ĐẢM BẢO AN NINH QUỐC GIA TRONG BỐI CẢNH CHUYỂN ĐỔI SỐ

ĐỖ XUÂN MƯỜI
Học viện Cảnh sát nhân dân

Nhận bài ngày 02/11/2025. Sửa chữa xong 15/12/2025. Duyệt đăng 23/12/2025.

Abstract

This article analyzes key challenges to national security amid the rapid digital transformation taking place in Viet Nam and globally. Comprehensive digitalization across economic, political, defense, and social security sectors has created significant opportunities for development but has also introduced emerging security risks, including cyberattacks, data breaches, information manipulation, disruption of essential services, and increased hostile activities in cyberspace. Based on this assessment, the paper proposes several strategic solutions to enhance national security protection in the digital transformation era: improving the legal and institutional framework for cybersecurity; investing in and modernizing digital infrastructure and security technologies; developing a highly qualified cybersecurity workforce; strengthening international cooperation; and raising digital safety awareness and skills across society.

Keywords: *Cyber security, digital transformation, information security, national security, solutions.*

1. Đặt vấn đề

Trong bối cảnh toàn cầu bước vào kỷ nguyên chuyển đổi số (CĐS) mạnh mẽ, mọi hoạt động của đời sống kinh tế - xã hội đang ngày càng phụ thuộc vào hạ tầng số, dữ liệu số và các nền tảng công nghệ mới. Quá trình này không chỉ mở ra cơ hội thúc đẩy tăng trưởng, đổi mới sáng tạo và nâng cao năng lực cạnh tranh quốc gia mà còn kéo theo nhiều thách thức lớn đối với an ninh quốc gia (ANQG). Không gian mạng đang trở thành "không gian chủ quyền" mới, nơi các mối đe dọa về an ninh diễn biến nhanh, khó đoán định và có tính xuyên biên giới. Tại Việt Nam, CĐS được xác định là động lực quan trọng để phát triển đất nước, hướng tới xây dựng Chính phủ số, kinh tế số và xã hội số. Tuy nhiên, quá trình số hóa toàn diện cũng mở rộng bề mặt tấn công, gia tăng nguy cơ lộ lọt dữ liệu, tấn công mạng, gián đoạn dịch vụ trọng yếu cũng như sự can thiệp, thao túng thông tin nhằm gây bất ổn xã hội. Các thế lực thù địch, tổ chức tội phạm công nghệ cao và các nhóm lợi ích có thể lợi dụng các lỗ hổng của hệ thống thông tin, trí tuệ nhân tạo (AI), điện toán đám mây hay mạng xã hội để tiến hành các hoạt động chống phá. Trong khi đó, nhận thức, năng lực bảo vệ an ninh mạng và an toàn thông tin của nhiều cơ quan, tổ chức còn chưa theo kịp tốc độ phát triển của công nghệ. Hệ thống pháp luật dù đã từng bước hoàn thiện nhưng vẫn cần tiếp tục cập nhật để phù hợp với các dạng tấn công mới, công nghệ mới và mô hình vận hành mới trong nền kinh tế số. Vì vậy, vấn đề đảm bảo ANQG trong bối cảnh CĐS đang đặt ra yêu cầu cấp thiết đối với Nhà nước, các doanh nghiệp công nghệ, tổ chức xã hội và từng cá nhân công dân. Việc nhận diện đúng tính chất, mức độ và xu hướng của các nguy cơ đe dọa, đồng thời xây dựng chiến lược, mô hình quản trị an ninh số phù hợp là điều kiện tiên quyết để bảo vệ chủ quyền quốc gia, tài sản số, dữ liệu công dân và duy trì ổn định chính trị - xã hội trong thời đại mới.

2. Nội dung nghiên cứu

2.1. Cơ hội đảm bảo an ninh quốc gia trong bối cảnh chuyển đổi số

2.1.1. Nâng cao năng lực bảo vệ an ninh quốc gia nhờ công nghệ hiện đại

Chuyển đổi số mang đến cơ hội lớn giúp các cơ quan chức năng ứng dụng công nghệ hiện đại để

Email: doxuanmuoit02@gmail.com

tăng cường khả năng giám sát, phát hiện và xử lý các mối đe dọa an ninh. Những công nghệ như AI, máy học (ML), phân tích dữ liệu lớn (Big Data) cho phép phát hiện hành vi bất thường trên hệ thống mạng nhanh hơn và chính xác hơn nhiều so với các phương pháp thủ công truyền thống. Chẳng hạn, hệ thống phân tích hành vi người dùng (UEBA) có thể nhận diện dấu hiệu xâm nhập tiềm ẩn qua các hành vi bất thường, từ đó cảnh báo sớm các cuộc tấn công mạng. Điều này giúp lực lượng an ninh phản ứng nhanh, giảm thiểu thiệt hại và nâng cao hiệu suất bảo vệ quốc gia [1, tr. 16].

2.1.2. Tăng cường khả năng quản lý nhà nước thông qua chính phủ điện tử và dữ liệu số

Việc xây dựng Chính phủ số và CĐS trong các cơ quan công quyền giúp nâng cao hiệu quả quản lý, điều hành và khả năng bảo vệ ANQG. Nhờ sử dụng cơ sở dữ liệu quốc gia, hệ thống quản lý tập trung và các nền tảng dùng chung, Nhà nước có điều kiện quản lý dân cư, quản lý biên giới, giám sát tội phạm và điều phối lực lượng chức năng hiệu quả hơn. Ví dụ: cơ sở dữ liệu quốc gia về dân cư kết nối với hệ thống căn cước công dân gắn chip giúp xác minh danh tính nhanh chóng, giảm nguy cơ gian lận, giả mạo giấy tờ, từ đó hỗ trợ phòng chống tội phạm, tội phạm mạng và đảm bảo an ninh nội địa. Những tiến bộ này giúp cơ quan nhà nước tối ưu hóa nguồn lực và tăng cường khả năng dự báo tình huống.

2.1.3. Thúc đẩy tự chủ công nghệ và củng cố sức mạnh quốc gia

Chuyển đổi số vừa là thách thức nhưng cũng mở ra cơ hội để quốc gia phát triển các công nghệ cốt lõi, giảm phụ thuộc vào nước ngoài. Việc đầu tư vào AI, chip bán dẫn, điện toán đám mây nội địa, 5G/6G và an ninh mạng giúp xây dựng năng lực tự chủ công nghệ, đây là nền tảng quan trọng đảm bảo chủ quyền số. Ví dụ: nhiều quốc gia đã phát triển dịch vụ đám mây nội địa đạt chuẩn quốc tế, vừa phục vụ cho doanh nghiệp trong nước vừa đảm bảo dữ liệu quốc gia không bị lưu trữ ở nước ngoài. Việc làm chủ công nghệ giúp quốc gia nâng cao tự lực, giảm nguy cơ bị kiểm soát bởi các tập đoàn xuyên quốc gia và tăng cường vị thế trên trường quốc tế [2, tr. 19].

2.1.4. Cơ hội phát triển ngành An ninh mạng và công nghiệp số trong nước

Nhu cầu bảo vệ an ninh mạng tăng mạnh tạo động lực thúc đẩy sự phát triển của ngành công nghiệp an toàn thông tin trong nước. Các doanh nghiệp công nghệ Việt Nam có cơ hội phát triển sản phẩm bảo mật "Make in Vietnam", cung cấp dịch vụ an ninh mạng, giải pháp bảo vệ dữ liệu, nền tảng điện toán đám mây và phần mềm phân tích rủi ro. Đây không chỉ là cơ hội kinh tế mà còn góp phần xây dựng sức mạnh ANQG từ khu vực tư nhân. Thực tế cho thấy nhiều doanh nghiệp trong nước đã phát triển thành công giải pháp giám sát an ninh thông tin toàn diện (SIEM) hoặc hệ thống phòng chống tấn công DDoS, cạnh tranh được với sản phẩm quốc tế. Điều này vừa tạo việc làm vừa góp phần củng cố "lá chắn số" quốc gia.

2.1.5. Nâng cao khả năng hợp tác quốc tế trong lĩnh vực an ninh mạng

Trong thời đại số, hợp tác quốc tế về an ninh mạng trở nên mạnh mẽ hơn nhờ khả năng kết nối toàn cầu. Quốc gia có thể tham gia mạng lưới chia sẻ thông tin về mối đe dọa mạng, mô hình ứng phó sự cố và công nghệ bảo mật. Nhờ dữ liệu phong phú từ nhiều nước, Việt Nam (hoặc bất kỳ quốc gia nào) có thể nhận cảnh báo sớm về mã độc mới, hình thức tấn công tinh vi hay nguy cơ xâm nhập từ các nhóm tin tặc quốc tế. Đây là cơ hội nâng cao năng lực an ninh mạng mà không cần nguồn đầu tư quá lớn. Hơn nữa, hợp tác quốc tế còn thúc đẩy việc xây dựng tiêu chuẩn an ninh mạng chung, giúp quốc gia dễ dàng tham gia vào chuỗi giá trị công nghệ toàn cầu một cách an toàn.

2.1.6. Ứng dụng AI và tự động hóa trong phòng thủ và phản ứng sự cố

AI và các công nghệ tự động hóa tạo cơ hội giúp lực lượng an ninh mạng cải thiện tốc độ xử lý sự cố. Trong môi trường số, các cuộc tấn công diễn ra trong tích tắc nên con người khó có thể phản ứng kịp thời bằng phương pháp truyền thống. Những công cụ AI có khả năng tự động phát hiện bất thường, khoanh vùng tấn công, khóa lỗ hổng hoặc cách ly hệ thống bị xâm nhập mà không cần đợi chuyên gia can thiệp thủ công. Ví dụ: hệ thống SOAR (Security Orchestration, Automation and Response) đã được nhiều quốc gia sử dụng để tự động hóa quy trình ứng phó sự cố, giảm thời gian phản ứng từ hàng giờ xuống chỉ còn vài giây. Điều này gia tăng đáng kể hiệu quả phòng thủ mạng quốc gia [3, tr. 25].

2.1.7. Thúc đẩy hình thành xã hội số an toàn và chủ động

Chuyển đổi số giúp nâng cao nhận thức cộng đồng về an toàn thông tin. Khi người dân sử dụng các dịch vụ trực tuyến, họ sẽ dần hình thành thói quen bảo mật như sử dụng xác thực hai lớp, kiểm tra thông tin trước khi chia sẻ hoặc cảnh giác trước các thủ thuật lừa đảo. Sự chủ động này giúp hình thành "lá chắn con người", hỗ trợ rất lớn cho ANQG. Ví dụ: khi người dân được cảnh báo về các cuộc gọi lừa đảo mạo danh cơ quan nhà nước, tỷ lệ nạn nhân giảm đáng kể, góp phần ngăn chặn tội phạm mạng ở cấp độ xã hội. Nhờ đó, quốc gia không chỉ dựa vào lực lượng chuyên trách mà còn xây dựng nền tảng an ninh từ chính cộng đồng.

2.1.8. Tối ưu hóa công tác dự báo, cảnh báo và hoạch định chính sách

Dữ liệu lớn và phân tích dữ liệu giúp cơ quan hoạch định chính sách dự báo chính xác hơn các xu hướng tội phạm, nguy cơ bất ổn xã hội hoặc các mối đe dọa quốc phòng - an ninh. Ví dụ: phân tích dữ liệu mạng xã hội có thể giúp phát hiện sớm làn sóng tuyên truyền chống phá hoặc thông tin giả có khả năng gây ảnh hưởng lớn. Những dự báo kịp thời này giúp cơ quan chức năng chủ động xây dựng phương án ứng phó, ban hành chính sách và cung cấp thông tin chính xác để ổn định xã hội. Đây là cơ hội lớn để nâng cao hiệu lực quản lý nhà nước và bảo vệ lợi ích quốc gia trong thời đại số.

2.2. Thách thức đảm bảo an ninh quốc gia trong bối cảnh chuyển đổi số

2.2.1. Gia tăng các cuộc tấn công mạng quy mô lớn và tinh vi

Một trong những thách thức nghiêm trọng nhất đối với ANQG hiện nay là sự gia tăng nhanh chóng của các cuộc tấn công mạng có chủ đích (APT), tấn công từ chối dịch vụ (DDoS) và xâm nhập hệ thống để đánh cắp dữ liệu. Những cuộc tấn công này không chỉ do các tổ chức tội phạm công nghệ cao mà còn có sự tham gia của các nhóm tin tặc nhà nước, hành động vì mục tiêu chính trị, kinh tế hoặc quân sự. Tính chất xuyên biên giới của không gian mạng khiến việc xác định nguồn gốc, thủ phạm và phương thức tấn công trở nên vô cùng khó khăn. Khi các cơ quan chính phủ, hạ tầng trọng yếu, ngân hàng, bệnh viện hay hệ thống điều khiển công nghiệp bị tấn công, hậu quả để lại không chỉ là thiệt hại kinh tế mà còn ảnh hưởng trực tiếp đến chủ quyền và ANQG [4, tr. 31].

2.2.2. Lộ lọt dữ liệu và nguy cơ mất kiểm soát tài nguyên số

Dữ liệu hiện được coi là "nguồn tài nguyên chiến lược" của quốc gia. Tuy nhiên, tình trạng thu thập, lưu trữ và xử lý dữ liệu trên nền tảng số ngày càng phổ biến kéo theo rủi ro lớn về lộ lọt hoặc bị đánh cắp dữ liệu. Không ít tổ chức quản lý dữ liệu nhạy cảm như dữ liệu dân cư, y tế, tài chính vẫn chưa đáp ứng các tiêu chuẩn an ninh đủ mạnh, tạo cơ hội cho tin tặc khai thác. Khi dữ liệu chiến lược rơi vào tay các tổ chức nước ngoài hoặc thế lực thù địch, chúng có thể bị sử dụng để phân tích hành vi, can thiệp chính sách, kiểm soát thị trường hoặc tiến hành chiến tranh thông tin. Đây là mối đe dọa ngày càng hiện hữu đối với mọi quốc gia trong thời đại số.

2.2.3. Chiến tranh thông tin và thao túng dư luận trên không gian mạng

Không gian mạng đang trở thành "mặt trận mới" của các hoạt động chiến tranh thông tin. Các thế lực thù địch lợi dụng mạng xã hội và các nền tảng số để phát tán thông tin giả, bóp méo sự thật, gây hoang mang dư luận hoặc kích động biểu tình, bạo loạn. Với tốc độ lan truyền nhanh và sức ảnh hưởng rộng, thông tin sai lệch có thể gây ảnh hưởng lớn đến ổn định chính trị, niềm tin xã hội và hình ảnh quốc gia. Sự phát triển của AI, đặc biệt là deepfake và nội dung tạo sinh, khiến việc phân biệt thật, giả trở nên khó khăn hơn, gia tăng mức độ phức tạp của các chiến dịch tuyên truyền chống phá.

2.2.4. Rủi ro từ sự phụ thuộc vào công nghệ nước ngoài

Trong bối cảnh CĐS, nhiều quốc gia trong đó có Việt Nam đang phụ thuộc vào các nền tảng công nghệ, thiết bị phần cứng và phần mềm từ các tập đoàn nước ngoài. Điều này tiềm ẩn nguy cơ về "cửa hậu" (backdoor), lộ lọt dữ liệu hoặc bị ngắt kết nối khi xảy ra xung đột địa chính trị. Bên cạnh đó, phụ thuộc vào công nghệ ngoại nhập khiến một quốc gia khó làm chủ chuỗi cung ứng công nghệ số, dễ bị tổn thương khi biến động thị trường hoặc bị tác động từ các chính sách kiểm soát công nghệ của các cường quốc. Vì vậy, xây dựng năng lực tự chủ về công nghệ cốt lõi trở thành yêu cầu cấp thiết để bảo đảm ANQG.

2.2.5. Hình thức tội phạm công nghệ cao ngày càng đa dạng

Tội phạm công nghệ cao đang phát triển với tốc độ tương ứng với sự bùng nổ của công nghệ số.

Các chiêu thức như lừa đảo trực tuyến, đánh cắp tài khoản ngân hàng, mã độc tống tiền (ransomware), chiếm đoạt dữ liệu và tấn công thông qua thiết bị IoT xuất hiện ngày càng nhiều. Mức độ chuyên nghiệp của tội phạm ngày càng cao, chúng thường xuyên sử dụng công nghệ mã hóa, VPN, AI hay các công cụ tấn công tự động để che giấu hành vi. Điều này khiến công tác điều tra và xử lý trở nên phức tạp hơn, đặt ra thách thức lớn cho lực lượng an ninh và cơ quan quản lý.

2.2.6. Hạ tầng số và hệ thống thông tin trọng yếu thiếu an toàn

Nhiều hệ thống thông tin trọng yếu quốc gia như điện lực, ngân hàng, giao thông, viễn thông, y tế… đang trong quá trình CĐS nhưng chưa hoàn toàn được thiết kế theo tiêu chuẩn an ninh mạng ngay từ đầu. Các thiết bị cũ, thiếu cập nhật hoặc sử dụng phần mềm không bản quyền là những lỗ hổng dễ bị khai thác. Khi các hệ thống này bị tấn công hoặc gián đoạn, hậu quả không chỉ ảnh hưởng đến kinh tế mà còn có thể dẫn đến khủng hoảng xã hội hoặc đe dọa an ninh, quốc phòng. Đây chính là lý do hạ tầng số an toàn được xem như một dạng "phòng tuyến quốc gia" mới trong kỷ nguyên số.

2.2.7. Hạn chế về nhân lực và nhận thức an ninh mạng

Một trong những điểm yếu lớn nhất của nhiều quốc gia đang phát triển là thiếu nguồn nhân lực có chuyên môn sâu về an ninh mạng. Trong khi đó, sự phát triển nhanh của công nghệ đòi hỏi nguồn nhân lực phải liên tục cập nhật kỹ năng mới. Không chỉ thiếu nhân lực chuyên trách, nhận thức của người dân và doanh nghiệp về bảo mật thông tin còn hạn chế. Việc sử dụng mật khẩu yếu, chia sẻ thông tin cá nhân tùy tiện hoặc truy cập các đường link độc hại vẫn diễn ra phổ biến, tạo môi trường thuận lợi cho tội phạm mạng hoạt động và gây ảnh hưởng rộng hơn đến ANQG.

2.2.8. Hành lang pháp lý chưa theo kịp tốc độ phát triển công nghệ

Mặc dù nhiều quốc gia đã ban hành Luật An ninh mạng, Luật Bảo vệ dữ liệu cá nhân và các quy định liên quan nhưng thực tế cho thấy pháp luật thường chậm hơn so với sự phát triển của công nghệ. Những vấn đề mới như AI tạo sinh, dữ liệu lớn, tài sản số, hạ tầng đám mây xuyên biên giới hay tiền mã hóa vẫn chưa được điều chỉnh đầy đủ. Khoảng trống pháp lý khiến việc xử lý các hành vi vi phạm trên không gian mạng gặp khó khăn, đồng thời hạn chế hiệu quả quản trị ANQG trong thời đại số.

2.3. Giải pháp nâng cao hiệu quả đảm bảo an ninh quốc gia trong bối cảnh chuyển đổi số

2.3.1. Hoàn thiện hành lang pháp lý về an ninh mạng và bảo vệ dữ liệu

Một trong những giải pháp quan trọng hàng đầu là tiếp tục hoàn thiện hệ thống pháp luật liên quan đến an ninh mạng, bảo vệ dữ liệu cá nhân và quản trị không gian mạng. Sự phát triển nhanh của công nghệ như AI, dữ liệu lớn, điện toán đám mây và Internet vạn vật khiến luật pháp hiện hành đôi khi không theo kịp thực tế. Vì vậy, các quy định pháp luật cần được cập nhật thường xuyên để bao quát các nguy cơ mới, đảm bảo việc xử lý vi phạm rõ ràng, minh bạch và khả thi. Ví dụ: Nghị định về bảo vệ dữ liệu cá nhân của Việt Nam đã đánh dấu bước tiến quan trọng nhưng để ứng phó với deepfake hay AI tạo sinh cần bổ sung thêm cơ chế kiểm soát chặt chẽ hơn. Một khung pháp lý đầy đủ sẽ tạo nền tảng vững chắc để ngăn chặn, xử lý và phòng ngừa các hành vi xâm phạm ANQG trên không gian mạng [5].

2.3.2. Đầu tư, củng cố và hiện đại hóa hạ tầng số trọng yếu

Hạ tầng số, bao gồm trung tâm dữ liệu, hệ thống điều khiển công nghiệp, mạng viễn thông và các nền tảng điện toán đám mây cần được thiết kế theo tiêu chuẩn an ninh cao ngay từ đầu. Các quốc gia phải ưu tiên phát triển hạ tầng số độc lập, có tính tự chủ để giảm phụ thuộc vào công nghệ nước ngoài. Ví dụ: việc xây dựng trung tâm dữ liệu quốc gia tại nhiều nước giúp đảm bảo dữ liệu dân cư, y tế, quốc phòng được lưu trữ trong lãnh thổ quốc gia, giảm nguy cơ bị truy cập trái phép từ bên ngoài. Đồng thời, việc triển khai các hệ thống giám sát an ninh mạng theo thời gian thực trong ngành Điện lực hoặc ngân hàng giúp phát hiện sớm và ngăn chặn tấn công mạng vào các lĩnh vực thiết yếu, tránh gây gián đoạn dịch vụ quy mô lớn.

2.3.3. Phát triển nguồn nhân lực an ninh mạng chất lượng cao

Nguồn nhân lực là yếu tố then chốt quyết định khả năng tự chủ trong bảo vệ ANQG. Các trường đại học, học viện và doanh nghiệp công nghệ cần phối hợp xây dựng chương trình đào tạo chuyên sâu về an ninh mạng, từ các kỹ năng cơ bản đến chuyên môn cao như phân tích mã độc, điều tra số (digital forensics) và

phòng thủ mạng nâng cao. Ví dụ: một số quốc gia đã triển khai mô hình Cyber Range - môi trường mô phỏng tấn công mạng để lực lượng an ninh luyện tập giúp nâng cao năng lực thực chiến. Bên cạnh đội ngũ chuyên gia cần nâng cao nhận thức an toàn thông tin cho toàn xã hội thông qua các chiến dịch truyền thông, khóa học miễn phí hoặc các hệ thống cảnh báo sớm dành cho người dân và doanh nghiệp nhỏ [6, tr. 8].

2.3.4. Tăng cường hợp tác quốc tế về an ninh mạng

Không gian mạng không có biên giới nên các mối đe dọa an ninh mạng mang tính toàn cầu, đòi hỏi các quốc gia phải hợp tác để chia sẻ thông tin, kinh nghiệm và hỗ trợ kỹ thuật. Việc tham gia các hiệp định quốc tế, diễn đàn an ninh mạng hoặc các mạng lưới CERT (đội ứng cứu sự cố) giúp quốc gia có cơ hội tiếp cận cảnh báo sớm về tấn công mạng. Ví dụ: nhiều nước Đông Nam Á đã phối hợp thông qua ASEAN CERT để trao đổi dữ liệu về mã độc mới và phương thức tấn công tinh vi. Hợp tác quốc tế không chỉ giúp nâng cao năng lực ứng phó sự cố mà còn góp phần xây dựng một môi trường mạng an toàn, đáng tin cậy và tuân thủ luật pháp quốc tế.

2.3.5. Xây dựng năng lực phát hiện và xử lý thông tin xấu độc trên mạng

Chiến tranh thông tin và thao túng dư luận trên không gian mạng ngày càng tinh vi, vì vậy cần xây dựng hệ thống giám sát, đánh giá và phân tích dữ liệu mạng xã hội theo thời gian thực. Các công cụ AI có thể được sử dụng để phát hiện thông tin giả, nội dung độc hại hoặc các chiến dịch truyền thông có tổ chức. Ví dụ: một số nền tảng trong nước đã phát triển thuật toán phát hiện tin giả bằng cách phân tích tốc độ lan truyền và mức độ bất thường của nguồn tin. Bên cạnh đó, lực lượng chức năng cần nâng cao kỹ năng truyền thông phản bác, cung cấp thông tin chính xác, kịp thời, tránh để khoảng trống thông tin bị lợi dụng nhằm gây hoang mang xã hội.

2.3.6. Khuyến khích doanh nghiệp công nghệ Việt Nam tham gia bảo vệ an ninh số

Doanh nghiệp công nghệ đóng vai trò quan trọng trong phát triển hệ sinh thái số an toàn, bền vững nên Chính phủ cần thúc đẩy chính sách hỗ trợ doanh nghiệp đầu tư vào các giải pháp an ninh mạng, bảo mật dữ liệu và công nghệ lõi (chip, AI, điện toán đám mây). Ví dụ: việc các doanh nghiệp trong nước xây dựng nền tảng điện toán đám mây nội địa giúp giảm nguy cơ rò rỉ dữ liệu qua biên giới và đảm bảo quy định pháp lý về an toàn thông tin. Đồng thời, doanh nghiệp cũng có thể hợp tác với cơ quan nhà nước trong việc triển khai hệ thống giám sát an ninh mạng quốc gia, qua đó tăng cường khả năng phòng thủ mạng trên quy mô lớn [7, tr. 61].

2.3.7. Nâng cao ý thức và kỹ năng an toàn thông tin cho toàn dân

Ngoài các giải pháp kỹ thuật và pháp lý, yếu tố con người vẫn là mắt xích quan trọng. Người dân và doanh nghiệp nhỏ thường là mục tiêu của tội phạm mạng vì thiếu kiến thức bảo mật. Do vậy, việc tổ chức các chương trình phổ biến kỹ năng như bảo vệ mật khẩu, nhận diện lừa đảo, tránh click vào đường link độc hại hay sử dụng xác thực hai lớp là cần thiết để hình thành "lá chắn" an ninh mạng từ cộng đồng. Ví dụ: nhiều quốc gia đã triển khai Tháng An toàn thông tin quốc gia, tổ chức hội thảo, khóa huấn luyện trực tuyến và chiến dịch truyền thông trên mạng xã hội để nâng cao nhận thức của người dân, qua đó giảm đáng kể tỷ lệ bị tấn công lừa đảo.

3. Kết luận

Chuyển đổi số đang mở ra một giai đoạn phát triển mới cho mỗi quốc gia, trong đó tài nguyên dữ liệu, hạ tầng số và công nghệ số trở thành trụ cột quan trọng của tăng trưởng kinh tế cũng như năng lực cạnh tranh quốc gia. Tuy nhiên, đi cùng với cơ hội là những thách thức chưa từng có tiền lệ đối với vấn đề ANQG, từ nguy cơ tấn công mạng quy mô lớn, đánh cắp hoặc thao túng dữ liệu, đến sự can thiệp từ bên ngoài vào các hoạt động chính trị, kinh tế - xã hội thông qua không gian mạng. Thực tiễn cho thấy bảo đảm ANQG trong thời đại số không chỉ là nhiệm vụ của riêng lực lượng chuyên trách mà là trách nhiệm chung của toàn xã hội. Điều này đòi hỏi một cách tiếp cận tổng thể, bao gồm: tăng cường năng lực quản trị an ninh số, phát triển hạ tầng số an toàn, đồng bộ, bền vững, hoàn thiện hành lang pháp lý phù hợp với tốc độ phát triển công nghệ; đồng thời xây dựng nguồn nhân lực chất lượng cao, nâng cao nhận thức an ninh mạng cho người dân, doanh nghiệp và cơ quan nhà nước. Đặc biệt, việc đảm bảo ANQG trong bối

cảnh CĐS cần được đặt trong tầm nhìn chiến lược dài hạn. Nhà nước phải chủ động đầu tư vào công nghệ cốt lõi, làm chủ dữ liệu, phát triển các nền tảng số quốc gia và các hệ thống phòng thủ mạng mạnh mẽ, hiện đại. Doanh nghiệp công nghệ phải trở thành lực lượng tiên phong trong đổi mới sáng tạo và đảm bảo an ninh, an toàn dữ liệu; các tổ chức xã hội và người dân phải có ý thức cao trong việc bảo vệ thông tin cá nhân và tham gia giữ gìn an ninh mạng. Có thể khẳng định CĐS chỉ thực sự thành công khi ANQG được bảo đảm vững chắc. Đó là nền tảng để xây dựng một đất nước số phát triển bền vững, chủ động, an toàn và tự cường, đồng thời khẳng định vị thế quốc gia trong thời đại số hóa toàn cầu.

Tài liệu tham khảo

[1] Bộ Công an (2022). *Báo cáo tổng kết công tác bảo đảm an ninh mạng và phòng, chống tội phạm công nghệ cao năm 2021-2022,* Hà Nội.

[2] Học viện Chính trị Quốc gia Hồ Chí Minh (2020). *An ninh phi truyền thống và vấn đề đặt ra đối với Việt Nam trong thời kỳ hội nhập số* (Giáo trình chuyên khảo).

[3] Nguyễn Văn Hưởng (2022). *Tăng cường năng lực an ninh mạng trong bối cảnh chuyển đổi số ở Việt Nam*. Tạp chí Công an nhân dân, tháng 5.

[4] Nguyễn Quang Trung (2022). *An ninh quốc gia trong kỷ nguyên số: Thách thức và giải pháp cho Việt Nam*. Tạp chí Quốc phòng toàn dân, tháng 6.

[5] Quang Phương, La Duy, Vũ Dung (2023). *Phát triển nguồn nhân lực để bảo vệ chủ quyền quốc gia trên không gian mạng, Bài 2: Nhân lực an ninh mạng - Sự thiếu hụt cả lượng và chất.* Nguồn: https://www.qdnd.vn/giao-duc-khoa-hoc/chuyen-doi-so/phat-trien-nguon-nhan-luc-de-bao-ve-chu-quyen-quoc-gia-tren-khong-gian-mang-bai-2-nhan-luc-an-ninh-mang-su-thieu-hut-ca-luong-va-chat-758367, ngày 29/12/2023.

[6] Quốc hội (2018). *Luật An ninh mạng*. Luật số 24/2018/QH14, ngày 12/6/2018.

[7] Trần Vi Dân (2019). *Tư duy mới về bảo vệ an ninh quốc gia.* Tạp chí Công an nhân dân, tháng 6.

PHÁT TRIỂN KỸ NĂNG DẠY HỌC NHẰM PHÁT TRIỂN NĂNG LỰC...

Tiếp theo trang 149

3.2. Kiến nghị

Trên cơ sở kết quả nghiên cứu, nhóm tác giả kiến nghị Trường Cao đẳng Sơn La cần tiếp tục quan tâm đổi mới nội dung và hình thức rèn luyện kỹ năng nghề nghiệp theo hướng PTNL, tăng cường hoạt động thực hành, lớp học mô phỏng và ứng dụng công nghệ trong đào tạo SV ngành GDMN. Đồng thời cần tăng cường phối hợp giữa trường sư phạm và các trường mầm non, mở rộng thời gian kiến tập, thực tập và tạo điều kiện để SV được tham gia trực tiếp vào các hoạt động giáo dục thực tiễn, qua đó nâng cao hiệu quả rèn luyện kỹ năng dạy học và năng lực nghề nghiệp cho SV. Kết luận và kiến nghị trên là cơ sở thực tiễn quan trọng để Trường Cao đẳng Sơn La tiếp tục đổi mới hoạt động đào tạo giáo viên mầm non theo hướng PTNL, đáp ứng yêu cầu của thời đại chuyển đổi số và giáo dục trong thế kỷ XXI.

Tài liệu tham khảo

[1] Bộ Giáo dục và Đào tạo (2018). *Thông tư số 29/2018/TT-BGDĐT, ngày 24/12/2018 quy định khối lượng kiến thức tối thiểu, yêu cầu về năng lực mà người học đạt được sau khi tốt nghiệp trình độ trung cấp, trình độ cao đẳng nhóm ngành đào tạo giáo viên; quy trình xây dựng, thẩm định và ban hành chương trình đào tạo trình độ trung cấp và trình độ cao đẳng nhóm ngành đào tạo giáo viên.*

[2] Bộ Giáo dục và Đào tạo (2024). *Thông tư số 01/2024/TT-BGDĐT, ngày 05/02/2024 ban hành chuẩn cơ sở giáo dục đại học.*

[3] Nguyễn Ánh Tuyết (2006). *Giáo dục học mầm non*. NXB Đại học Sư phạm, Hà Nội.

[4] Nguyễn Đức Quang (2015). *Đào tạo giáo viên mầm non theo định hướng phát triển năng lực*. NXB Đại học Sư phạm, Hà Nội.

[5] N.Đ. Lê-vi-tôp (1972). *Tâm lí học trẻ em và tâm lí học sư phạm* (Phạm Thị Diệu Vân dịch). NXB Giáo dục, Hà Nội.

[6] Nguyễn Thị Hồng Vân (2019). *Một số giải pháp nhằm nâng cao hiệu quả rèn luyện nghiệp vụ sư phạm theo chuẩn nghề nghiệp cho sinh viên ngành Giáo dục mầm non Trường Cao đẳng Sơn La*. Tạp chí Giáo dục, số 450, kỳ 2 tháng 3, tr. 29-32, 23.

[7] Nguyễn Thị Hồng Vân (2020). *Một số giải pháp phát triển năng lực tự học cho sinh viên ngành Giáo dục mầm non, Trường Cao đẳng Sơn La*. Tạp chí Giáo dục, số 475 kì 01 tháng 4, tr. 59-64.

[8] Quốc hội (2019). *Luật Giáo dục*. Luật số 43/2009/QH14, ngày 14/6/2019.

[9] Thủ tướng Chính phủ (2024). *Quyết định số 1705/QĐ-TTg ngày 31/12/2024 về phê duyệt chiến lược triển giáo dục đến năm 2030, tầm nhìn đến năm 2045*.

[10] Thủ tướng Chính phủ (2025). *Quyết định số 525/QĐ-TTg ngày 06/03/2025 ban hành kế hoạch thực hiện Chỉ thị số 29-CT/TW ngày 05/01/2024 của Bộ Chính trị về công tác phổ cập giáo dục, giáo dục bắt buộc, xóa mù chữ cho người lớn và đẩy mạnh phân luồng học sinh trong giáo dục phổ thông đến năm 2030.*

[11] Thái Duy Tuyên (2013). *Triết học giáo dục Việt Nam*. NXB Đại học Sư phạm, Hà Nội.