Một số giải pháp đảm bảo an toàn, an ninh mạng tại Việt Nam hiện nay

TS. NGUYỄN THỊ THÚY MAI
Học viện Báo chí và Tuyên truyền; Email: thuymai.hvbctt@gmail.com

Nhận ngày 18 tháng 7 năm 2023; chấp nhận đăng tháng 11 năm 2023.

Tóm tắt: *Trong bối cảnh toàn cầu hóa và sự phát triển của khoa học kỹ thuật, của công nghệ 4.0, cùng sự bùng nổ ngày càng mạnh mẽ của Internet vạn vật, các quốc gia đang phát triển, trong đó có Việt Nam đang phải đối mặt với nhiều thách thức và sự đe dọa thường trực về vấn đề đảm bảo an toàn, an ninh mạng nói riêng và đối với nền an ninh quốc gia nói chung. Bài viết nhằm mô tả những khó khăn, thách thức trong việc đảm bảo an toàn, an ninh mạng của Việt Nam, trên cơ sở đó đề xuất một số giải pháp nhằm đảm bảo an toàn, an ninh mạng trong nền an ninh quốc gia của Việt Nam trong bối cảnh hiện nay.*
Từ khóa: *an toàn, an ninh mạng, Internet vạn vật, đảm bảo an ninh mạng.*

Abstract: *Developing countries, including Vietnam, are facing significant challenges and constant threats regarding safety, cybersecurity, and national security in the context of globalization and technological development, the advent of the 4.0 industry, and the pervasive explosion of the Internet. This article describes the difficulties and challenges in ensuring safety and cybersecurity in Vietnam. It also proposes several solutions to ensure safety and cybersecurity in the national security framework of Vietnam in the current context.*
Keywords: *safety, cybersecurity, Internet of Things, cybersecurity assurance.*

1. Vấn đề an toàn, an ninh mạng ở Việt Nam hiện nay

Với sự phát triển nhanh chóng của công nghệ 4.0 đặc biệt là sự phát triển của Internet vạn vật (Internet of Things) đã mang lại nhiều lợi ích to lớn đối với con người. Internet đã trở thành phương tiện kết nối, trao đổi thông tin, hợp tác, giao lưu, giải trí□ giữa mọi tầng lớp trong xã hội. Internet cũng có vai trò quan trọng trong việc lưu trữ, tìm kiếm tài liệu, học tập, nghiên cứu, giao dịch□ nhằm đáp ứng được mọi nhu cầu của nhiều đối tượng khác nhau. Tuy nhiên, bên cạnh đó Internet cũng tiềm ẩn nhiều nguy cơ đối với cá nhân, tổ chức như bị rò rỉ, mất mát thông tin, xâm phạm quyền riêng tư, thậm chí còn đặt ra nhiều thách thức đối với toàn xã hội, đối với nền an ninh của các quốc gia trên toàn thế giới như: chiến tranh mạng, chiến tranh thông tin, khủng bố mạng, tội phạm mạng□ trong đó có Việt Nam.

Tại Việt Nam, an ninh mạng và đảm bảo an ninh mạng hiện nay đang là vấn đề khá phức tạp. Biểu hiện là trong những năm gần đây các thế lực phản động tăng cường lợi dụng không gian mạng để hoạt động tình báo, gián điệp, khủng bố, phá hoại hệ thống thông tin; phát tán thông tin xấu, độc, bịa đặt, bóp méo sự thật, xuyên tạc vấn đề, □đổi trắng thay đen□và định hướng dư luận bằng luận điệu thù địch... nhằm tác động toàn diện trên các lĩnh vực. Thống kê, trung bình mỗi năm, các cơ quan chức năng đã phát hiện trên 850.000 tài liệu chiến tranh tâm lý, phản động, ân xá quốc tế, tài liệu tuyên truyền tà đạo trái phép; gần 750.000 tài liệu tuyên truyền chống Đảng, Nhà nước được tán phát vào Việt Nam qua đường bưu chính. Từ năm 2010 đến năm 2019 đã có 53.744 lượt cổng thông tin, trang tin điện tử có tên miền .vn bị tấn công, trong đó có 2.393 lượt cổng thông tin, trang tin điện tử của các cơ quan Đảng, Nhà nước □.gov.vn□, xuất hiện nhiều cuộc tấn công mang màu sắc chính trị, gây ra những

hậu quả nghiêm trọng[1].

Theo số liệu từ Cục An toàn thông tin, trong 11 tháng đầu năm 2022, đã có tới 11.213 cuộc tấn công mạng hướng vào Việt Nam, tăng 44,2% so với cùng kỳ năm ngoái. Trong đó, có 3.930 cuộc tấn công giả mạo, 1.524 cuộc tấn công thay đổi nội dung, 5.759 cuộc tấn công phần mềm độc hại[2]. Ngoài ra, có rất nhiều các cuộc tấn công nhằm vào hệ thống sân bay, ngân hàng, các trang cá nhân và của tổ chức để lấy cắp thông tin, lừa đảo, chiếm đoạt tài sản, đe dọa an ninh an toàn. Ví dụ như cuộc tấn công nhằm vào hệ thống trang web của Vietnam Airlines để đánh cắp thông tin khách hàng của sân bay Quốc tế Nội Bài và sân bay Quốc tế Tân Sơn Nhất vào 29 tháng 7 năm 2016. Trong tháng 8 năm 2016, một khách hàng của Vietcombank cũng bị mất hơn 500 triệu đồng thông qua giao dịch ngân hàng điện tử. Và trong những năm gần đây, rất nhiều các cá nhân, tổ chức đã bị lừa đảo chiếm đoạt tài sản thông qua các tài khoản, tín dụng.

Theo thống kê Việt Nam có tổng cộng 77,93 triệu người dùng Internet, đạt tỷ lệ sử dụng Internet là 79,1% trên tổng dân số[3]. Bên cạnh những lợi ích to lớn của việc kết nối Internet thì cũng tiềm ẩn nhiều nguy cơ mất an toàn đối với người dùng và an ninh quốc gia...

2. Một số khó khăn trong việc đảm bảo an ninh mạng ở Việt Nam

Với số lượng người dùng ngày càng gia tăng nhanh chóng ở Việt Nam cũng như sự phát triển nhanh mạnh của công nghệ số, đặt ra một số khó khăn đối với công tác đảm bảo an ninh mạng của chúng ta hiện nay. Cụ thể là:

Thứ nhất, hệ thống chính sách, pháp luật còn thiếu tính cụ thể.

Đảng và Nhà nước ta đã có nhiều chủ trương, ban hành nhiều chính sách, pháp luật như: Luật Giao dịch điện tử, 51/2005/QH11, ngày 29/11/2005; Luật Công nghệ thông tin 67/2006/QH11, ngày 12/07/2006; Nghị định 26/2007/NĐ-CP ngày 15/02/2007, quy định chi tiết việc thực hiện các Luật Giao dịch điện tử chữ ký số và dịch vụ chứng thực chữ ký số; Nghị định số 27/2007/NĐ-CP ngày 02/02/2007 về Giao dịch điện tử trong hoạt động Tài chính; Nghị định số 90/2008/NĐ-CP ngày 13/8/2008 về chống thư rác; Luật An ninh mạng; Luật Bảo vệ bí mật nhà nước và nhiều văn bản hướng dẫn thi hành khác. Tuy nhiên, nhìn chung tính cụ thể và việc thực thi các văn bản vẫn còn nhiều bất cập, chưa sát với thực tế, chưa mang lại hiệu quả cao. Hệ thống văn bản quy phạm pháp luật hiện hành ở nước ta chưa quy định cụ thể hình thức, biện pháp thu thập chứng cứ từ nguồn dữ liệu, gây nhiều khó khăn cho việc củng cố chứng cứ, không đủ căn cứ chứng minh hành vi sử dụng không gian mạng để phạm tội của đối tượng để xử lý theo quy định của pháp luật. Một số văn bản hướng dẫn thực hiện chậm được ban hành để thống nhất thực hiện, như: hướng dẫn về "nơi xảy ra tội phạm", "nơi phát hiện tội phạm" để xác định thẩm quyền điều tra đối với các vụ án, vụ việc mà đối tượng phạm tội chiếm đoạt tiền của bị hại thông qua dịch vụ chuyển tiền nhanh E-banking, ví điện tử... Hành lang pháp lý quy định về giao dịch tiền "ảo", tiền kỹ thuật số còn chậm ban hành, tạo kẽ hở cho các đối tượng lợi dụng để trục lợi. Các quy định về dịch vụ mạng Internet, mạng viễn thông, dịch vụ ngân hàng tạo thuận lợi cho nhân dân đăng ký, sử dụng, phát triển kinh tế - xã hội của đất nước nhưng cũng là điều kiện để các đối tượng lợi dụng lừa đảo chiếm đoạt tài và tìm mọi kẽ hở nhằm đối phó với sự phát hiện, đấu tranh của cơ quan chức năng. Ngoài ra, chế tài xử phạt một số hành vi chưa cao, chưa đủ sức răn đe.

Sự thay đổi, phát triển về công nghệ nhanh chóng theo từng ngày trong khi nhiều quy định pháp luật trên một số lĩnh vực có liên quan còn chưa đầy đủ, thiếu đồng bộ, chưa phù hợp với thực tiễn, chưa được sửa đổi, bổ sung kịp thời. Công tác quản lý nhà nước trong một số lĩnh vực còn tồn tại nhiều kẽ hở, thiếu sót. Sự phối hợp giữa các cơ quan, ban, ngành, các cấp, các tổ chức xã hội còn chưa đồng bộ, chặt chẽ, chưa mang lại hiệu quả.

Thứ hai, nhận thức về an ninh mạng, an toàn thông tin còn nhiều hạn chế.

Nhận thức của con người về an ninh mạng cũng là một trong những yếu tố quan trọng tác động đến quản trị an ninh mạng, theo SasseandFlechais (2005) các yếu tố này bao gồm: gặp sự cố do sử dụng công cụ bảo mật không chính xác; không hiểu tầm quan trọng của dữ liệu, phần mềm và hệ thống

đối với tổ chức của họ; không tin rằng tài sản có thể gặp nguy cơ (tức là họ sẽ bị tấn công); hoặc không hiểu rằng hành vi của mình sẽ khiến hệ thống gặp rủi ro[4]. Và do vậy việc đảm bảo an ninh mạng không đơn thuần chỉ quan tâm về mặt công nghệ mà nâng cao nhận thức của các cá nhân với vấn đề này rất quan trọng[5].

Trong thực tế, nhận thức của người dân Việt Nam về an ninh mạng cũng là một trong những vấn đề lớn nhất. Theo cảnh báo khẩn cấp từ Trung tâm ứng cứu sự cố máy tính Việt Nam (VNCERT) ngày 27/12/2017, khoảng 1,4 tỷ tài khoản email và mật khẩu đã bị lộ trên toàn thế giới và 437.664 tài khoản là của Việt Nam, trong đó có 930 tài khoản thuộc người làm việc nhà nước[6]. ESET (2015) cũng chỉ ra vấn đề này trong Báo cáo an ninh mạng Việt Nam 2015 và nhấn mạnh người dùng Việt Nam nhận thức về an ninh mạng còn thấp và chưa có biện pháp phòng ngừa thích hợp. Chưa đến 30% số người được hỏi nhận ra những rủi ro nghiêm trọng từ các mối đe dọa phổ biến như ứng dụng không an toàn, thư rác và quảng cáo biểu ngữ, và hơn 40% trong tổng số người được hỏi có quan niệm sai lầm về các vấn đề an ninh mạng phổ biến, đặc biệt là (1) kết nối với Wifi công cộng miễn phí được coi là an toàn, (2) tin rằng máy tính dễ bị tấn công hơn thiết bị di động và (3) sử dụng thông tin cá nhân dễ nhớ để tạo mật khẩu. Điều này dẫn đến nhiều hành vi nguy hiểm trên mạng và khiến một bộ phận lớn người dùng Việt Nam trở thành mục tiêu dễ dàng cho các cuộc tấn công mạng và tội phạm mạng[7].

Không chỉ các cá nhân người Việt Nam nhận thức chưa đầy đủ về an ninh mạng, mà nhiều doanh nghiệp, cơ quan, tổ chức cũng chưa chú trọng đến vấn đề an ninh mạng, an toàn thông tin (ATTT). Có khoảng 81% các doanh nghiệp không biết hoặc không có quy trình xử lý sự cố và việc xây dựng hệ thống ATTT theo chuẩn quốc tế hoặc Việt Nam còn vẫn rất xa lạ đối với doanh nghiệp Việt. Hầu hết các doanh nghiệp không biết đơn vị mình đã có chứng chỉ theo chuẩn quốc tế ISO 27001 hay chuẩn Việt Nam TCVN 11930:2017[8] hay chưa. Hiện nay hầu hết các cơ quan nhà nước còn rất lúng túng nếu bị tấn công, chỉ có khoảng gần 10% các cơ quan có giám sát ATTT mạng, 50% không có bộ phận chuyên trách về ATTT[9].

Thứ ba, vấn đề đảm bảo an toàn thông tin chưa được coi trọng đúng mức, thiếu sự đầu tư về trang thiết bị cũng như nguồn nhân lực.

Theo kết quả khảo sát của Hiệp hội An toàn thông tin Việt Nam (VNISA) năm 2018 thì một trong những điểm yếu của việc đảm bảo an toàn thông tin mạng của Việt Nam đó là Chính sách đầu tư và chi phí cho an ninh mạng[10]. Thực tế hiện nay cũng cho thấy, hầu hết các cơ quan, doanh nghiệp đều sử dụng thiết bị thông minh mà chưa có các biện pháp đảm bảo an toàn thông tin, như sử dụng phần mềm sao chép, không có bản quyền. Việc sử dụng phần mềm không chính thống sẽ dẫn đến nguy cơ mất dữ liệu, thông tin cá nhân. Các cơ quan nhà nước luôn bị tin tặc coi là mục tiêu tấn công APT, DOS/DDOS nhằm chiếm các tài liệu, dữ liệu quan trọng. Mặt khác, các cơ quan, tổ chức chưa chú trọng đầu tư nguồn kinh phí cho hoạt động đảm bảo an ninh mạng. Theo báo cáo của nhiều địa phương và tổ chức thì việc đầu tư cho an toàn thông tin chưa được chú trọng cả về kỹ thuật và nhân lực cao cho hoạt động đảm bảo an ninh mạng. Ví dụ, theo báo cáo Bộ công an (2022) thì ngân sách đầu tư của Nhà nước cho ngành công nghiệp an ninh còn hạn hẹp dẫn tới quy mô nghiên cứu nhỏ lẻ thiếu đồng bộ và dẫn tới tỷ lệ cung ứng sản phẩm công nghiệp an ninh thấp[11].

Thứ tư, kỹ thuật và thủ đoạn tin tặc ngày càng tinh vi.

Hoạt động tấn công không gian mạng rất đa dạng và tinh vi như: làm mất kết nối Internet, đánh sập các website của chính phủ, cơ quan, đơn vị, nhà trường, doanh nghiệp; giả mạo các website nhằm lừa đảo; đột nhập vào máy tính cá nhân hoặc lấy tài khoản và mật khẩu; đánh cắp dữ liệu cá nhân (hình ảnh, file, video); tấn công bằng mã độc; tấn công ẩn danh bằng những phần mềm độc hại (phần mềm diệt virus, các trình duyệt); tấn công qua usb, đĩa CD, địa chỉ IP, server, Đã có nhiều cuộc tấn công mạng diễn ra trên phạm vi toàn thế giới gây những thiệt hại to lớn về kinh tế - xã hội. Với tốc độ phát triển nhanh chóng của công nghệ, các thủ đoạn tấn công phức tạp, kế hoạch và cách thức thực hiện tinh vi nhằm lẩn tránh khỏi sự phát hiện của các hệ thống bảo mật, phát hiện như tấn công sử dụng lỗ hổng

zero-day, tấn công kỹ nghệ xã hội, tấn công phát tán mã độc, tấn công có chủ đích (APT)... Khi phát hiện ra sự tấn công thì đã có những thiệt hại nhất định trên toàn hệ thống. Ngoài tấn công mạng, các hiểm họa tấn công từ chính trong mạng nội bộ, mạng LAN của cơ quan, tổ chức cũng là một trong những mối đe dọa tiềm tàng, thường trực gây ra những hậu quả nghiêm trọng, nếu như không có biện pháp phòng chống. Tóm lại, các cuộc tấn công này rất khó bị phát hiện theo các cách thức và kỹ thuật thông thường.

Với sự phổ biến của 5G và Internet kết nối vạn vật, các đối tượng có thể kiểm soát hàng triệu thiết bị, camera an ninh□ tạo ra các mạng máy tính ma để tấn công có chủ đích, gây gián đoạn đến toàn bộ hệ thống mạng Internet của một quốc gia. Ngoài ra, chúng cũng có thể tạo nên những video giả mạo khuôn mặt hoặc tái tạo giọng nói của người dùng để vượt qua hàng rào bảo vệ sinh trắc học, đánh cắp tài khoản ngân hàng, thực hiện thanh toán trái phép. Đây sẽ là những thách thức to lớn đối với vấn đề an ninh mạng trong kỷ nguyên số.

3. Một số giải pháp đảm bảo an toàn, an ninh mạng tại Việt Nam

Những yếu tố gây mất an toàn, an ninh mạng đều gây ảnh hưởng nghiêm trọng tới hoạt động của cơ quan đơn vị, thậm chí là an ninh quốc gia. Do đó, đảm bảo an ninh mạng là nhiệm vụ quan trọng và cần thiết đối với mỗi cá nhân và tổ chức, để làm được điều đó cần tập trung vào một số giải pháp sau đây:

Một là, tiếp tục xây dựng và hoàn thiện hệ thống chính sách pháp luật về an toàn, an ninh mạng.

Thường xuyên phổ biến, quán triệt chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước về an toàn, an ninh mạng, coi đây là nhiệm vụ quan trọng của cả hệ thống chính trị. Cần tiếp tục bổ sung và kiện toàn các quy định về quản lý an toàn thông tin, an ninh mạng đảm bảo môi trường pháp lý rõ ràng, minh bạch, công khai, bình đẳng. Mặt khác, khi xây dựng cơ chế chính sách an ninh mạng cần chú ý đến đặc thù của từng ngành nghề lĩnh vực cụ thể. Bên cạnh đó cần xây dựng chế tài xử lý các hành vi vi phạm an ninh mạng một cách chặt chẽ, đủ sức răn đe đối với từng hành vi cụ thể.

Cần xây dựng cơ chế, chính sách khuyến khích thúc đẩy các doanh nghiệp tại Việt Nam trong việc nghiên cứu và cung ứng dịch vụ an ninh mạng. Nên giao trách nhiệm chính cho một đơn vị hoặc cơ quan chuyên trách chính về vấn đề an toàn, an ninh mạng, tránh chồng chéo nhiệm vụ giữa các cơ quan hoặc nhiều cơ quan cùng đảm nhiệm vấn đề này dẫn tới khó khăn trong việc phối hợp, quy trách nhiệm quản lý.

Hai là, nâng cao nhận thức của người dân, các đơn vị, tổ chức về vấn đề an toàn, an ninh mạng.

Nâng cao nhận thức, trách nhiệm của các cấp ủy đảng, chính quyền, Mặt trận Tổ quốc, các tổ chức chính trị - xã hội, người dân, doanh nghiệp trong công tác bảo đảm an toàn, an ninh mạng. Người đứng đầu cấp ủy trực tiếp lãnh đạo, chỉ đạo và chịu trách nhiệm về công tác an toàn, an ninh mạng, chủ động rà soát, xác định rõ những vấn đề trọng tâm, trọng điểm để chỉ đạo thực hiện hiệu quả.

Tăng cường tuyên truyền, phổ biến các quy định của pháp luật về đảm bảo an toàn thông tin và Luật An ninh mạng nhằm bảo vệ người dùng hợp pháp trên không gian mạng, đồng thời cũng cần tuyên truyền về những hành vi bị cấm trong Luật An ninh mạng, các quy định hình thức xử phạt. Mặt khác, các hình thức tuyên truyền cũng cần đa dạng hóa, phong phú và linh hoạt giữa các cơ quan, địa phương, doanh nghiệp như nói chuyện chuyên đề, cuộc thi tìm hiểu, góp ý xây dựng luật□ Thậm chí, các cơ sở giáo dục nên sớm đưa nội dung giáo dục bảo đảm an toàn, an ninh không gian mạng quốc gia vào chương trình dạy học phù hợp với ngành học, cấp học.

Tăng cường tập huấn, bồi dưỡng nâng cao ý thức và kỹ năng đảm bảo an toàn thông tin cho cá nhân, cơ quan, tổ chức giúp họ có kiến thức để nhận diện các thông tin xấu độc, cách phòng tránh, cách bảo vệ thông tin cá nhân□ qua đó giúp nâng cao ý thức chính trị, trách nhiệm, nghĩa vụ công dân đối với nhiệm vụ bảo vệ không gian mạng quốc gia.

Phát huy sự tham gia có hiệu quả của quần chúng nhân dân trong công tác bảo đảm an toàn, an ninh mạng và chủ động ứng phó với các nguy cơ, thách thức từ không gian mạng.

Ba là, tăng cường áp dụng các biện pháp kỹ thuật trong quản lý không gian mạng đồng thời đẩy mạnh và phát triển ngành công nghiệp an ninh mạng.

Có thể thấy, tin tặc và thủ đoạn tấn công ngày

càng tinh vi khó lường do vậy chúng ta cần chủ động và đầu tư sử dụng các kỹ thuật nhằm phát hiện, lọc, ngăn chặn hoạt động phát tán phần mềm độc hại, tin giả, thông tin vi phạm pháp luật xuất phát từ Internet thuộc phạm vi quản lý.

Triển khai hệ thống giám sát, điều hành an toàn, an ninh thông tin mạng tập trung nhằm tự động, thu thập, phân tích, cảnh báo khả năng mất an toàn, an ninh thông tin mạng trên hạ tầng kỹ thuật, ứng dụng của tổ chức, cơ quan, đơn vị. Bố trí đủ nhân lực chuyên trách, chịu trách nhiệm về an toàn, an ninh mạng trong các cơ quan, đơn vị; đầu tư nguồn lực để xây dựng hệ thống kỹ thuật, công cụ và triển khai các hoạt động bảo đảm an toàn, an ninh mạng và trong hoạt động của các cơ quan, đơn vị.

Phát triển và định hình nền công nghiệp an ninh mạng và an toàn thông tin nhằm tự chủ về công nghệ và trang thiết bị, không để bị lệ thuộc vào nước ngoài. Cần có lộ trình phát triển các doanh nghiệp công nghệ thông tin và an ninh mạng, trong đó, lựa chọn các lĩnh vực mà Việt Nam có thế mạnh để ưu tiên phát triển. Để làm được điều đó, Đảng và Nhà nước cần có chính sách và cơ chế hỗ trợ, khuyến khích phát triển công nghiệp an ninh mạng; Hoàn thiện các chính sách nhằm khuyến khích, huy động mọi nguồn lực xã hội trong nghiên cứu khoa học, phát triển và ứng dụng công nghệ thông tin và an ninh mạng; Tăng cường hợp tác, trao đổi nghiên cứu với các đơn vị mạnh trong và ngoài nước nhằm huy được hết tiềm năng, nội lực, khai thác các lợi thế, các thành tựu của thế giới để phát triển và tiến tới làm chủ các công nghệ tiên tiến; Tăng cường nghiên cứu, phát triển, sử dụng các phần mềm, dịch vụ thông tin riêng của Việt Nam, đáp ứng yêu cầu bảo mật thông tin, sự an toàn của bí mật nhà nước, giám sát an ninh mạng; Tập trung phát triển nguồn nhân lực cao thông qua đào tạo, bồi dưỡng cán bộ, tạo môi trường học tập, tạo điều kiện để họ có cơ hội học tập và phát triển năng lực.

Có thể thấy, các mối đe dọa trên không gian mạng ngày càng phức tạp hơn và ảnh hưởng nhiều hơn đến hiệu quả hoạt động của cả quốc gia. Ở các nước đang phát triển, cùng với sự bùng nổ của các loại hình kinh doanh trên nền tảng không gian mạng, nguy cơ còn nghiêm trọng hơn rất nhiều. Do vậy, đối với Việt Nam cần có sự vào cuộc, chung tay của cả hệ thống chính trị, bên cạnh đó cần có cách thức, phương pháp triển khai một cách chiến lược, đồng bộ trong việc đảm bảo an toàn, an ninh mạng một cách toàn diện trên các phương diện về cơ chế, chính sách, con người, công nghệ□ /.

(1) Lâm Đông Hồ và Nguyễn Xuân Hoàng (2023), *Thực trạng an toàn thông tin mạng hiện nay ở Việt Namvà giải pháp phòng chống vi phạm pháp luật trên không gian mạng, Tạp chí cơ quan Thông tin điện tử*, https://tapchicongthuong.vn/bai-viet/thuc-trang-an-toan-thong-tin-mang-hien-nay-o-viet-nam-va-giai-phap-phong-chong-vi-pham-phap-luat-tren-khong-gian-mang-103127.htm

(2) https://vtv.vn/cong-nghe/so-cuoc-tan-cong-mang-huong-vao-viet-nam-tang-hon-44-20221124150606854.htm

(3) Thống kê của Vnetwork, Internet Việt Nam 2023: *Số liệu mới nhất và xu hướng phát triển.*

https://www.vnetwork.vn/news/internet-viet-nam-2023-so-lieu-moi-nhat-va-xu-huong-phat-trien

(4) A. SasseandI. Flechais (2005), *Usable Security: Why Do We Need It? How Do We Get It?* In: Cranor, LFand Garfinkel,S, (eds.)Security and usability: Designing secure systems that people can use. Sebastopol, US: O□Reilly, 2005.

(5) A. SasseandI. Flechais (2005), *Usable Security: Why Do We Need It? How Do We Get It?* In: Cranor, LFand Garfinkel,S, (eds.)Security and usability: Designing secure systems that people can use. Sebastopol, US: O□Reilly, 2005.

(6) Vu Phuong Linh (2019), *Cybersecurity legal frameworks in Vietnam and Japan: a comparative analysis*, Master□s thesis of public policy, Vietnam Japan University, Hanoi.

(7) Dẫn theo Trần Thị Hằng (2016), *Nghiên cứu tìm hiểu thực trạng về an ninh mạng và biện pháp khắc phục*, Luận văn Thạc sỹ công nghệ thông tin, Trường Đại học Dân lập Hải Phòng.

(8) Kiều Anh (2019), *□Đầu tư cho an toàn thông tin như phòng chống rủi ro□*, Báo Khoa học phát triển, truy cập ngày 15/7/2023, https://khoahocphattrien.vn/thoi-su-trong-nuoc/bo-khcn-phai-thuc-hien-tot-3-yeu-cau-cua-thu-tuong/202307130930537p882c918.htm

(9) Kiều Anh (2019), *□Đầu tư cho an toàn thông tin như phòng chống rủi ro□*, Báo Khoa học phát triển, truy cập ngày 15/7/2023, https://khoahocphattrien.vn/thoi-su-trong-nuoc/bo-khcn-phai-thuc-hien-tot-3-yeu-cau-cua-thu-tuong/202307130930537p882c918.htm.

(10) Hiệp hội An toàn thông tin Việt Nam (VNISA) (2018), *kết quả khảo sát đánh giá chỉ số an toàn thông tin mạng Vnisa Index 2018*, https://drive.google.com/drive/folders/18K93h_lsx93hW3UiQ4JzyCvb3pWBmWC7

(11) Bộ công an (2022), *Báo cáo Tổng kết kết quả xây dựng, phát triển công nghiệp an ninh từ đại hội Đảng lần thứ XI đến nay,* https://bocongan.gov.vn/KND/vb/vbqp/Lists/GioiThieuVanBan/Attachments/1036/09.Baocao.1003.BC.BCA.pdf