кУДК 004.421.2:378

Н.О. Маслова, канд. техн. наук, доц.
О.Л.Половинка, аспірант
Донецький національний технічний університет, м. Покровськ, Україна,
masgpp2@gmail.com

Застосування методів пошуку асоціацій при створенні тестів з інформаційної безпеки

Метод тестування є одним з інструментів підвищення якості знань. Це дуже важливо при вивченні основ інформаційної безпеки. Тестування дозволяє визначити початковий рівень знань студентів і прогрес після навчального курсу. В роботі використані дві методики - з контролем і без контролю ступеня оволодіння навчальним матеріалом. Виділено три етапи дослідження. На третьому пропонується застосування апріорного алгоритму для вибору тестових завдань контрольного тесту. Наведено схему алгоритму і результати його застосування. Показано, що використання інтелектуальних алгоритмів дозволяє скласти контрольний тест, в який включено максимальну кількість різноманітних питань з усіх досліджуваних тем. Використання модифікації методу пошуку асоціацій при формуванні контрольних тестових завдань дозволяє підвищити повноту висвітлення навчального матеріалу та рівень отриманих знань.

Ключові слова: тестування, якість знань, інформаційна безпека, контроль, навчальний матеріал, апріорний алгоритм

DOI: 10.31474/1996-1588-2019-1-28-47-53

Вступ

Забезпечення інформаційної безпеки - одна з актуальних проблем сучасності. В Україні розвитку цього напрямку приділяється значна увага. Удосконалюється законодавча база, розробляються і приймаються стандарти, розпочата активна підготовка фахівців з безпеки в багатьох вищих навчальних закладах.

Сучасною тенденцією для підтвердження цифровий грамотності є отримання сертифікатів ECDL. Це загальноприйнятий у ряді країн Європи і США стандарт, який підтверджує наявність знань і навичок в напрямку інформаційних технологій одного з трьох рівнів – початкового, поглибленого та професійного. Наявність сертифікату підтверджує факт володіння персональним комп'ютером і вміння користуватися поширеними програмними додатками. Важливим напрямком програми є питання забезпечення інформаційної безпеки, що включають навички зниження ризику від реалізації кіберзагроз, орієнтація на безпечні інформаційно-комунікаційні технології.

За результатами конкурсу 2018року Донецький національний технічний університет став учасником проекту "Еразмус +" Digital competence framework for Ukrainian teachers and other citizens" (598236-EPP-1-2018-1-LT-EPPKA2-CBHE-SP).

Основним завданням програми є підвищення цифрової (комп'ютерної) грамотності різних респондентів - в першу чергу, вчителів, а також і інших осіб: студентів, учнів, незайнятих верств населення.

Мета дослідження: підвищення цифрової грамотності з інформаційної безпеки, відповідність знань студентів міжнародним вимогам.

Завдання дослідження: пошук способів прискорення процесу навчання, поглиблення знань в області інформаційної безпеки.

Опис дослідження.

Дослідження складається з декількох етапів.

Перший - визначення початкового рівня знань студентів, які не мають попередньої підготовки в галузі інформаційної безпеки (пробне тестування).

Другий - освоєння навчального матеріалу дисциплін професійної орієнтації студентів і оцінювання ступеня його засвоєння. Особливістю другого етапу є можливість повторного, вже самостійного навчання, поки не буде досягнуто значення показника ступеня володіння навчальним матеріалом на рівні 0,6 або вище.

Третій - заключний, при проведенні якого використовуються як питання ECDL - тесту, розміщені на сайті організації, так і спеціально підготовлені питання, які передбачають поглиблені знання матеріалу.

На одному з етапів програми dComFra в межах All Digital Week було проведено пробне тестування студентів перших-третіх курсів IT-спеціальностей університету. Результати тестування і загальна зацікавленість проектом сприяли проведенню дослідження.

Тестування дозволяє [1]:

- визначити початковий рівень знань досліджуваної групи;

- виявити теми, які потребують детального вивчення через низькі показників володіння матеріалом;

- адаптувати необхідні матеріали в навчальному середовищі;

- активізувати процес пізнання.

В процесі визначення початкового рівня знань студентів (пробне тестування) був використаний так званий ICT security skills barometer, наведений в [2].

Питання тесту розбито на три розділи. Перший розділ дозволяє оцінити знання загальних принципів захисту даних. Другий аналізує наявність навичок роботи з Інтернетом і електронною поштою. Третій містить питання, пов'язані з використанням соціальних мереж. Загальна кількість питань тесту - тридцять п'ять. Особа, що відповідає на питання тесту, отримує бал в кожній з категорій і усереднену за результатами відповідей на питання всіх трьох розділів оцінку.

Студенти третього курсу проходили тестування на англійській мові (мова оригіналу тесту). Першому-другому курсу пропонувався варіант питань, переведених на українську або російську мову. Загальна тривалість тесту - 40 хвилин. Питання не вимагали спеціальних знань і розрахунків, орієнтовані на визначення загального уявлення про предмет дослідження, а саме – навичками з забезпечення інформаційної безпеки.

Характерними питаннями тесту є, наприклад:

- які методи захисту існують в операційній системі вашого персонального комп'ютера;

- який режим захисту можна включити на вашому смартфоні;

- з метою полегшення запам'ятовування пароля чи застосовуєте ви єдиний пароль для різних комунікаційних пристроїв наявних у вашому розпорядженні;

- чи включають ваші логін або пароль дату народження або будь-які інші пам'ятні дати, ім'я, прізвище тощо.

У дослідженні і пробному тестуванні прийняли участь 40 студентів першого курсу, 30 другого й 13 студентів 3-го курсу.

Найбільш проблемними виявилися питання банківської безпеки та парольного захисту носіїв інформації. Серед питань безпеки, пов'язаних з технічними засобами прийому-передачі інформації проблемними виявилися принципи застосування Bluetooth та призначення брандмауера. У розділі забезпечення безпеки програмного забезпечення проблемою виявився захист від небажаного програмного забезпечення.

В цілому за результатами першого етапу отримали 3, 6% відмінних оцінок, 78.6% добрих, 10,7% задовільних та 7,1% мали незадовільний результат.

71% надали правильну відповідь на 21 питання та більше. 8,4% не володіють знаннями з захисту інформації (рівень знань «дуже низький» - нижче за 35балів).

На другому етапі учасників дослідження було розбито на дві групи. Для однієї проводився контроль рівня володіння навчальним матеріалом за кожним розділом. При цьому, якщо результати тесту були незадовільними, студент повторно опановував матеріал, без доступу до нової теми.

Для другої групи пропонувалося послідовне вивчення матеріалу зі звичайним тематичним контролем, але без контролю ступеня володіння навчальним матеріалом. У цьому випадку студенти з будь-яким рівнем знань вивчали наступну тему.

Для вимірювання ступеня володіння навчальним матеріалом на кожному рівні у відповідності з [3] використовувався коефіцієнт:

$$K_\alpha = \frac{P_1}{P_2}$$

де P_1-кількість правильно наданих відповідей за темою Т для рівня α в процесі тестування;

P_2 - загальна кількість питань в тесті за темою Т на відповідному рівні.

Питання за іншими темами, що належать до більш низьких рівнів, в цей перелік не включаються, таким чином,

$$0 \le K_\alpha \le 1.$$

Оцінювання якості знань студента і формування оцінок виконувалося згідно таблиці 1.

Таблиця 1. Критерії оцінювання

$K_\alpha <= 0.6$	Незадовільно, перехід на наступний рівень не відбувається, потрібно самостійне вивчення матеріалу і повторне тестування
$0.6 < K_\alpha <= 0.73$	Якість знань задовільна
$0.74 < = K_\alpha < 0.90$	Знання мають рівень «добре»
$K_\alpha > = 0.9$	Рівень знань відмінний

Граничний рівень контролю був свідомо знижено до 60% (в порівнянні з рекомендованим, наприклад, в [3] 70%) з метою уніфікації шкали оцінювання знань і узгодження її з вживаною в вузі.

Процес навчання в групі з контролем рівня засвоєння навчального матеріалу відбувається наступним чином:

- студент включається в групу, якщо він має деякі базові знання на нульовому рівні засвоєння, оцінені в процесі попереднього тестування балом «задовільно», «добре» або «відмінно», за цими результатами він проходить на наступний рівень;

- студент вивчає новий навчальний матеріал, після чого проводиться перевірка засвоєння цього матеріалу і, якщо студент проходить цю перевірку

з коефіцієнтом більш 0.6, то він переходить до вивчення наступної теми.

- відбувається перевірка знань і, якщо він її проходить, перехід до вивчення третьої, четвертої тем й так далі.

Якщо необхідне значення коефіцієнту не досягнуто, перехід на наступний рівень не відбувається. Студент самостійно повторно вивчає матеріал і знову проходить тестування.

У групі зі звичайним тематичним контролем (без обмеження ступеня володіння навчальним матеріалом) студенти з будь-яким рівнем знань (коефіцієнтом К) після оцінювання вивчали наступну тему.

Графічно це відображено на рисунках 1 і 2.

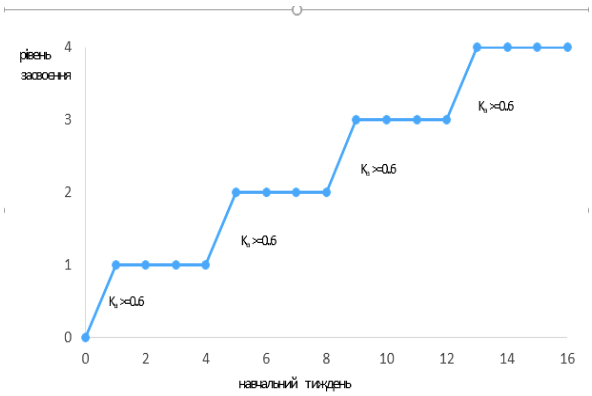

Рисунок 1 – Схема навчання в групі з контролем рівня засвоєння навчального матеріалу

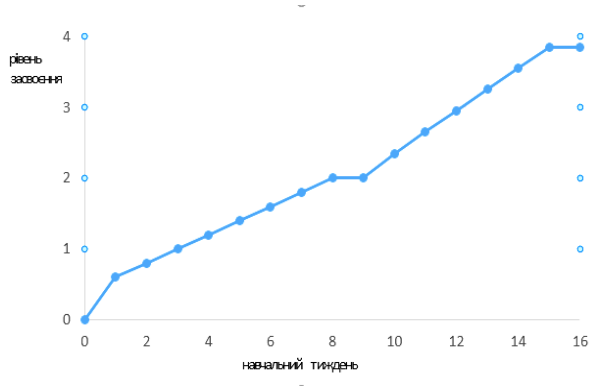

Рисунок 2 – Схема навчання в групі зі звичайним тематичним контролем

Дослідження другого етапу показали, що студенти, для яких проводився контроль рівня засвоєння навчального матеріалу опанували матеріал в більш короткі терміни (за 13 навчальних тижнів), у більшому обсязі й з більш високими показниками (середнє значення коефіцієнта $К_{СР1}$ = 0,87).

Результати другої групи - одну з тем курсу передано на самостійне вивчення. Середнє значення коефіцієнта $К_{СР2}$ = 0,74.

Однією з найбільш складних проблем третього етапу з'явився підбір тестових завдань і складання тестів різного рівня складності. Тестові завдання використовувалися для проведення поточного (навчального) і контрольного (семестрового) контролю.

Кожен тест отримує унікальний код, що складається з номерів модуля, теми, лекції, розділу, тестового питання і ознаки його складності (1 питання відкритої форми, 2-питання на відповідність, 3 - питання на послідовність, 4 - питання закритої форми).

Наприклад, m1t02L04r07q13h2.

У тестовому завданні питання комбінуються за складністю і за тематикою. Наприклад, для тестування обрані друга і третя теми. Загальний вигляд тестового завдання наведено в таблиці 2.

Таблиця 2. Кодування тестового завдання

1	m1t02L04r07q13h4	2	m1t03L09r02q11h4
3	m1t02L05r07q10h4	4	m1t02L05r07q09h3
5	m1t02L06r07q06h4	6	m1t03L09r07q02h3
7	m1t03L07r07q03h4	8	m1t02L06r07q04h2
9	m1t03L08r07q08h4	10	m1t03L08r07q10h2

Для повноти охоплення навчального матеріалу, уникнення ідентичності навчальних і контрольних тестів, використовують випадковий вибір тестових питань із заданого переліку за їх умовним номером. База питань загалом повинна значно перевищувати кількість питань у тесті та мати досить великий розмір [5].

Але навіть при базі питань значного розміру, є ймовірність появи як невикористаних, так і неодноразово повторюваних питань.

Це вимагає наявності якісного генератора випадкових чисел, що повинен відповідати певним вимогам, сформульованим в [4].

Але класичний підхід не враховує взаємопов'язаність питань і кількість самостійних «тренувальних» спроб навчального тестування.

Крім того, питання в рамках однієї теми логічно пов'язані між собою, що не враховується при випадковому доборі питань тесту, але може впливати на достовірність оцінки знань.

Це все складається в проблему, яку треба вирішувати на етапі вибору тестових завдань та включення їх у контрольний тест .

Комбінації питань, які зустрічалися при підготовці до контрольного тестування, відомі. Ставиться завдання вибрати питання, що найбільш рідко зустрічалися в навчальному тестуванні, побудувати їх набори та пов'язати структуру тесту з очікуваними результатами тестування. Останню вимогу слід розуміти так, що треба задовольнити необхідний рівень складності тестів та необхідний рівень знань навчального матеріалу з інформаційної безпеки.

Опис пропонованого методу.

Задача визначення наборів об'єктів, які часто зустрічаються у наборі даних відноситься до проблем побудови асоціативних правил. Існує досить

багато алгоритмів для генерації асоціативних правил. Найбільш відомі з них – алгоритми Apriori, Eclat, FP-Growth.

Методи пошуку асоціативних правил засовуються для знаходження типових шаблонів покупок (логістика), в криптографії (виявлення вторгнень), для пошуку інформації на веб-ресурсах (Web-mining), при вирішенні виробничих завдань (безперервне виробництво), для аналізу медичних та фармакологічних даних, застосовуються для інтелектуального аналізу даних, особисто, у продуктах Microsoft, у системі Oracle Data Mining. Досить новим є застосування асоціативних правил до аналізу даних навчального процесу вишу [6].

Пропонується використання методу Апріорі в учбовому процесі та застосування його для вибору тестових завдань для контрольних тестів з урахуванням питань, що вже було задано в процесі тестування, початкового рівня знань та вимог до його підвищення.

Загалом, апріорний алгоритм призначений для пошуку повторюваних наборів елементів і виявлення на їх основі взаємозв'язків в даних.

Під елементом в даному випадку розуміємо окреме тестове завдання, код якого записаний в комірку таблиці як показано вище.

Набір - це кілька елементів, тестових завдань, які зустрічаються одночасно в межах одного тесту.

Існує методично обґрунтована рекомендована кількість завдань у тесті. Ця кількість залежить від багатьох факторів. Наприклад, мети тестування, аудиторії, віку учасників тестувань, й т.д. Але загалом набір, а у даному випадку тест, може включати досить велику кількість завдань. Так, у [7] пропонуються тести з інформаційної безпеки, що включають від 150 до 450 питань. Апріорні алгоритми призначені для роботи з великими обсягами даних. У випадку, якщо довжина тесту становить 30 питань, то кількість можливих поєднань з 150 питань по 30 (без повторень) становить $32*10^{30}$, що обумовлює доцільність застосування методів пошуку асоціацій.

В якості послідовності обрані тестові завдання, які включаються в тест, але тільки ті з них, на які на протязі тренувальних спроб отримано вірні відповіді.

Фрагмент бази даних для обробки й виявлення кількості повторювань наведено в таблиці 3.

Таблиця 3. Фрагмент бази даних

код	Тестові питання
T1	m1t02L02r02q03h4
T2	m1t02L02r01q06h4, m1t02L02r01q07h2
T3	m1t03L03r02q03h1
T4	m1t02L02r01q08h4, m1t03L04r02q03h4, m1t04L06r01q05h3, m1t05L07r02q02h2

Робота методу типу Апріорі починається з відсіювання неінформативних значень у впорядкованої по спадаючій послідовності.

Спочатку розглядаються набори з одного елементу. На другій ітерації аналізують двох елементні набори. На третій – трьох елементні й так далі, поки алгоритм надає інформативні результати (формує правила).

Відсікання неінформативних значень у методі Апріорі виконується з застосуванням спеціальних показників. Це support (підтримка) і confidence (достовірність).

У нашому випадку підтримка характеризує, як часто конкретне тестове завдання застосовується у загальному обсязі тестових питань. Достовірність означає частоту виникнення подій. У базовому алгоритмі при завданні конкретних значень відсіваються набори, значення коефіцієнтів підтримки і достовірності для яких нижчі за відповідні порогові значення.

Якщо A – деякий набір елементів (тестових завдань), то підтримка набора елементів розраховується за формулою:

$$S(A)= N_s(A)/N,$$

де $N_s(A)$ – кількість рядків у таблиці, в яких застосовано тестове завдання A;
N – загальне число рядків в таблиці.

Допустимо, C(A→B) - достовірність правила виду A→B. Тоді формула визначення достовірності має вид:

$$C(A→B)= S(A→B)/ S(A).$$

Наприкінці кожної ітерації апріорний алгоритм поділяє набори елементів на дві групи - значення підтримки яких більше деякого попередньо заданого контрольного значення та ті, де це значення менш рівня підтримки.

Після виявлення наборів елементів Апріорний алгоритм залишає для подальшого застосування тільки ті з них, величина підтримки яких більше деякого наперед заданого контрольного значення, тобто ті, для яких виконується умова:

$$S(A)\geq pdr, \quad (1)$$

де *pdr* – мінімальне (контрольне, порогове) значення підтримки наборів елементів.

Процедура триває до тих пір, поки не будуть розглянуті всі набори різної, поступово зростаючої розмірності.

З наборів елементів, що залишилися після відсіву за умовою (1), будуються правила виду A → B. З числа цих правил відсіваються ті, для яких не виконується умова:

$$C (A \rightarrow B) \geq dst, \quad (2)$$

де dst - мінімальне значення достовірності правил.

Правила, які пройшли перевірку за умовою (2), є шуканими асоціативними правилами. Для цих правил роблять висновок про взаємозв'язок у вихідних даних і прогнозують значення наступного елементу даних.

У нашому випадку алгоритм був дещо модифіковано.

На першій ітерації відсікаємо елементи, рівень підтримки котрих не вище, а нижче заданого. Це дозволяє отримати перелік питань, що з'являлися у робочих тестах менш часто.

На другому етапі складаються пари неповторюваних питань так, щоб вони відносились до різних тем й мали різний рівень складності.

При цьому формуються правила, що дозволяють пропонувати включення в тест наступних питань.

Схема методу наведена на рис.3.

На схемі застосовано наступні позначення:

$A=\{A_1, A_2, A_3, \dots, A_i\}$ – безліч наборів елементів розмірності i, які знайдено для вхідних даних, тестових завдань. i (максимальна розмірність зі знайдених);

j – номер ітерації, на якій було знайдено i-елементний набір;

$R=\{R_1, R_2, R_3, \dots, R_k\}$ – безліч правил виду A→B, які отримано для A;

k– число знайдених правил.

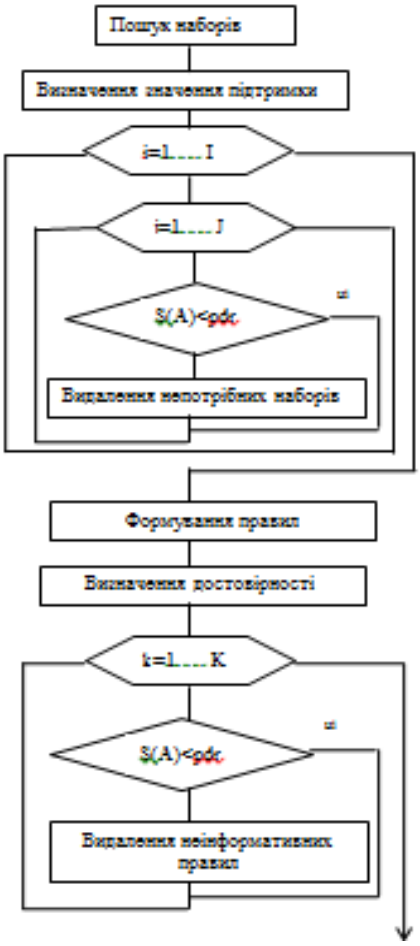

Рисунок 3 Схема методу

Нехай кількість питань, занесених до бази по кожній темі, фіксована і дорівнює A.

Задаємо рівень підтримки ptr, який вважаємо достатнім для оцінювання рівня знань за темою T.

Подальші дії:

Відкидання тих наборів, за якими в процесі навчального тестування правильні відповіді отримані більш ніж на M поставлених запитань.

Відкидання тих, за якими правильні відповіді отримані більш ніж на M-1 поставлених запитань (незалежно від черги їх слідування).

І так далі, поки у переліку не залишаться тестові питання, правильні відповіді на питання по яким отримані не більше ніж в 60% випадків. Далі робота з питаннями.

З решти відкидаються питання, на які відповіді були отримані i, i-1, ... раз, поки не отримаємо перелік питань, які не застосовувалися в процесі навчального тестування.

Перша ітерація методу апріорі – пошук питань, що не були застосовані в процесі учбового тестування.

Друга ітерація – пошук пар питань, що не випадали в учбових тестах

Третя ітерація – якщо перелік питань до конкретної теми ще не вичерпано, то створення таких трійок для контрольного тесту.

Якщо ввести в задачу параметр Y, який показує, скільки різних тестових завдань застосовано при складанні тестів, $Y_z=Sum(A_i)$ та Q – загальну кількість тестових питань, отримуємо значення параметру P, що відображає ступінь застосування тестового матеріалу: $P_z=Y_z/Q*100$. Результати побудови тестів з застосуванням алгоритму пошуку асоціативних правил (Y_2) та тестів без обробки методами інтелектуального аналізу даних (Y_1) для тестового матеріалу з 150 питань зібрано в Таблиці 4.

Таблиця 4 Повнота відображення учбового матеріалу

№ заміру	кількість, Y_1	%, Y_1	кількість, Y_2	%, Y_2
1	127	84,7	138	92,0
2	113	75,3	142	94,7
3	136	90,7	143	95,3
4	128	85,3	149	99,3
5	116	77,3	137	91,3
6	141	94,0	139	92,7
7	139	92,7	148	98,7
8	125	83,3	146	97,3
9	119	79,3	143	95,3
10	132	88,0	138	92,0
середнє	127	85,1	142	94,9

Таким чином, в експерименті без застосування методів інтелектуального аналізу у формуванні тестів було задіяно 127 питань з 150. В експери-

менті з застосуванням методу Apriori для обрання тестових питань для формування тестів було застосовано 142 питання з 150, що на 9,8% вище від першого випадку.

В результаті застосування апріорного алгоритму п'ятнадцять питань було обрано з тих, що у першому випадку не застосовувались. Якщо вважати, що кожне тестове питання охоплює конкретну кількість матеріалу без повторень, вдалося покращити повноту охоплення учбового матеріалу. Й, таким чином, забезпечити необхідний рівень знань з інформаційної безпеки.

Висновки

В процесі проведення досліджень було виконано наступне:

- визначено початковий рівень знань студентів першого – третього курсів з інформаційної безпеки;
- виявлено теми, які потребують детального вивчення через низькі показників володіння матеріалом;
- отримано дані щодо можливості збільшення обсягу навчального матеріалу у випадку постійного контролю рівня засвоєння навчального матеріалу;
- запропоновано застосування одного з методів пошуку асоціативних правил для вибору тестових завдань;
- отримано й проаналізовано експериментальні результати.

Застосування ідей і результатів дослідження призвело до поліпшення результатів навчання з дисципліни «Основи інформаційної безпеки» студентів другого і третього курсів непрофільних спеціальностей (опанували матеріалом в більш короткі терміни й отримали більш високі показники при бальному оцінюванні знань).

В той же час для студентів профільної спеціальності (кібербезпека) тестування стало контрольною точкою для коригування програми навчання.

Використання методу Апріорі при формуванні контрольних тестів дозволило виключити з них питання, що використовувалися для проміжного контролю й більш повно охопити учбовий матеріал при тестуванні. Безумовно, це поліпшило якість контролю знань та сприяло вирішенню проблеми формування різноманітних тестових наборів.

Загалом, для підвищення рівня успішності доцільно виявити аспекти, що мають на нього вплив, та встановити його характер. Тоді знаючи, що призводить до поліпшення успішності, а що - до її зниження, можна внести такі зміни в навчальний процес, які свідомо покращать його якість. Деякі аспекти, що впливають на успішність цілком зрозумілі і легко виявляються при експертному розгляді проблеми. Інші можуть бути непомітні на перший погляд, але мати істотний вплив на ефективність навчання. Такі, непомітні на перший погляд чинники можна виявити шляхом використання інтелектуального аналізу даних для дослідження та вдосконалення учбового процесу.

Автори вважають, що дослідження має елементи наукової новизни, яка полягає у пропозиціях щодо використання модифікації методу пошуку асоціацій при формуванні контрольних тестових завдань. Це дозволяє забезпечити повноту охоплення учбового матеріалу, й, безумовно, рівень отриманих знань студентів.

Запропонована схема може бути використана для підвищення рівня знань і прискорення вивчення навчальних курсів, що входять в програму навчання студентів технічного університету.

Список літератури

1. Біляковська О. О. Дидактика вищої школи : навч. посіб. / О. О. Біляковська, І. Я. Мищишин, С. Б. Цюра. – Львів : ЛНУ імені Івана Франка, 2013. – 360 с.
2. "ICT security skills barometer . Test your skills", available at: http://dev.ecdl.lt/project/eguardtest/index.php?lang=en
3. Дуплик С. В. Модели педагогического тестирования [Електронний ресурс] http://www.dupliksv.hut.ru/pauk/papers/testmodel.html
4. L'Ecuyer, Pierre. Random Number Generation // Springer Handbooks of Computational Statistics. - 2007. - С. 93 – 137
5. Методические рекомендации по процедуре проведения итогового тестирования. – Харьков: ХНУРЭ, 2003. – 31с.
6. Казмина И.И. Модификация априорного алгоритма для анализа данных учебного процесса вуза / И.И. Казмина, Е.В. Нужнов. Известия ЮФУ. Технические науки, 2016.- С.28-39
7. Глобальная система тестирований [Електронний ресурс] https://testserver.pro/index/pro/it/os

References

1. Bilyakovs′ka O. O. (2013). Didactics of food schools [Dydaktyka vyshchoyi shkoly: navch. posib. / O. O. Bilyakovs′ka, I. YA. Myshchyshyn, S. B. Tsyura. - L′viv: LNU imeni Ivana Franka, 360p.
2. "ICT security skills barometer. Test your skills", available at: http://dev.ecdl.lt/project/eguardtest/index.php?lang=en
3. Duplik S. V., "Modeli pedahohichnoho testuvannya", available at: http://www.dupliksv.hut.ru/pauk/papers/testmodel.html
4. L'Ecuyer, Pierre. (2007), Random Number Generation // Springer Handbooks of Computational Statistics, pp. 93 - 137
5. Metodychni rekomendatsiyi po protseduri provedennya pidsumkovoho testuvannya. - Kharkiv: KHNURE, 2003. - 31s.
6. Kazmina I.I., Nuzhnov E.V. (2016) "Modyfikatsiya apriornoho alhorytmu dlya analizu danykh navchal′noho protsesu vuzu" [Modification of the a priori algorithm for the analysis of the educational process of the university]. Yzvestyya PFU. Tekhnichni nauky, pp..28-39
7. "Hlobal′na systema testuvan", available at: https://testserver.pro/index/pro/it/os

Надійшла до редакції 01.10.2019

Н.А. МАСЛОВА, О.Л.ПОЛОВИНКА
Донецкий национальный технический университет, Покровск, Украина

ПРИМЕНЕНИЕ МЕТОДОВ ПОИСКА АССОЦИАЦИЙ ПРИ СОЗДАНИИ ТЕСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Метод тестирования является одним из инструментов повышения качества знаний. Это весьма важно при изучении основ информационной безопасности. Тестирование позволяет определить начальный уровень знаний студентов и прогресс после учебного курса. В работе использованы две методики - с контролем и без контроля степени овладения учебным материалом. Выделены три этапа исследования. На третьем предлагается применение априорного алгоритма для выбора тестовых заданий контрольного теста. Приведена схема алгоритма и результаты его применения. Показано, что использование интеллектуальных алгоритмов позволяет составить контрольный тест, в который включено максимальное количество разнообразных вопросов по всем изучаемым темам. Использование модификации метода поиска ассоциаций при формировании контрольных тестовых заданий позволяет повысить полноту охвата учебного материала и уровень полученных знаний

Ключевые слова: тестирование, качество знаний, информационная безопасность, контроль, учебный материал, априорный метод.

N. MASLOVA, O.POLOVINKA
Donetsk National Technical University, Pokrovsk, Ukraine

APPLICATION OF METHODS FOR SEARCHING ASSOCIATIONS WHEN CREATING TESTS FOR INFORMATION SECURITY.

The testing method is one of the tools to improve the quality of knowledge. This is very important in learning the basics of information security. Testing allows you to determine the initial level of students' knowledge and progress after the training course. Two methods were used in the work - with and without control of the degree of mastery of educational material. Three stages of the study are identified. The application of the Apriori algorithm to the selection of test tasks of the control test at the third stage are proposed. The scheme of the algorithm and the results of its application are given. It is shown that the use of intelligent algorithms allows you to create a control test, which includes the maximum number of diverse questions on all topics studied. Using a modification of the method of searching for associations in the formation of control test tasks can increase the completeness of the coverage of educational material and the level of knowledge gained.

Keywords: testing, quality of knowledge, information security, control, studying material, algorithm Apriori.