PHÁT TRIỂN NGUỒN NHÂN LỰC CHẤT LƯỢNG CAO VỀ AN NINH CÔNG NGHỆ Ở VIỆT NAM

★ **PGS, TS NGUYỄN THỊ TRƯỜNG GIANG**
Học viện Báo chí và Tuyên truyền

● ***Tóm tắt:*** ***Trong bối cảnh khoa học, công nghệ phát triển mạnh mẽ, những cuộc chiến thông tin và công nghệ gay gắt, việc bảo đảm an ninh công nghệ không chỉ liên quan đến cá nhân, hay tổ chức, doanh nghiệp mà còn là vấn đề chủ quyền, an ninh và lợi ích quốc gia. Vì thế, hầu hết các quốc gia trên thế giới, trong đó có Việt Nam rất quan tâm đến an ninh công nghệ, an ninh công nghệ trong an ninh mạng, đặc biệt là vấn đề nguồn nhân lực an ninh công nghệ. Bài viết làm sáng tỏ thực trạng, đồng thời phân tích, đánh giá xu hướng phát triển, nhu cầu về nguồn nhân lực chất lượng cao nhằm bảo đảm an ninh công nghệ trong an ninh mạng, trên cơ sở đó, gợi mở một số hàm ý chính sách cho Việt Nam. Bài viết là kết quả nghiên cứu trong khuôn khổ Đề tài cấp nhà nước KX04.32/21-25 "Vấn đề an ninh phi truyền thống, trọng tâm là an ninh mạng trong nền an ninh quốc gia".***

● ***Từ khóa: nguồn nhân lực chất lượng cao; an ninh công nghệ; an ninh mạng.***

1. Mở đầu

Cho đến nay, an ninh công nghệ là một khái niệm chưa có sự nhận thức thống nhất, tuy nhiên để hiểu về nó, có thể phân tích các thuật ngữ liên quan và đặt nó trong bối cảnh hiện tại, ở góc độ nghiên cứu an ninh mạng, an ninh phi truyền thống.

Luật Khoa học và công nghệ năm 2022 định nghĩa: "Công nghệ là giải pháp, quy trình, bí quyết kỹ thuật có kèm theo hoặc không kèm theo công cụ, phương tiện dùng để biến đổi nguồn lực thành sản phẩm". Công nghệ được xem như một thành tố quan trọng của xã hội con người, có vai trò thúc đẩy sự tiến bộ nói chung.

Về khái niệm an ninh, hiểu một cách đơn giản nhất, là khả năng giữ vững sự an toàn trước các mối đe dọa. An ninh công nghệ có thể coi là sự an toàn để công nghệ có thể phát triển và thực hiện vai trò thúc đẩy tiến bộ trong mọi lĩnh vực xã hội. Như vậy, *an ninh công nghệ là trạng thái an toàn, phát triển vững mạnh về công nghệ của quốc gia để tham gia hiệu quả vào các lĩnh vực quản lý đất nước, ứng phó với các nguy cơ an ninh quốc gia.*

2. Tầm quan trọng và thách thức đối với an ninh công nghệ hiện nay

Tầm quan trọng của an ninh công nghệ trong thế giới hiện đại, đặc biệt trong bối cảnh

Cách mạng công nghiệp lần thứ tư, có thể so sánh với tầm quan trọng của lĩnh vực an ninh quân sự trong an ninh truyền thống. Năng lực công nghệ là một trong những vũ khí bảo vệ đất nước trước những nguy cơ an ninh phi truyền thống, trong đó có an ninh mạng. Đứng trước những nguy cơ đến từ tội phạm công nghệ cao, không có cách nào khác hơn là phải bảo vệ an ninh quốc gia bằng một năng lực công nghệ vượt trội. Do vậy, bảo vệ an ninh và chủ quyền quốc gia trên không gian mạng là nhiệm vụ trọng yếu của mỗi quốc gia, không gian mạng được xem là một vùng lãnh thổ đặc biệt, được quản lý bằng chính sách, pháp luật và năng lực công nghệ. Vì lẽ đó, an ninh công nghệ trong nền an ninh mạng cũng là vấn đề đáng quan tâm.

Tầm quan trọng của an ninh công nghệ trong thế giới hiện đại, đặc biệt trong bối cảnh Cách mạng công nghiệp lần thứ tư, có thể so sánh với tầm quan trọng của lĩnh vực an ninh quân sự trong an ninh truyền thống. Năng lực công nghệ là một trong những vũ khí bảo vệ đất nước trước những nguy cơ an ninh phi truyền thống, trong đó có an ninh mạng. Đứng trước những nguy cơ đến từ tội phạm công nghệ cao, không có cách nào khác hơn là phải bảo vệ an ninh quốc gia bằng một năng lực công nghệ vượt trội.

Thách thức đối với an ninh công nghệ

Trong bối cảnh của cuộc Cách mạng công nghiệp lần thứ tư, những nguy cơ và thách thức trên không gian mạng tác động mạnh mẽ đến an ninh của mọi quốc gia. Những hoạt động xâm phạm an ninh quốc gia trên không gian mạng xuất hiện ngày càng phức tạp, ngay cả ở các quốc gia hàng đầu thế giới về khoa học và công nghệ. Đó là: chiến tranh mạng (dùng các công cụ "vũ khí" tấn công mạng để tấn công vào các website trọng yếu của cơ quan chính phủ, hệ thống ngân hàng,...), gián điệp mạng (tấn công vào các hệ thống máy tính để đánh cắp dữ liệu, bí mật thông tin hoặc chiếm quyền kiểm soát), khủng bố mạng (tấn công trên mạng nhằm mục đích khủng bố, sử dụng không gian mạng để đe dọa khủng bố), tội phạm mạng (xâm nhập bất hợp pháp trên không gian mạng, lấy cắp, sửa đổi, phá hoại dữ liệu và thông tin của người dùng, gây ra các thiệt hại nghiêm trọng)[1].

Rõ ràng, trong kỷ nguyên 4.0, những vũ khí được tạo ra bằng gõ bàn phím trên máy tính có thể gây ra những thiệt hại về kinh tế và xã hội, cả tính mạng con người, thậm chí có nguy cơ hủy diệt hàng loạt (nếu như tin tặc tấn công vào các cơ sở hạt nhân). Đó là những hậu quả thảm khốc mà không quốc gia nào có thể đứng ngoài cuộc. Nguy hiểm hơn nữa, trong tình hình chính trị thế giới phức tạp hiện nay, không chỉ có những lực lượng tin tặc hoặc cực đoan tiến hành tấn công mạng, mà để trả đũa chính trị, chính quyền nhiều nước cũng sẵn sàng sử dụng sức mạnh công nghệ của mình để tấn công đối phương.

Những nguy cơ an ninh mạng này xuất phát từ nhiều nguyên nhân, trong đó có nguyên nhân đến từ thách thức an ninh công nghệ liên quan đến không gian mạng. Các thách thức đó được chia thành 3 dạng thức: thách thức về kỹ thuật; thách thức về cơ chế, chính sách; thách thức về nguồn nhân lực (con người).

Về mặt kỹ thuật, thách thức công nghệ phải đối mặt là: *Một*, lỗ hổng bảo mật - lỗ hổng này là cái tự thân, vốn có của bất kỳ hệ thống (nền tảng) nào trên không gian mạng. Quá trình

Đội Cảnh sát phòng chống tội phạm sử dụng công nghệ cao, Phòng Cảnh sát kinh tế Công an Quảng Ninh _ Ảnh: congan.quangninh.gov.vn

phát hiện lỗ hổng là cuộc chạy đua giữa những nhà bảo đảm an toàn công nghệ với hacker (những kẻ tấn công mạng); và trên thực tế, khi phát hiện lỗ hổng, báo cáo lên đơn vị sở hữu hệ thống thì thường đã quá muộn do hacker đi trước, đã phát hiện và lợi dụng lỗ hổng để tấn công mạng. *Hai,* phần mềm mục đích gây hại được cài vào thiết bị, hoặc hệ thống (nền tảng mạng xã hội) một cách tinh vi, khó phát hiện, không hiện hữu ngay mà chờ thời điểm kích hoạt... *Ba,* sự phát triển của những thiết bị công nghệ cao cũng tạo điều kiện cho tội phạm công nghệ hoạt động.

Về mặt cơ chế, chính sách quản lý, nhiều quốc gia chưa hoàn thiện luật, văn bản dưới luật quản lý không gian mạng, tạo ra những khoảng trống dẫn đến mất an toàn công nghệ trên không gian mạng.

Về mặt nguồn nhân lực, lực lượng bảo đảm an toàn công nghệ trên không gian mạng nói riêng và an ninh mạng nói chung trên thế giới có những hạn chế nhất định về năng lực, về cơ chế hoạt động dẫn đến công tác bảo đảm an toàn an ninh công nghệ còn gặp nhiều khó khăn.

Những thách thức an ninh công nghệ kể trên thực sự đang hiện hữu ở Việt Nam, làm cho tình hình an ninh mạng ở Việt Nam ngày càng phức tạp. Theo báo cáo "Đổi mới công nghệ ở Việt Nam: Đóng góp của công nghệ vào tăng trưởng kinh tế" trong khuôn khổ dự án nghiên cứu chung giữa Bộ Khoa học và công nghệ Việt Nam và Tổ chức CSIRO's Data 61 của Ôxtrâylia đã chỉ ra, từ năm 2015, đổi mới công nghệ đã trở thành động lực chính thúc đẩy tăng trưởng ở Việt Nam. Tuy nhiên, số liệu cho thấy, Việt Nam vẫn còn chậm trong việc tiếp nhận công nghệ khi so sánh với các nước có cùng mức thu nhập[2]. Từ việc chậm trễ này, các nguy cơ tội phạm công nghệ cao gia tăng.

Tình hình an ninh mạng và tội phạm công nghệ cao ở Việt Nam được đánh giá là: hạ tầng kỹ thuật chưa đáp ứng yêu cầu chủ động phòng, chống tội phạm mạng; hoạt động tấn công mạng ở Việt Nam khá nghiêm trọng; tội phạm sử dụng mạng để lừa đảo, chiếm đoạt tài sản gia tăng; hoạt động sử dụng mạng để xâm phạm an ninh quốc gia đang trở nên phức tạp và nguy hiểm; công tác quản lý nhà nước về an toàn, an ninh mạng chưa đáp ứng được nhu cầu trong tình hình mới[3].

Việt Nam cũng đang phải đối mặt với chiến lược "diễn biến hòa bình" trên không gian mạng, các loại hoạt động gián điệp mạng và tội phạm công nghệ cao, nguy cơ chiến tranh mạng và nguy cơ mất an toàn thông tin mạng đe dọa an ninh quốc gia. Theo các tổ chức an ninh mạng Kaspersky và Symantec, Việt Nam là quốc gia đứng đầu thế giới về nguy cơ bị nhiễm mã độc, phần mềm độc hại (qua USB, thẻ nhớ), với gần 70% người dùng máy tính có nguy cơ bị lây nhiễm; đứng thứ ba về số lượng người dùng di động bị mã độc tấn công trên thế giới; đứng thứ tư trên thế giới về nguy cơ bị nhiễm độc khi sử dụng internet. Hệ quả là năm 2020, có tới hơn 73% số vụ lộ, lọt bí mật nhà nước xảy ra trên không gian mạng, tăng khoảng 3% so với năm 2019[4].

3. Thực trạng nguồn nhân lực an ninh công nghệ trong an ninh mạng tại Việt Nam

Hiện nay, số lượng nhân lực làm việc trong lĩnh vực an ninh công nghệ đang thiếu hụt khá trầm trọng. Tỷ lệ nhân lực công nghệ thông tin Việt Nam chỉ chiếm 1,1% tổng số lao động, còn thấp so với nhiều nước[5]. Đội ngũ làm việc trong lĩnh vực an ninh mạng có khoảng 50.000 người, trong khi nhu cầu thật sự là khoảng 700.000 người[6].

Bên cạnh đó, chất lượng của nguồn nhân lực cũng chưa đáp ứng nhu cầu. Các khảo sát của Fortinet (một công ty đa quốc gia về bảo mật và an toàn thông tin) cho thấy, 71% các doanh nghiệp Việt Nam đang phải đối mặt với khó khăn trong việc tuyển dụng nhân lực đủ tiêu chuẩn về an ninh mạng[7]. Trường đại học CMC, một trong những cơ sở đào tạo ngành công nghệ thông tin cho biết, chỉ 35% sinh viên ra trường đáp ứng yêu cầu nhà tuyển dụng. Theo "Chiến lược phát triển nguồn nhân lực số" mới đây của FPT Digital, Việt Nam có gần 400.000 kỹ sư công nghệ thông tin và hơn 50.000 sinh viên chuyên ngành công nghệ thông tin tốt nghiệp mỗi năm. Tuy vậy, chỉ có khoảng 30% lực lượng nhân sự công nghệ thông tin đáp ứng được yêu cầu thực tế của công việc[8]. Trên thực tế, mức lương và đãi ngộ của ngành này đang khá cao so với mặt bằng chung, nhưng vẫn khó tuyển nhân sự đạt yêu cầu.

Nhìn chung, nhân lực an toàn công nghệ (để bảo đảm an ninh mạng) đang thiếu hụt trầm trọng và trở thành vấn đề cấp thiết. Điều này sẽ làm gia tăng tình trạng mất an toàn thông tin, gia tăng các nguy cơ về an ninh mạng. Các vụ việc xâm phạm an ninh mạng có xu hướng ngày càng tăng trong những năm gần đây. Điều đó càng đẩy nhu cầu nhân sự lên và làm phức tạp thêm bài toán nhân lực trong bối cảnh hiện nay.

4. Nhu cầu phát triển nguồn nhân lực an ninh công nghệ chất lượng cao trong an ninh mạng của Việt Nam thời gian tới

Sự phát triển của khoa học công nghệ thúc đẩy nhu cầu có một đội ngũ nhân lực chất lượng cao về an ninh công nghệ. Khoa học và công nghệ từ trước tới nay đã luôn là động lực phát triển xã hội, đến kỷ nguyên số 4.0 hiện nay, không ngành, nghề, lĩnh vực nào có thể đứng ngoài cơn lốc của sự chuyển biến công nghệ. Việt Nam không phải là quốc gia sớm tiếp cận internet, nhưng khi đã kết nối thì phát

triển nhanh chóng, trở thành quốc gia có số lượng người sử dụng internet thuộc top cao nhất thế giới. Từ đó, ứng dụng công nghệ thông tin được sử dụng ở hầu hết các ngành, nghề, các doanh nghiệp, cơ quan nhà nước, các hoạt động kinh tế, quản lý xã hội...

Thời gian tới, một số công nghệ dự báo sẽ được ứng dụng rộng rãi. Thí dụ, sự phát triển của máy tính lượng tử sẽ có thể thay thế cho máy tính thông thường; bảo mật điện toán đám mây; ứng dụng trí thông minh nhân tạo; Blockchain (công nghệ chuỗi - khối, cho phép truyền tải dữ liệu một cách an toàn dựa trên hệ thống mã hóa phức tạp, chống gian lận, ngăn chặn thay đổi dữ liệu...), thực tế ảo (VR), trải nghiệm thực tế tăng cường (AR),... Bên cạnh đó, xu hướng *chuyển đổi số và làm việc từ xa* sẽ ngày càng phát triển.

Những xu hướng trên có thể khiến cho tỷ lệ tội phạm mạng và nguy cơ bị tấn công mạng gia tăng, đòi hỏi thế giới cần một lực lượng lao động có trình độ cao trong ngành khoa học máy tính, công nghệ thông tin, đặc biệt là an ninh mạng để bảo đảm các công nghệ thông tin an toàn, phát triển phục vụ tích cực cho con người.

Xu hướng của an ninh công nghệ tại Việt Nam cũng là nhân tố dẫn đến nhu cầu phát triển nguồn nhân lực chất lượng cao về lĩnh vực an ninh công nghệ

Công nghệ thông tin càng phát triển và được ứng dụng rộng rãi trong mọi lĩnh vực kinh tế - xã hội, thì các vấn đề an ninh trên mạng càng phát sinh và được quan tâm nhiều hơn. Việc nghiên cứu, ứng dụng khoa học và công nghệ vào công tác bảo đảm an ninh mạng đang được Bộ Công an, Bộ Khoa học và Công nghệ ưu tiên hàng đầu. Từ năm 2016, chương trình phối hợp hoạt động giữa 2 bộ đã được ký kết và triển khai, trong đó có nội dung nghiên cứu, ứng dụng khoa học và công nghệ phòng, chống tội phạm sử dụng công nghệ cao.

Quá trình tích cực ứng dụng công nghệ trong an ninh mạng là phấn đấu làm chủ hệ sinh thái các sản phẩm an toàn an ninh mạng, tiến tới xây dựng một nền công nghiệp an toàn an ninh mạng vững mạnh. Đây sẽ là một ngành công nghiệp mới đang có cơ hội phát triển rất tốt ở Việt Nam. Tự chủ trong các sản phẩm và các dịch vụ an toàn, an ninh mạng sẽ là giải pháp bền vững cho an ninh trên môi trường mạng và an ninh quốc gia. Mỗi cơ quan, doanh nghiệp có công cụ để bảo đảm an toàn cho riêng mình là góp phần vào sự ổn định chung.

Bộ Thông tin và Truyền thông đang tích cực thúc đẩy ngành công nghiệp mới này, xây dựng đề án phát triển, đề xuất mua sắm máy móc, thiết bị, đẩy mạnh nhu cầu sử dụng các sản phẩm an toàn an ninh mạng trong nước. Mục tiêu là nâng mức đầu tư cho an toàn thông tin của Việt Nam. Hiện nay, mức đầu tư khá thấp, chỉ chiếm 0,04% GDP, trong khi con số trung bình của thế giới là 0,13%. Nếu các cơ quan đơn vị tăng mức đầu tư an toàn thông tin, tăng cường sử dụng các sản phẩm bảo mật, thì quy mô thị trường của ngành công nghiệp mới này sẽ nhanh chóng đạt giá trị cao[9].

Với nhu cầu của ngành bảo mật thông tin, ngành an ninh mạng ngày càng phát triển, Việt Nam cần có một đội ngũ nhân sự chất lượng cao "gác cửa" và lan tỏa giá trị để bảo đảm an toàn công nghệ, thông tin.

5. Giải pháp phát triển nguồn nhân lực chất lượng cao về an ninh công nghệ của Việt Nam

Từ những yêu cầu cấp thiết của vấn đề bảo vệ an ninh trên không gian mạng, nâng cao năng lực công nghệ của quốc gia, Việt Nam cần có hệ thống chính sách hỗ trợ tối ưu cho việc giải những bài toán về nguồn nhân lực.

Một là, về đào tạo, bồi dưỡng

Đây là giải pháp then chốt, góp phần tạo nên kết quả bền vững cho vấn đề nguồn nhân lực. Từ năm 2014, Thủ tướng Chính phủ đã ra quyết định phê duyệt đề án "Đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020" với kinh phí 470 tỷ đồng. Theo đó, Đề án hỗ trợ kinh phí cho các cơ sở đào tạo trọng điểm kỹ sư, cử nhân chất lượng cao của ngành học này. Tuy nhiên đến nay, nguồn nhân lực của ngành này vẫn đang được đánh giá là thiếu hụt trầm trọng. Mặc dù số lượng nhân sự đã tăng lên, nhưng vẫn chưa đáp ứng đủ nhu cầu của các doanh nghiệp, tổ chức.

Ngày 06-01-2021, Thủ tướng Chính phủ đã ban hành Quyết định số 21/QĐ-TTg phê duyệt Đề án "Đào tạo và phát triển nguồn nhân lực an toàn thông tin giai đoạn 2021-2025". Những nỗ lực của Chính phủ trong việc phát triển nguồn nhân lực công nghệ thông tin thông qua đào tạo là rất cao. Tuy nhiên, những kết quả thu được vẫn chưa bắt kịp nhu cầu thực tế. Vì vậy, cần tiếp tục có những chính sách và hành động mạnh mẽ, quyết liệt hơn trong vấn đề này.

Trước hết, cần quy hoạch hệ thống các cơ sở đào tạo nguồn nhân lực an ninh mạng để có chính sách đầu tư phát triển những trung tâm đào tạo, bồi dưỡng, cung cấp nguồn nhân lực an ninh mạng chất lượng cao. Trước những nguy cơ cận kề về an ninh quốc gia khi thiếu nguồn nhân lực mạng, cần có những ưu tiên thích hợp để nâng cao chất lượng đào tạo cho hệ thống đào tạo ngành này. Từ đội ngũ giảng dạy, chương trình, cơ sở vật chất cần được đầu tư nâng cấp, phù hợp với đặc thù các ngành đào tạo. Nắm bắt yêu cầu từ các cơ sở đào tạo, học hỏi kinh nghiệm để đổi mới theo hướng hiện đại và hiệu quả nhất.

Hiện nay, tỷ lệ sinh viên ra trường đáp ứng được nhu cầu công việc thực tế còn thấp, và nhiều ý kiến đề xuất sinh viên nên đi thực tế ngay từ những năm đầu, kết hợp đào tạo giữa trường lớp và thực tiễn. Sinh viên cần có thực hành và chuẩn hóa các kỹ năng, thu nhận trải nghiệm từ những tình huống thực tiễn trong an ninh mạng. Điều này cũng làm cho chuẩn đầu ra của các cơ sở đào tạo gần hơn với chuẩn đầu vào của các đơn vị tuyển dụng. Vì vậy, cơ chế hợp tác giữa nhà trường và tổ chức, doanh nghiệp trong đào tạo cần được hoàn chỉnh hơn và chặt chẽ hơn.

Chương trình đào tạo cũng cần có quy trình đổi mới, cập nhật nhanh hơn để phù hợp với tốc độ phát triển nhanh chóng của khoa học, công nghệ giai đoạn hiện nay. Mô hình đào tạo nhân lực liên quan đến những sản phẩm công nghệ đột phá cần được thực hiện từ các bậc học phổ thông và có những ngành cần được xã hội hóa nhiều hơn thay vì Nhà nước thực hiện hoàn toàn. Nên có chính sách hỗ trợ chi phí đào tạo, tài trợ học bổng cho những ngành học an ninh công nghệ. Ngoài ra, việc tăng cường các chương trình bồi dưỡng ngắn hạn cũng nên được quan tâm, như một hình thức đào tạo rút gọn, nhanh chóng, kịp thời cập nhật tri thức mới, bổ sung năng lực cho nguồn nhân sự đang làm việc.

Hai là, về cơ chế thu hút nhân tài

Ở Việt Nam, nhiều chủ trương, chính sách đã được ban hành nhằm thu hút, trọng dụng nguồn nhân lực chất lượng cao. Nhưng trong lĩnh vực an ninh công nghệ, việc thu hút nhân tài bằng lương và các chế độ đãi ngộ không phải dễ dàng. Đây là ngành có mức lương cao, nhiều công ty tư nhân và cả các công ty nước ngoài săn đón, trong khi đó điều kiện kinh tế đất nước còn khó khăn, ngân sách chi trả cho

lương còn hạn chế. Tuy vậy, cần có cơ chế thu hút nhân tài với đội ngũ nhân lực chất lượng cao trong ngành an ninh mạng vào làm việc tại các cơ quan nhà nước.

Trước hết, cần xây dựng nhận thức thống nhất về thu nhập vượt trội của nhân lực chất lượng cao ngành an ninh mạng là hoàn toàn xứng đáng với tính chất lao động và đóng góp quan trọng của họ. Bên cạnh đó, cần xây dựng chế độ tiền lương đúng giá trị sức lao động đặc biệt, tạo sự minh bạch và công bằng, làm động lực cho các cá nhân phấn đấu, tin tưởng và cống hiến.

Ba là, về môi trường làm việc

Cùng với lương và đãi ngộ, việc đổi mới chính sách tuyển dụng, sử dụng nhân lực, xây dựng môi trường làm việc cũng là một giải pháp giữ nhân tài hiệu quả. Môi trường làm việc là yếu tố tác động mạnh mẽ đến khả năng tập trung, sáng tạo. Đa phần các chuyên gia và nhà khoa học, các cá nhân có sự say mê trong công việc là những người quan tâm tới môi trường và điều kiện làm việc hơn cả mức đãi ngộ. Họ cần nhận được sự tin tưởng, tôn trọng, trao quyền chủ động trong tuyển nhân sự, chủ động thời gian và nguồn lực để tiến hành nghiên cứu, tìm tòi giải pháp cho các vấn đề đặc thù của an ninh mạng. Từ thực tế đó, khu vực công nên có sự đổi mới toàn diện trong khía cạnh sử dụng nhân lực chất lượng cao hiệu quả và hợp lý.

Hơn nữa, cần có sự cải tiến những trì trệ thường xuất hiện trong khu vực công, có chính sách ghi nhận, trọng dụng nhân lực minh bạch. Giữ chân và phát huy được nhân tài cũng là một phương cách quan trọng nhất để bảo đảm an ninh công nghệ trong an ninh mạng.

6. Kết luận

Về bản chất, an ninh công nghệ trong an ninh mạng luôn gắn với con người và thói quen sử dụng của con người. Ý thức được vai trò của con người và nguồn nhân lực làm việc trong lĩnh vực này, Việt Nam đã có nhiều nỗ lực cố gắng trong việc phát triển nguồn nhân lực chất lượng cao trong lĩnh vực an ninh công nghệ (trong an ninh mạng), tuy nhiên vẫn còn có một số hạn chế. Thực hiện những giải pháp trên, Việt Nam sẽ sớm khắc phục được những hạn chế, bảo đảm an toàn an ninh công nghệ trong an ninh mạng ❐

Ngày nhận bài: 04-02-2024; Ngày bình duyệt: 20-3-2024; Ngày duyệt đăng: 22-3-2024.

(1), (4) Cao Anh Dũng: *Bảo vệ an ninh quốc gia trên không gian mạng trong bối cảnh cuộc Cách mạng công nghiệp lần thứ tư theo định hướng Đại hội XIII của Đảng*, https://tinhdoanquangninh.vn.

(2) Phạm Thu Hiền: *Mô hình phát triển công nghệ tại Việt Nam, 2023*, https://www.qdnd.vn.

(3) Nguyễn Văn Thành: *Chủ quyền quốc gia trên không gian mạng - những yêu cầu đảm bảo các chỉ số an ninh - an toàn trong bối cảnh hiện nay*, http://dhannd.edu.vn.

(5), (8) Hoàng Hà: *Nhân lực công nghệ thông tin Việt Nam chỉ chiếm 1,1% tổng số lao động, doanh nghiệp phải "xoay xở" như thế nào?*, https://vneconomy.vn.

(6) *Thiếu hụt nhân sự bảo mật đang làm gia tăng rủi ro an ninh mạng*, https://mic.gov.vn/, đăng ngày 06-4-2023.

(7) *Lĩnh vực an ninh mạng đối mặt tình trạng thiếu hụt nhân lực*, https://dantri.com.vn/, đăng ngày 10-6-2022.

(9) *An ninh mạng: Ngành công nghiệp tỷ đô mới*, https://nghenghiepcuocsong.vn, đăng ngày 09-12-2020.