью

В статье рассматриваются продуктивные методы обучения будущих специалистов по защите информации и управлению информационной безопасностью. Автор приводит когнитивные методы обучения, такие как метод: эвристических вопросов, сравнений, фактов, исследований, конструирование понятий, конструирование правил, прогнозирование, ошибок, метод «Что будет, если...?».

Ключевые слова: методы обучения, продуктивные методы, когнитивные методы.

За нестандартною класифікацією методів навчання, яку запропонував А. Хуторський [1] методи навчання умовно складаються з трьох груп: 1. *методів продуктивного навчання*; 2. *евристичних методів*; 3. *системи занять, що утворені шляхом трансформації методів навчання до рівня форм навчання*.

Для сприяння особистісно-орієнтованого та діяльнісного творчого навчання розглянемо використання продуктивних методів та прийомів, з урахуванням специфіки їх застосування саме для майбутніх фахівців в галузі захисту інформації та управління інформаційною безпекою.

Продуктивні – значить необхідні, діяльнісні, міцні, постійно актуальні, сформовані на належному рівні засвоєння знань та умінь. «Продуктивна технологія виділяє головне, дає потрібне, програмує успіх і гарантує якість, а тому стає найбільш затребуваною» [2, с. 5].

Навчання, що ґрунтується на продуктивній орієнтації професійної освіти, спирається на такі види діяльності, які дозволяють студентам: а) пізнавати навколишній світ (*когнітивні методи*), б) створювати при цьому освітню продукцію (*креативні методи*), в) організовувати освітній процес (*методи організації діяльності*) відносять до продуктивних методів навчання.

Методологічний підхід до з'ясування сутності методів навчання як багатоякісного, багатовимірного явища, який має різні сторони прояву, розділяють вітчизняні (А. Алексюк, Н. Бібик, В. Бондар, С. Бондар, В. Вихрущ, В. Лозова, І. Малафіїк, Л. Момот, Н. Мойсеюк, В. Паламарчук, І. Підласий, В. Онищук, О. Савченко) та зарубіжні (Ю. Бабанський, Д. Вількеєв, М. Левіна, І. Лернер, М. Махмутов, В. Сітаров, В. Оконь, М. Скаткін та ін.) дидакти. Проте, прагнучи до оптимального визначення, яке охоплювало б родові (загальні) і найбільш специфічні (суттєві) ознаки, в працях цих науковців не достатньо висвітлені продуктивні методи навчання. З огляду на специфіку професійної підготовки майбутніх фахівців із захисту інформації та управління інформаційною безпекою такі методи навчання зовсім не вивчені, тому **метою даної статті** є спроба розгляду продуктивних методів навчання майбутніх фахівців з інформаційної безпеки.

Ґрунтуючись на гуманістичній та діяльнісній парадигмі і враховуючи здобутки сучасної педагогічної теорії й методики професійної освіти, ми в якості **завдань цієї статті** взяли проблеми використання саме тих продуктивних методів навчання, які пов'язані з когнітивною складовою діяльності того, кого навчають.

Метод евристичних запитань був розроблений ще давньоримським педагогом та оратором Квінтіліаном. Для відшукання відомостей про якусь подію або об'єкт ставляться такі сім ключових запитань: Хто? Що? Навіщо? Де? Чим? Як? Коли?

Наприклад, при вивченні базової статті з теорії інформації Клода Шеннона «Теорія зв'язку у секретних системах» ставляться такі запитання: Хто впер-

ше пов’язав мову спілкування з імовірнісним процесом? Що таке надмірність мови? Навіщо вимірювати надмірність мови? Де можна використовувати статистичну структуру повторюваності букв? Чим характерна секретна система з позиції множини можливих повідомлень на множину можливих криптограм? Як, використовуючи імовірності можливих повідомлень і ключів, розкрити криптограму? Коли система має абсолютну секретність?

Парні сполучення наведених запитань породжують нове запитання, наприклад: Як – Коли? Наприклад: Як, використовуючи імовірності можливих повідомлень і ключів, розкрити криптограму? і Коли система має абсолютну секретність?

Відповідь на ці парні сполучення запитань студенти можуть найти самі, або при наймі піддивитися у автора самої статті: «Потрібно, щоб імовірності різних повідомлень, які отримані після перехоплення супротивником криптограми, дорівнювали б у точності імовірностям тих же повідомлень до перехоплення».

Як бачимо, відповіді на ці запитання та їх можливі сполучення породжують незвичні ідеї та вирішення стосовно об'єкта що досліджується, тому метод евристичних запитань має великі спонукальні можливості.

Метод порівнянь застосовується для порівняння: версій різних технічних систем захисту інформації; версій різних програмних систем захисту інформації; версій різних управлінських систем інформаційної безпеки; різних систем кодування інформації; різних систем шифрування інформації; версій різних студентів; версій студентів з класичними аналогами по захисту інформації або шифруванню, які були сформульовані великими вченими; різноманітних аналогів по витоку інформації, дешифруванню і таке ін.

Для навчання цього методу студентам пропонуються питання: 1) Що значить «порівняти»? 2) Чи завжди і все можна порівнювати? 3) Вкажіть, що, на вашу думку, не підлягає порівнянню, а після цього зробіть спробу порівняти те, що порівнювати не можна.

Метод фактів. Фізичні органи чуттів людини вимагають послідовного розвитку, це може бути підґрунтям в його пізнавальній діяльності, тому усвідомлене

володіння студентами пошуку фактів, відмінність їх від «не-фактів» – це один із шляхів досконалого творчого пошуку. Досвід показує, що студентам непросто відрізняти те, що вони бачать, чують, відчувають, від того, про що вони думають. Необхідність природного сприймання освітніх об'єктів за допомогою органів чуттів вимагає застосування методу фактів, перегляду та змін звичного змісту освіти.

Наприклад, трудно знайти підтвердження того, що не знаючи секрету можна розрахувати однобічну математичну функцію (вона використовується в криптографії) в зворотному напрямку за доступний для обчислень реальний час. Знаходження не тільки фактів підтвердження використання таких однобічних функцій, але й алгоритмів, які б давали можливість обчислити такі функції в прямому напрямку за секунди, а для обчислення в зворотному – місяців і років (або якщо зворотне обчислення взагалі можливе), дає «їжу» для мислення майбутньому фахівцю-криптологу, розвиває його творчі пошукові здібності, сприяє професійному саморозвитку. Щодо однобічних функцій, то деякі факти їх використання в криптографії уже знайдено: факторинг – процес пошуку співмножників (факторів) деякого цілого числа, добуток яких дає теж вихідне ціле число; використання дискретного алгоритму, еліптичних кривих та ін., але залишається безліч інших недосліджених математичних підходів та прийомів.

Метод досліджень. Вибирається об'єкт дослідження – у нашому випадку, об'єкт захисту інформації. Наприклад, методика шифрування тексту за системою Віженера. Студентам пропонується самостійно дослідити вибраний об'єкт за таким планом: мета дослідження – план роботи – достоїнства і недоліки методики – схема шифрування, надійність криптосистеми, нові факти – питання та проблеми, що виникли, версії відповідей, гіпотези – рефлексійні міркування – усвідомлені способи діяльності та результати – висновки.

Така алгоритмізація діяльності студентів жодною мірою не применшує їх творчості. Навпаки, послідовне виконання усіх перелічених кроків практично дає кожному майбутньому фахівцю в галузі захисту інформації неминучу можливість отримати свій власний освітній результат. За допомогою систематично-

го повторення алгоритмічних етапів дослідження викладач допомагає студентам збільшити обсяг і якість такого результату.

Метод конструювання понять. Формування у студентів понять, що вивчаються, починається з актуалізації уявлень, які вони вже мають. Порівнюючи та обговорюючи уявлення студентів про поняття, викладач допомагає довести їх до деяких узагальнених форм. Причому необов'язково до тих, що є у підручниках, або які уже загальноприйняті у сфері використання. Результатом такої роботи виступає колективний творчий продукт – спільно сформульоване визначення поняття, яке записують на дошці в якості висновку. Одночасно викладач пропонує студентам ознайомитися з іншими формулюваннями цього поняття, які наведені авторами різних підручників або навчальних посібників. Різні формулювання залишаються у конспектах студентів як умова їх особистого самовизначення щодо поняття, що вивчається.

Наприклад, при вивченні поняття «інформаційна безпека» багато студентів визначають цю дефініцію як «діяльність по запобіганню витоку інформації, яку захищають від несанкціонованих і ненавмисних впливів», або як «спроможність користувача інформації протистояти загрозам противника». Але ж, у процесі довгих дискусій та множини різних самовизначень студентів доводиться це поняття саме до базової основи – «стан»: «інформаційна безпека – це *стан* захищеності інформації, яка обробляється засобами обчислювальної техніки і автоматизованої системи, від внутрішніх і зовнішніх загроз» [3, с.40]. Таким чином, у майбутніх фахівців вимальовуються відмінні риси цього поняття, які зіставляються із ознаками іншого ключового слова – «діяльність», що являє фундаментальною основою іншого поняття – «інформаційний захист».

Метод конструювання правил. Правила можуть бути створені, або «відкриті» самими студентами. Для цього викладач вибудовує спеціальну систему запитань, завдань, підказок, тобто залучається зазначений алгоритм учбових направляючих дій, які залежать від поставленого завдання.

Наприклад, розбираючи «фибоначчієву» криптографію, що ґрунтується на застосуванні узагальнених «фибоначчієвих» Q_p-матриць для шифрування та

дешифрування вихідного повідомлення *A*, застосовують алгоритм: $A \times Q_p^n = E$. При множенні вихідної матриці *A* на матрицю Q_3 (Q_3-матриця 4-го порядку), одержують наступне співвідношення:

$$E = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_5 & a_6 & a_7 & a_8 \\ a_9 & a_{10} & a_{11} & a_{12} \\ a_{13} & a_{14} & a_{15} & a_{16} \end{pmatrix} \times \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a_1 + a_4 & a_1 & a_2 & a_3 \\ a_5 + a_8 & a_5 & a_6 & a_7 \\ a_9 + a_{12} & a_9 & a_{10} & a_{11} \\ a_{13} + a_{16} & a_{13} & a_{14} & a_{15} \end{pmatrix}$$

Порівнюючи вихідну матрицю з її шифрованим еквівалентом, викладач сам формулює правило, що дозволяє відразу одержати результат множення матриць: «Для множення вихідної матриці на Q_p-матрицю необхідно зрушити всі елементи вихідної матриці вправо на один стовпець і сформувати перші елементи кожного рядка шляхом додавання першого елемента кожного рядка вихідної матриці з її останнім елементом».

При дешифруванні, розглядаючи множення на зворотну матрицю $A = E \times Q_p^{-1}$, студенти уже самі формулюють подібне правило: «Для множення вихідної матриці на зворотну матрицю Q_p^{-1} необхідно зрушити всі елементи вихідної матриці вліво на один стовпець і сформувати останні елементи кожного рядка шляхом вирахування другого елемента кожного рядка вихідної матриці з її першим елементом».

Метод «Що буде, якщо...?». Цей метод ще називають *метод гіпотез*, тому що припускає висування гіпотез і розвивається під час виконання прогностичних завдань типу «Що буде, якщо... ?».

Студентам треба теоретично сконструювати версії відповідей на поставлене викладачем запитання або проблему. Спочатку необхідно вибрати підстави для конструювання версій. Ті, кого навчають, пропонують вихідні позиції або точки зору на проблему, засвоюють різноплановий підхід до конструювання гіпотез. Потім, спираючись на логіку та інтуїцію, навчаються найбільш повно й чітко формулювати варіанти своїх відповідей на запитання не тільки викладача, але й на свої власні.

Серед викладачів, що ведуть заняття у групах, де готують майбутніх фахівців із захисту інформації та управління інформаційною безпекою цей метод одержує ефективне використання, тому що в майбутній професійній діяльності таких фахівців напевно будуть виникати подібні питання. Адже з можливими погрозами на збереження конфіденційної інформації, випадковим чи ненавмисним втручанням у канали її передачі, охороною фізичних об'єктів інформаційного захисту та з іншими подібними проблемами, будуть постійно мати справу фахівці такого профілю.

Метод прогнозування відрізняється від методу гіпотез тим, що застосовується до реального процесу або дії, що планується. Наприклад, студентам пропонується дослідити поведінку усіх співробітників, які задіяні в охороні інформаційних об’єктів і показати стан захисту цього конфіденційного об’єкту. Студенти роблять спостереження та обчислення, використовують для цього комп’ютерну техніку із залученням спеціальних програм моделювання та прогнозування. Викладач пропонує їм показати, як будуть розвиватися події через конкретний інтервал часу. Студенти, спираючись на попередні спостереження, результати моделюючих програм та на власні прогностичні здібності, а також на закономірності, які при цьому були виявлені, докладають про стан захищеності, указують на слабкі місця, де може бути виток секретної інформації та пропонують шляхи удосконалення системи захисту. Через визначений час прогноз порівнюють з реальністю, проводиться обговорення результатів, робляться висновки.

Метод помилок. Помилка в цьому методі розглядається як джерело протиріч, феноменів, виняток з правил, джерело нових знань, які народжуються при протиставленні загальноприйнятих точок зору. Перш за все, цей метод передбачає зміну негативного ставлення до помилок, заміну його на конструктивне їх використання (псевдопомилок), для поглиблення освітніх процесів.

Увага до помилки може бути актуалізована не тільки з метою її виправлення, а й для з'ясування її причини, способів її припущення. Знаходження взаємозв'язків помилки з правильним рішенням стимулює евристичну діяльність студентів, веде їх до розуміння відносності та варіативності будь-яких знань.

Нагадаємо, що завдяки помилці, було зроблено відкриття явища радіоактивності.

Французький вчений А. Бекерель досліджував світіння речовин (солей урану), попередньо опромінених сонячним світлом. У лютому 1898 року він не міг провести чергове дослідження через хмарну погоду, але випадково поклав фотопластинку в шухляду столу, поклавши на неї зверху мідний хрест, який був покритий сіллю урану. Проявивши про усякий випадок пластинку два дні потому, він знайшов на ній почорніння у формі виразної тіні хреста; це означало, що солі урану створюють невідоме раніше випромінювання – радіоактивність.

Висновки та перспективи досліджень. При виборі продуктивних методів навчання необхідно враховувати такі чинники: можливості конкретних методів у реалізації поставлених цілей і завдань заняття, відповідність методів до специфіки навчального предмета, змісту й обраних форм організації навчання майбутніх фахівців з інформаційної безпеки.

Представлені вище когнітивні методи навчання – це тільки мала частина розв'язуваного комплексного завдання побудови цілісної системи використовуваних продуктивних методів навчання. У майбутньому потребують детального розгляду такі методи навчання, які пов'язані з чуттєво-пізнавальною діяльністю того, кого навчають, а саме: метод перевтілення, метод смислового бачення, метод символічного бачення.

Література

1. **Хуторской А.В.** Современная дидактика: Учебник для вузов. – СПб. : Питер, 2001. – 544 с.

2. **Подласый И.П.** Продуктивная педагогика: Книга для учителя.– М. : Народное образование, 2003. – 496 с.

3. **Термінологічний** довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнєцов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К. : ДУШКТ, 2007. – 365 с.

Kolyada M.G.

Productive methods of training of the future experts on protection of the information and management of information security

In article productive methods of training of the future experts on protection of the information and management of information security are considered. The author results cognitive methods of training, such as a method: heuristic questions, comparisons, the facts, researches, designing of concepts, designing of rules, forecasting, mistakes, a method «That will be, if...?».

Keywords: methods of training, productive methods, cognitive methods.

Відомості про автора

Коляда Михайло Георгійович – докторант Луганського національного університету імені Тараса Шевченка; кандидат педагогічних наук, доцент кафедри радіотехніки та захисту інформації Донецького національного технічного університету.