DẠY HỌC XÁC SUẤT THỐNG KÊ CHO HỌC VIÊN CHUYÊN NGÀNH TRINH SÁT KĨ THUẬT TẠI HỌC VIỆN KHOA HỌC QUÂN SỰ

NGUYỄN VĂN ĐẠI*

Ngày nhận bài: 16/10/2017; ngày sửa chữa: 08/11/2017; ngày duyệt đăng: 15/11/2017.

Abstract: *Probability and Statistics is a subject with very wide applicability in various fields and different ways. The article mentions application of the subject in teaching in the major Technical Reconnaissance. This major focuses on language research for use in cryptanalysis and decryption. Therefore, teaching contents of Probability and statistics in this major must be carefully considered. This article also explores the approaches to develop contents and proposes methods of teaching Probability and Statistics towards integration with professional practice to technical reconnaissance students at Military Science Academy in order to improve their practical skills.*

Keywords*: Probability and statistics, integration, cryptanalysis, decryption.*

1. Đặt vấn đề

Trong các học viện, trường đại học, việc dạy học môn toán cho học viên (HV) với mục đích chính là giúp HV nâng cao khả năng tư duy và biết vận dụng toán học như là công cụ để giải quyết các vấn đề thực tiễn (TT) nghề nghiệp (NN) ngay trong quá trình đào tạo cũng như khi đã bước vào công việc thực tế. Vì vậy nội dung dạy học môn toán cần phải gắn bó mật thiết với TT, trực tiếp với NN được đào tạo của HV, nhằm giúp HV phát triển được năng lực NN. Do đó, khi xây dựng chương trình môn học, vấn đề hàng đầu là cần phải xác định đâu là nội dung cần dạy, dạy cái gì và biện pháp giảng dạy nào hiệu quả nhất để giúp HV nhanh chóng và dễ dàng thực hiện công việc sau khi ra trường.

Để làm được điều đó thì người xây dựng nội dung chương trình môn học cũng như giảng viên tham gia giảng dạy cần phải nghiên cứu, tìm hiểu thật kĩ về mục tiêu đào tạo và đặc điểm NN của người được đào tạo để có định hướng đúng đắn.

2. Nội dung nghiên cứu

2.1. Một số cơ sở xác định nội dung dạy học môn Xác suất và thống kê (XSTK) tại Học viện Khoa học Quân sự (HVKHQS)

2.1.1. Nhiệm vụ, mục tiêu đào tạo tại Học viện Khoa học Quân sự

HVKHQS có nhiệm vụ đào tạo HV các ngành về Khoa học quân sự và ngoại ngữ phục vụ cho Quân đội. Một trong những nhiệm vụ hàng đầu của HVKHQS trong giai đoạn hiện nay là đào tạo và phát triển ngành Trinh sát kĩ thuật (TSKT). Trên tinh thần đó, HVKHQS đã xây dựng và tích cực thực hiện đề án "*Đổi mới quy trình, chương trình, nội dung đào tạo cán bộ các cấp tại Học viện, trong đó nòng cốt là đào tạo cán bộ chuyên ngành (CN) TSKT*". Với mục tiêu đào tạo đội ngũ HV, cán bộ chiến sĩ CN TSKT có phẩm chất bản lĩnh chính trị vững vàng, giỏi về chuyên môn nghiệp vụ, biết vận dụng linh hoạt kiến thức đã được đào tạo vào công việc cụ thể tại đơn vị.

Môn học *XSTK* được giảng dạy 45 tiết, thuộc khối kiến thức ngành, nhằm trang bị cho HV tri thức khoa học, phương pháp luận nghiên cứu, các kĩ năng, kĩ xảo của môn *XSTK,* góp phần nâng cao khả năng kết nối với môn học CN của HV, giúp HV giải một số bài toán liên quan đến thực tế và là công cụ hỗ trợ đắc lực cho các môn học CN như môn học về mật mã, thám mã và giải mã. Với vị trí môn học đó, yêu cầu XSTK phải phục vụ cho CN TSKT, nội dung phải gắn liền với CN TSKT, việc giảng dạy XSTK phải phù hợp với đối tượng người học, nội dung XSTK cần phải được lồng ghép, tích hợp với kiến thức CN.

2.1.2. Đặc điểm nghề nghiệp của học viên Trinh sát kĩ thuật

Công việc chính của người lính TSKT là thu thập thông tin đối phương, thám mã, giải mã tin tức thu thập được, phân tích số liệu, ra tin, báo cáo kết quả cho chỉ huy cấp trên. Để làm tốt công việc đó, HV CN TSKT cần được trang bị đầy đủ, hệ thống các tri thức cần thiết liên quan đến ngành nghề làm việc, như kiến thức về mật mã học, phân tích xử lí tin, toán học, ngôn ngữ học, công nghệ thông tin. Trong đó, lí thuyết XSTK có nhiều ứng dụng cho việc thực hiện yêu cầu nói trên.

Ngành TSKT chủ yếu nghiên cứu về ngôn ngữ phục vụ cho công việc giải mã, thám mã. Bởi vậy, XSTK của TSKT chủ yếu dùng để phân tích và nghiên cứu về ngôn ngữ, đối tượng của nó là ngôn ngữ (bản rõ và bản mã hóa). Do đó khi xây dựng chương trình môn học cần đặc biệt chú trọng đến yếu tố NN của HV, giảng dạy các kiến thức mà người học cần cho phát triển NN, khi lấy ví dụ, hệ thống bài tập hay các tình huống giả định bám sát hoặc trực tiếp với NN của người được đào tạo để tăng tính TT trong dạy học.

2.1.3. Thực trạng nội dung giảng dạy môn XSTK tại Học viện Khoa học Quân sự

*** Học viện Khoa học Quân sự**

Môn học XSTK được đưa vào chương trình giảng dạy cho HV CN TSKT từ năm 1998. Giai đoạn 1998-2014, môn học thuộc khối kiến thức giáo dục đại cương. Nhìn chung trong giai đoạn này, nội dung giảng dạy môn XSTK nhằm giúp HV tăng khả năng tư duy, kiến thức XSTK ít có sự liên hệ, kết nối với TT NN của HV.

Từ năm học 2015-2016 đến nay, môn học XSTK thuộc khối kiến thức ngành, yêu cầu nội dung giảng dạy tinh gọn, đảm bảo tính logic, hệ thống, nâng khả năng tư duy và có liên hệ mật thiết với CN đào tạo của HV, nội dung chương trình môn học được xây dựng theo định hướng phát triển năng lực NN của người học. Tuy nhiên giáo trình và nội dung giảng dạy hiện tại vẫn còn nhiều hạn chế, tính ứng dụng chưa cao, chưa khai thác hết các yếu tố XSTK trong CN đào tạo để đưa vào giảng dạy, dẫn đến sự tiếp thu và kết nối XSTK với CN của HV còn yếu. Điều tra, phỏng vấn 30 HV sau khi kết thúc học môn học CN, kết quả như sau:

Bảng 1. Điều tra về vai trò hỗ trợ và ứng dụng của môn XSTK đối với môn học CN TSKT

Thứ tự	Câu hỏi điều tra	Kết quả
1	Nội dung môn XSTK giảng dạy hiện tại có phù hợp với nhận thức của HV?	Dễ tiếp thu: 90% Khó tiếp thu: 10%
2	Lí thuyết XSTK có cần thiết đối với CN học hay không?	Cần thiết: 100% Không cần thiết: 0%
3	Nội dung môn XSTK giảng dạy hiện tại đã đáp ứng mục tiêu hỗ trợ môn học CN và công việc thực tế chưa?	Đã đáp ứng mục tiêu hỗ trợ: 30% Chưa đáp ứng mục tiêu hỗ trợ: 70%
4	Có cần thiết đổi mới nội dung giảng dạy môn XSTK theo hướng gắn với TT CN đào tạo?	Cần thiết: 100% Không cần thiết: 0%
5	Ý kiến khác	Đưa thêm các ví dụ liên hệ với TT CN đào tạo, khai thác các yếu tố XSTK trong các môn học CN và xây dựng lí thuyết theo hướng tích hợp với CN đào tạo.

Kết quả điều tra cho thấy, tất cả HV đều nhận thức được vai trò của lí thuyết XSTK trong cuộc sống cũng như trong CN học. Tuy nhiên, 70% HV cho rằng, nội dung môn XSTK giảng dạy hiện tại chưa đáp ứng mục tiêu hỗ trợ cho môn học CN và công việc thực tế, nhiều ý kiến nhận xét nội dung lí thuyết đưa vào giảng dạy chưa khai thác hết các yếu tố XSTK trong CN, cần lấy thêm nhiều ví dụ và bài tập liên hệ với TT hơn nữa.

2.2. Sơ lược về lí thuyết thông tin và vai trò của XSTK trong lí thuyết thông tin

Lí thuyết thông tin là một nhánh của toán học ứng dụng và kĩ thuật điện nghiên cứu về đo đạc lượng thông tin. Lí thuyết thông tin được xây dựng bởi C.E Shannon để xác định giới hạn cơ bản trong các hoạt động xử lí tín hiệu chẳng hạn như nén dữ liệu hay lưu trữ và truyền dẫn dữ liệu. Ngay từ những ngày đầu, nó đã mở rộng phạm vi ứng dụng ra nhiều lĩnh vực khác, bao gồm suy luận thống kê, xử lí ngôn ngữ tự nhiên, mật mã học,...

Lí thuyết thông tin nằm ở phần giao nhau giữa toán học, thống kê, khoa học máy tính, vật lí và kĩ thuật điện. Các ngành hẹp quan trọng của lí thuyết thông tin bao gồm mã hóa nguồn, mã hóa kênh, lí thuyết thông tin thuật toán, mật mã, thám mã, giải mã.

Trong hệ thống truyền tin trên, để dạy lí thuyết XSTK cho HV CN TSKT ta quan tâm đến các khối về lí thuyết mã (LTM) như mã hóa, thám mã và giải mã.

Trong LTM, thì lí thuyết về XSTK có vai trò hết sức quan trọng. Nhờ những ứng dụng của lí thuyết XSTK mà ta có thể đánh giá được chất lượng của một hệ thống mã hóa, hoặc khảo sát, đánh giá nguồn tin trước khi có những bước xử lí tiếp theo. Một số ứng dụng trực tiếp của lí thuyết XSTK trong LTM đó là: Sử dụng XSTK để tính tần suất xuất hiện các chữ cái trong mỗi ngôn ngữ, tính chỉ số trùng hợp của xâu văn bản, sử dụng XSTK để tính độ bất định của thông tin (Entropy), ứng dụng XSTK vào lập mã nén dữ liệu như mã nguồn thống kê tối ưu của Shannon và Huffman, ứng dụng XSTK để tham mã và giải mã mật, ...

2.3. Các biện pháp dạy học XSTK cho học viên chuyên ngành Trinh sát kĩ thuật tại Học viện Khoa học Quân sự

2.3.1. Cung cấp, hoàn thiện kiến thức về môn học XSTK theo hướng gắn với LTM:

- Trang bị cho HV vốn kiến thức cơ bản, cốt lõi về bộ môn XSTK: Dạy học phần XSTK, trên cơ sở đảm bảo các nội dung kiến thức và thời gian quy định, giảng viên cần phải chọn lọc và tìm hiểu xem thực tế NN hoặc các môn CN thường xuyên sử dụng những nội dung nào mà XSTK có, từ đó lựa chọn các ví dụ hướng tới bản chất và ứng dụng của XSTK đối với LTM, không nên quá sa đà vào việc dạy học dàn trải; không trọng tâm; không định hướng hiểu biết NN.

- Tăng cường mối quan hệ liên môn giữa kiến thức XSTK với kiến thức LTM: Do phân phối chương trình môn học, các môn học CN thường học sau các học phần về toán, do đó cần phải xây dựng kiến thức liên môn để HV định hướng được những kiến thức XSTK nào hỗ trợ cho môn học kế tiếp hoặc sử dụng kiến thức XSTK trực tiếp vào công việc thực tế. Để tăng cường mối quan hệ liên môn ta dạy trực tiếp các ứng dụng của lí thuyết XSTK vào LTM, chẳng hạn:

+ Ứng dụng XSTK để tính tần suất xuất hiện các chữ cái trong ngôn ngữ.

Nhiều kĩ thuật thám mã sử dụng đặc điểm thống kê của tiếng Anh, trong đó dựa vào tần suất xuất hiện của 26 chữ cái trong văn bản thông thường để tiến hành phân tích mã.

Becker và Piper đã chia 26 chữ cái thành năm nhóm và chỉ ra xác suất của mỗi nhóm như sau: +) E, có xác suất khoảng 0,120; +) T, A, O, I, N, S, H, R, mỗi chữ cái có xác xuất nằm trong khoảng từ 0,06 đến 0,09; +) D, L, mỗi chữ cái có xác suất xấp xỉ 0,04; +) C, U, M, W, F, G, Y, P, B, mỗi chữ cái có xác suất nằm trong khoảng từ 0,015 đến 0,023; +) V, K, J, X, Q, Z, mỗi chữ cái có xác xuất nhỏ hơn 0,01; +) Ngoài ra, tần suất xuất hiện của dãy hai hay ba chữ cái liên tiếp được sắp theo thứ tự giảm dần như sau: TH, HE, IN, ER ... THE, ING, AND, HER...

Bảng 2. Bảng phân phối tần suất xuất hiện các kí tự trong tiếng Anh

Kí tự	Xác suất	Kí tự	Xác suất	Kí tự	Xác suất	Kí tự	Xác suất
A	0,082	H	0,061	O	0,075	V	0,010
B	0,015	I	0,070	P	0,019	W	0,023
C	0,028	J	0,002	Q	0,001	X	0,001
D	0,043	K	0,008	R	0,060	Y	0,020
E	0,127	L	0,040	S	0,063	Z	0,001
F	0,022	M	0,024	T	0,091		
G	0,020	N	0,067	U	0,028		

+ Tính chỉ số trùng hợp của xâu văn bản

Trong khám phá mật mã, chỉ số trùng hợp (hay còn gọi là chỉ số trùng khớp) là kĩ thuật đặt hai văn bản bên cạnh nhau và đếm số lần mỗi chữ cái xuất hiện cùng một vị trí trong hai văn bản. Tìm chỉ số trùng lặp với mục đích dự đoán, suy xét xem văn bản ấy thuộc lĩnh vực nào để định hướng khám phá mã.

Chỉ số trùng hợp trong một xâu văn bản Latin: Giả sử x = $x_1x_2...x_n$ là một xâu kí tự. Chỉ số trùng hợp của x (kí hiệu là $I_c(x)$) được định nghĩa là xác suất để hai phần tử ngẫu nhiên của x là đồng nhất. Nếu kí hiệu các tần số của các kí tự của bảng chữ cái trong x tương ứng là $f_0, f_1,..., f_N$, (N số kí tự trong bảng chữ cái) ta có công thức ước lượng chỉ số trùng hợp là:

$$I_c(x) = \frac{\sum_{i=0}^{N-1} f_i(f_i - 1)}{n(n-1)}.$$

Chỉ số trùng hợp của hai xâu văn bản Latin: Giả sử x = $x_1x_2...x_n$ và y = $y_1y_2...y_n$, là các chuỗi có n và n› kí tự tương ứng. Chỉ số trùng hợp tương hỗ của x và y (kí hiệu là $MI_c(x, y)$) được xác định là xác suất để một phần tử ngẫu nhiên của x giống với một phần tử ngẫu nhiên của y. Nếu ta kí hiệu tần số xuất hiện của các kí tự của bảng chữ cái trong x và y lần lượt là $f_0, f_1,..., f_N$ và $f›_0, f›_1,..., f›_N$ (N là số kí tự của bảng chữ cái) thì $MI_c(x, y)$ sẽ được tính theo công thức:

$$MI_c(x,y) = \frac{\sum_{i=0}^{N-1} f_i f_i'}{nn'}$$

+ Ứng dụng XSTK để tính Entropy

Một khái niệm cơ bản của lí thuyết thông tin là số lượng của thông tin trong thông báo, gọi là nội dung thông tin, có thể xác định và đo được bằng đại lượng toán học. Thuật ngữ "nội dung" ở đây không liên quan gì đến nội dung của thông báo được truyền đi, mà là xác suất nhận được thông báo đã cho từ một tập hợp các thông báo có thể. Giá trị cao nhất đối với nội dung thông tin được gán cho thông báo có ít khả năng nhất, tức là có độ không xác định lớn nhất. Bởi vì độ không xác định của một phép thử càng lớn thì sự xác định kết quả của nó sẽ cho một thông tin càng lớn. Nếu thông báo được mong đợi với 100% chắc chắn thì nội dung của nó bằng 0, và khi đó độ không xác định của nó cũng bằng 0. Độ không xác định của thông tin còn được gọi là entropy.

Giả sử ta có một biến ngẫu nhiên X nhận các giá trị trên một tập hữu hạn theo một phân bố xác suất p(X). Thông tin thu nhận được bởi một sự kiện xảy ra tuân theo một phân bố p(X) là gì? Tương tự, nếu sự kiện còn chưa xảy ra thì cái gì là độ bất định về kết quả? Đại lượng này được gọi là entropy của X và được kí hiệu là H(X). H(X) được tính theo công thức sau: $H(X) = -\sum_{i=1}^{n} p_i . \log_2 p_i$. Nếu các giá trị có thể của X là $x_i, 1 \le i \le n$ thì ta có:

$$H(X) = -\sum_{i=1}^{n} p(X = x_i).\log_2 p(X = x_i).$$

Đại lượng entropy có ứng dụng rộng rãi trong nhiều lĩnh vực. Trong lĩnh vực mật mã học, việc ứng dụng entropy vào khảo sát bản mã trong một số tình huống cụ thể như: Có một đại lượng ngẫu nhiên X nhận các giá trị trên tập {a,..., z} theo một phân bố xác suất p(X) thì lượng tin của nguồn X có phân bố xác suất là gì? Muốn vậy ta phải khảo sát emtropy H(X). Nguồn tin X qua phép mã hóa thành nguồn tin Y nhận giá trị trên tập {a,..., z} có lượng tin là gì? Muốn vậy ta cũng phải khảo sát entropy H(Y). Trên cơ sở khảo sát H(X), H(Y) để đánh giá các yếu tố liên quan của hệ mã, như: mã pháp, độ mật,... nhằm phục vụ cho quá trình khám phá mật mã.

+ Ứng dụng XSTK để thám mã và giải mã mật

Trong thám mã các hệ mã cổ điển, công việc ban đầu là thống kê tần suất xuất hiện các chữ cái và nghiên cứu cấu trúc ngôn ngữ để tiến hành khám phá. Do vậy trong quá trình giảng dạy nội dung về XSTK, GV có thể kết hợp dạy cho HV cách khám phá một số bài toán mật mã đơn giản dựa vào phương pháp thống kê tần suất (có thể đó là bài tập, GV hướng dẫn cách giải để HV tự làm hoặc chia nhóm thảo luận).

Ví dụ: Bài tập về thám mã hệ mã thay thế, với bản mã như sau [5]: EMGLOSUDCGDNCUSWYSFHNSFCYK DPUMLWGYICOXYSIPJCKQPKUGKMG OLICGINCG

ACKSNISACYKZSCKXECJCKSHYSXCGOIDPKZCN KSHICGIWYGKKGKGOLDSILKGOIUSIGLEDSPWZUG FZCNDGYYSFUSZCNXEOJNCGYEOWEUPXEZGAC GNFGLKNSACIGOIYCKXCJUCIUZCFZCCNDGYY SFEUEKUZCSOCFZCCNCIACZEJNCSHFZEJZEGM XCYHCJUMGKUCY.

Bản rõ (tác giả bài báo dịch): I MAY NOT BE ABLE TO GROW FLOWERS, BUT MY GARDEN PRODUCES JUST AS MANY DEAD LEAVES, OLD OVERSHOES, PIECES OF ROPE, AND BUSHELS OF DEAD GRASS AS ANYBODY'S, AND TODAY I BOUGHT A WHEELBARROW TO HELP IN CLEARING IT UP. I HAVE ALWAYS LOVED AND RESPECTED THE WHEELBARROW. IT IS THE ONE WHEELED VEHICLE OF WHICH I AM PERFECT MASTER.

2.3.2. Dạy lí thuyết mã hóa nguồn Shannon và Huffman

Trong các hệ thống truyền tin rời rạc, khi truyền các tín hiệu liên tục, tin tức phải thông qua một số phép biến đổi, thường đổi thành số nhị phân rồi mã hóa. Sự mã hóa tin tức nhằm mục đích tăng tính hiệu quả và độ tin cậy của hệ thống truyền tin. Để tăng tốc độ lập tin, dùng phép mã hóa để thay đổi tính chất thống kê của nguồn tin. Shannon và Huffman đã nghiên cứu đưa ra thuật toán mã hóa nén dữ liệu làm cho chiều dài trung bình từ mã tối thiểu để tăng hiệu suất truyền tin. Nguyên tắc cơ bản của LTM hóa nguồn Shannon và Huffman là dựa trên cơ sở độ dài từ mã n_i tỉ lệ nghịch với xác suất xuất hiện p_i. Nghĩa là các từ mã dài sẽ dùng để mã hóa cho các tin có xác suất xuất hiện nhỏ và ngược lại, tùy từng bản mã mà hiệu xuất nén có thể đạt tới trên 70%. Do vậy trong quá trình giảng dạy XSTK, giảng viên kết hợp giới thiệu hai thuật toán mã hóa của trên cho HV thực hành lập mã, qua đó HV thấy được ý nghĩa TT của môn học.

2.3.3. Dạy học tích hợp XSTK với LTM

Do thời lượng giảng dạy có hạn , nếu cứ thiết kế nội dung chương trình giảng dạy môn học thành các module rời rạc nhau, không có sự gắn kết nội dung giữa các học phần sẽ làm kém hiệu quả của quá trình đào tạo, gây lãng phí thời gian hoặc giảng dạy những vấn đề không bổ ích cho người học. Vì vậy khi thiết kế nội dung bài giảng, ta nên lồng ghép tích hợp các bài toán XSTK có nội dung của LTM và rèn luyện HV kĩ năng chuyển đổi bài toán XSTK vào bài toán LTM.

Ví dụ khi dạy về xác suất điều kiện và công thức Bayes để tính xác suất của một biến cố, ta đưa vào bài toán tìm mối liên hệ về phân bố xác suất của không gian bản rõ và khóa như sau.

Trong phần này ta giả sử rằng, một khoá cụ thể chỉ dùng cho một bản mã. Giả sử có một phân bố xác suất trên không gian bản rõ *P*. Kí hiệu xác suất tiên nghiệm để bản rõ xuất hiện là $p_P(x)$. Cũng giả sử rằng, khóa K được chọn theo một phân bố xác suất xác định nào đó. (Thông thường khoá được chọn ngẫu nhiên, bởi vậy tất cả các khoá sẽ đồng khả năng, tuy nhiên đây không phải là điều bắt buộc). Kí hiệu xác suất để khóa K được chọn là $p_K(K)$, khóa được chọn trước khi biết bản rõ. Bởi vậy có thể giả định rằng khoá K và bản rõ x là các sự kiện độc lập.

Hai phân bố xác suất trên *P* và *K* sẽ tạo ra một phân bố xác suất trên *C*. Thật vậy, có thể dễ dàng tính được xác suất $p_P(y)$ với y là bản mã được gửi đi. Với một khoá $K \in K$, ta xác định:

$C(K) = \{ e_K(x) : x \in P \}$, ở đây C(K) biểu thị tập các bản mã có thể nếu K là khóa. Khi đó với mỗi $y \in C$, ta có : $p_C(y)$

$$= \sum_{\{k:y\in C(k)\}} p_K(K)p_P(d_K(y)).$$

Nhận thấy rằng, với bất kì $y \in C$ và $x \in P$, có thể tính được xác suất có điều kiện $p_C(y \mid x)$. (Tức là xác suất để y là bản mã với điều kiện bản rõ là

x): $p_C(y|x) = \sum_{\{K:x\ =\ d_K(y)\}} p_K(K)$ $\sum p_K(K)$.

Bây giờ ta có thể tính được xác suất có điều kiện $p_P(x \mid y)$ (tức xác suất để x là bản rõ với điều kiện y là bản mã) bằng cách dùng định lí Bayes. Ta thu được công thức sau:

$$p_P(x/y) = \frac{p_P(x).\sum_{\{K:x=d_K(y)\}} p_K(K)}{\sum_{\{k:y\in C(k)\}} p_K(K)p_P(d_K(y))}$$

Các phép tính này có thể thực hiện được nếu biết được các phân bố xác suất.

Sau đây sẽ trình bày một ví dụ đơn giản để minh hoạ việc tính toán các phân bố xác suất này.

Ví dụ. Giả sử $P = \{a,b\}$ với $p_P(a) = 1/4$, $p_P(b) = 3/4$. Cho $K = \{K_1, K_2, K_3\}$ với $p_K(K_1) = 1/2$, $p_K(K_2) = p_K(K_3) = 1/4$. Giả sử $C = \{1,2,3,4\}$ và các hàm mã được xác định là $e_{K1}(a) = 1$, $e_{K1}(b) = 2$, $e_{K2}(a) = 2$, $e_{K2}(b) = 3$, $e_{K3}(a) = 3$, $e_{K3}(a) = 4$. Hệ mật này được biểu thị bằng ma trận mã hoá sau:

	a b
K_1	1 2
K_2	2 3
K_3	3 4

Tính phân bố xác suất p_C ta có:

$p_C(1) = p_K(K_1).p_P(d_K(1)) = p_K(K_1).p_P(a) = 1/2.\ 1/4 = 1/8$,

$p_C(2) = p_K(K_1).p_P(b) + p_K(K_2).p_P(a) = 1/2.3/4 + 1/4.1/4 = 3/8 + 1/16 = 7/16$

$p_C(3) = 3/16 + 1/16 = 1/4$, $p_C(4) = 3/16$

(Xem tiếp trang 60)

nguồn lực để thực hiện, hoàn thành có hiệu quả các nhiệm vụ học tập. Thông qua các hoạt động học tập, HS được trải nghiệm, được trực tiếp quan sát, thảo luận, giải quyết vấn đề, thực hành vận dụng kiến thức vào thực tế cuộc sống theo khả năng nhận thức, khả năng sáng tạo của mỗi cá nhân. Từ đó, những biện pháp sư phạm của người GV cần chú trọng đến việc tạo điều kiện cho HS học tập với nhau.

Bên cạnh đó, GV bộ môn cần khuyến khích, tạo điều kiện thuận lợi để HS vận dụng những nguồn nội lực sẵn có như hiểu biết, kinh nghiệm, vốn sống phong phú của các em vào thực hiện, giải quyết những nhiệm vụ học tập, các bài tập, vấn đề, tình huống đạo đức kinh doanh. Nguyên tắc này cần phải được thực hiện trong toàn bộ quá trình GDĐĐKD trong môn *GDCD* ở THPT, từ việc thiết kế chủ đề/bài dạy học, tổ chức các hoạt động dạy học cho đến việc đánh giá kết quả học tập của HS. Điều này sẽ giúp các em phát huy được cao nhất tính tích cực, chủ động cũng như khả năng sáng tạo trong quá trình học tập, đồng thời giúp HS hình thành thói quen huy động, kết nối, phát huy những nguồn nội lực sẵn có với bản thân với những tri thức mới khi giải quyết những vấn đề, nhiệm vụ, tình huống đạo đức do cuộc sống đã, đang và sẽ đặt ra.

* * *

Việc đảm bảo thực hiện đúng MTBH, lựa chọn nội dung GDĐĐKD phải gắn lí luận với thực tiễn, đảm bảo tính vừa sức, phát huy tính tích cực, chủ động và vốn kinh nghiệm thực tế của HS là những nguyên tắc có mối quan hệ thống nhất biện chứng với nhau và đều thúc đẩy hiệu quả cao trong quá trình GDĐĐKD nói riêng và dạy học môn *GDCD* nói chung, giúp HS hình thành, phát triển được những năng lực cần thiết. Do đó, để đảm bảo hiệu quả việc tích hợp GDĐĐKD trong môn *GDCD* ở trường THPT, GV bộ môn cần căn cứ vào những nguyên tắc nói trên để lựa chọn, sử dụng các biện pháp sư phạm sao cho phù hợp. ❑

Tài liệu tham khảo

[1] Bộ GD-ĐT (2006). *Sách giáo khoa Giáo dục công dân lớp 10,11,12*. NXB Giáo dục.
[2] Bộ GD-ĐT (2006). *Sách giáo viên Giáo dục công dân lớp 10,11,12*. NXB Giáo dục.
[3] Bộ GD-ĐT (2015). *Tài liệu tập huấn dạy học tích hợp ở trường trung học cơ sở, trung học phổ thông*. NXB Đại học Sư phạm.
[4] Vũ Đình Bảy (chủ biên, 2016).*Thiết kế bài dạy học môn Giáo dục công dân ở trường phổ thông*. NXB Đại học Huế.
[5] Nguyễn Mạnh Quân (2012).*Giáo trình đạo đức kinh doanh và văn hóa công ty*. NXB Đại học Kinh tế Quốc dân.

Dạy học xác suất thống kê...

(Tiếp theo trang 30)

Bây giờ ta đã có thể các phân bố xác suất có điều kiện trên bản rõ với điều kiện đã biết bản mã. Ta có :

$p_P(a \mid 1) = 1$, $p_P(b \mid 1) = 0$, $p_P(a \mid 2) = 1/7$, $p_P(b \mid 2) = 6/7$

$p_P(a \mid 3) = 1/4$, $p_P(b \mid 3) = 3/4$, $p_P(a \mid 4) = 0$, $p_P(b \mid 4) = 1$

2.3.4. Biện pháp 4: Cải tiến giáo trình, tài liệu dạy học môn XSTK theo hướng gắn với LTM

Mục tiêu của việc biên soạn, giáo trình tài liệu dạy học XSTK trước đây là đáp ứng chuẩn kiến thức, kĩ năng, yêu cầu chung cho các ngành nghề ở trình độ đại học. Nhưng dạy để HV CN TSKT phát triển tốt NLNN thì mục tiêu của việc biên soạn giáo trình, tài liệu dạy học phải thay đổi. Để đáp ứng chuẩn đầu ra của chương trình đào tạo và đạt được các mục đích đào tạo, trong quá trình dạy học, biên soạn giáo trình, tài liệu môn XSTK cho HV CN TSKT, GV cần nghiên cứu kĩ chương trình học, nội dung học của HV CN TSKT xem họ cần gì ở môn XSTK, XSTK phục vụ gì cho họ. Nếu GV thấy vùng kiến thức nào quy định trong nội dung chương trình môn học chưa thích hợp với định hướng hình thành và phát triển NLNN cho HV thì GV có thể cải tiến, điều chỉnh nội dung trong chương trình, giáo trình để cung cấp cho HV kiến thức thiết thực hơn.

3. Kết luận

Các biện pháp đã đề xuất có thể góp phần nâng cao hiệu quả dạy học cho HV CN TSKT tại HVKHQS, đặc biệt theo hướng gắn với thực tiễn lao động sau đào tạo. Đồng thời, các biện pháp đó giúp HV hứng thú hơn trong học tập, chủ động sáng tạo trong việc vận dụng kiến thức XSTK vào TT, từ đó tạo nền tảng vững chắc cho HV học tập các môn học CN tiếp theo. ❑

Tài liệu tham khảo

[1] Đặng Vũ Hoạt - Hà Thị Đức (2006). *Lí luận và dạy học Đại học*. NXB Đại học Sư phạm.
[2] Đặng Đức Thắng (2003). *Lí luận dạy học đại học quân sự*. NXB Quân đội nhân dân.
[3] Nguyễn Bình (2013). *Giáo trình Lí thuyết thông tin*. NXB Học viện Công nghệ Bưu chính Viễn thông.
[4] Nguyễn Bình (2003). *Giáo trình Mật mã học*. NXB Học viện Công nghệ Bưu chính Viễn thông.
[5] Douglas Robert Stinson (2005). *Cryptography: Theory and Practive*. Chapman and Hall/CRC Press.