DOI: 10.62829/VNHN.360.35.40

PHÒNG CHỐNG TỘI PHẠM KHÔNG GIAN MẠNG HIỆN NAY LÝ LUẬN VÀ THỰC TIỄN

✍ **TS. Lê Văn Quyến**
Phân viện Học viện Hành chính Quốc gia tại TP. Hồ Chí Minh

● **TÓM TẮT:** *Trong thời đại công nghiệp lần thứ 4, công nghệ thông tin đóng vai trò hết sức quan trọng đối với sự phát triển kinh tế- xã hội, lợi ích của việc sử dụng không gian mạng sẽ là cầu nối xóa bỏ khoảng cách không gian giữa con người với nhau. Tuy nhiên, cùng với sự tiến bộ của khoa học công nghệ thì hoạt động sử dụng không gian mạng cần có quy định pháp lý rõ ràng để đảm bảo quyền và lợi ích của cá nhân, tổ chức là hết sức cần thiết.*

● ***Từ khóa:*** *phòng, chống tội phạm, không giam mạng, quốc gia, công nghệ thông tin, luật an ninh mạng*

● **ABSTRACT:** *In the 4th industrial era, information technology plays a very important role in socio-economic development, the benefits of using cyberspace will be a bridge to eliminate the spatial distance between people. However, along with the advancement of science and technology, the use of cyberspace needs clear legal regulations to ensure the rights and interests of individuals and organizations.*

● ***Keywords:*** *Crime prevention, no cyber detention, country, information technology, cyber security law*

Ngày nhận bài: 04/3/2025. Ngày bình duyệt: 17/3/2025 Ngày duyệt đăng: 20/3/2025

Công nghệ thông tin (CNTT) luôn đóng vai trò quan trọng trong các lĩnh vực khác nhau của đời sống xã hội, cong người đã ứng dụng (CNTT) vào hầu hết các hoạt động của xã hội đem lại lợi ích thiết thực giải phóng được rất nhiều sức lao động cho con người. Hay nói khác đi sự phát triển của Ngành CNTT cung cấp các công cụ và ứng dụng để tổ chức và quản lý thông tin, tăng cường hiệu quả và hiệu suất làm việc trong các tổ chức, doanh nghiệp, sự phát triển của công nghệ thông tin đã kết nối toàn cầu tạo cơ hội cho mọi cá nhân, tổ chức có kết nối gần nhau hơn để giải quyết các công việc. Nói đến không gian mạng được hiểu là không gian ảo, không gian này được hình thành từ mạng internet qua quá trình kết nối của các mạng, bao gồm: Internet, mạng viễn thông, hệ thống máy tính, bộ xử lý và điều khiển, chứa đựng cơ sở dữ liệu, không gian mạng hoạt động, không giới hạn về không gian, thời gian"

Với thành tựu công nghệ thông tin đã đem lại rất nhiều hữu ích cho nhân loại, tuy nhiên từ khi công nghệ thông tin phát triển cho đến nay có rất nhiều cá nhân, tổ chức trong và ngoài nước đã sử dụng công nghệ thông tin vào những mục đích khác nhau xâm phạm không giam mạng làm ảnh hưởng đến lợi ích của cá nhân, tổ chức, dân tộc và quốc gia trái với quy định của pháp luật.

Để ngăn chặn những hành vi sai trái, mỗi mội quốc gia có quy định cụ thể về nghĩa vụ và trách nhiệm của công dân, tổ chức khi khai thác sử dụng công nghệ thông tin vào không gian mạng hiện nay. Ở Việt Nam đã ban hành Luật An ninh mạng bộ luật hình sự năm 2015 sửa đổi bổ sung năm 2017 đã quy định cụ thể về những hành vi nguy hiểm cho xã hội được pháp luật nghiêm cấm và phải chịu trách nhiệm hình phạt, cụ thể: ***Điều 285*** *tội sản xuất, mua bán, trao đổi hoặc tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật;* ***Điều 286*** *Tội phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử quy định tại nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 01 năm đến 05 năm;* ***Điều 287*** *Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử*; ***Điều 288*** *Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông;* ***Điều 289*** *Tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác;* ***Điều 290*** *Tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản;* ***Điều 291*** *Tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng*; ***Điều 293*** *Tội sử dụng trái phép tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn, quốc phòng, an ninh;* ***Điều 294*** *Tội cố ý gây nhiễu có hại. Hình phạt với các nhóm tội trên phạt tiền ít nhất là 5.000.000 và cao nhất có thể là 20 năm tù.*

Bên cạnh luật hình sự thì nhằm cụ thể hóa quyền lợi và trách nhiệm cuarcas nhân, tổ chức trong quá trình khai thác sử dụng không gian mang, ngày 12 tháng 6 năm 2018 Quốc hội đã ban hành Luật số: 24/2018/QH14 về Luật an ninh mạng

Với những quy định của Luật hình sự và Luật an ninh mạng hiện nay cùng với hệ thống pháp luật hiện hành của Viêt Nam đã tạo hành lang pháp lý quan trọng trong qúa trình vận hành và quản lý xã hội ngày càng thiết thực và hiệu quả. Bộ Luật hình sự và Luật an ninh mạng đã có hiệu lực thi hành, mức hình phạt cụ thể được quy định trong Bộ Luật hình sự nhưng hàng năm có rất nhiều các nhân, tổ chức vi phạm, với nhiều phương thức thủ đoạn như:

Các cuộc tấn công mạng ngoài mục đích phá hoại chính trị vào hệ thống thông tin trọng yếu của các nước ngày càng gia tăng, gây thiệt hại nghiêm trọng về kinh tế, quốc phòng và an ninh, các cuộc lợi dụng thông tin mạng để phạm tội kinh tê, lừa đảo, lợi dụng tự do dân chủ làm ảnh hưởng đến quyền lợi ích của cá nhân, tổ chức. Tội phạm trên không gian mạng ngày càng nguy hiểm với các thủ đoạn hết sức tinh vi, sử dụng các loại mã độc ứng dụng trí tuệ nhân tạo để tấn công, xâm nhập vào dự liệu của cơ quan, tổ chức cá nhân một cách bất hợp pháp để khai thác thông tin để sử dụng vào việc vi phạm pháp luật.

Theo Bộ thông tin truyền thông đến nay, có 138 quốc gia (trong đó có 95 nước đang phát triển) đã ban hành Luật An ninh mạng. Trước những tác hại của việc tấn công an ninh mạng, tháng 9-2018, Mỹ đã công bố Chiến lược An ninh mạng, Mỹ tuyên bố đáp trả bằng các biện pháp quân sự nếu an ninh mạng quốc gia bị đe dọa, tấn công; sau nước Mỹ, thì tháng 12 năm 2018, Ô-xtrây-li-a đã ban hành Luật An ninh mạng, ngoài việc nhấn mạnh tầm quan trọng của an ninh mạng, Luật này còn cho phép cơ quan chức năng được truy cập vào các dữ liệu được mã hóa của các nhà mạng.

Ở nước Việt Nam hơn gần 30 năm kết

nối internet Việt Nam đã nằm trong nhóm các quốc gia có tốc độ phát triển internet nhanh nhất thế giới, không gian mạng ở nước ta cũng xuất hiện nhiều nguy cơ, thách thức lớn tác động đến an ninh quốc gia và trật tự an toàn xã hội, cụ thể là:

Thứ nhất: Bằng hệ thống công nghệ thông tin hiện đại, các thế lực thu địch đã dùng các máy chủ đặt ở nước ngoài đtăng cường sử dụng không gian mạng để phá hoại tư tưởng, phá hoại nội bộ, thực hiện âm mưu "diễn biến hòa bình", gây mâu thuẫn dân tộc, kích động biểu tình, bạo loạn nhằm chuyển hóa thể chế chính trị tại Việt Nam. Tình trạng tinh nhắn giả, cuộc điện thoại giả lừa đảo trên mạng ngày cangd nhiều và càng tinh vi, phức tạp làm làm tổn hại đến quyền và lợi ích hợp pháp của các tổ chức, cá nhân đang diễn ra nghiêm trọng. Hoạt động tội phạm sử dụng công nghệ cao gia tăng về số vụ, thủ đoạn tinh vi, gây thiệt hại nghiêm trọng về nhiều mặt và hệ lụy lâu dài cho xã hội, trong đó có các hoạt động tội phạm, như lừa đảo, tổ chức đánh bạc trực tuyến. Theo thống kê, trung bình mỗi năm ở nước ta, qua kiểm tra, kiểm soát 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. [1].

***Thứ hai*:** Tội phạm và vi phạm pháp luật trong lĩnh vực thông tin diễn biến phức tạp, gia tăng về số vụ, thủ đoạn tinh vi, gây thiệt hại nghiêm trọng về nhiều mặt. Các hành vi phá hoại cơ sở hạ tầng thông tin; gây mất an toàn, hoạt động bình thường, vững mạnh của mạng máy tính, mạng viễn thông, phương tiện điện tử của các cơ quan, tổ chức, cá nhân và hệ thống thông tin vô tuyến điện,… đã và đang gây ra những thiệt hại lớn về kinh tế, xâm hại trực tiếp đến quyền, lợi ích hợp pháp của các cơ quan, tổ chức và cá nhân. Theo kết quả đánh giá an ninh mạng do Tập đoàn công nghệ Bkav thực hiện, trong năm 2019, chỉ tính riêng thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam đã lên tới 20.892 tỷ đồng (tương đương 902 triệu USD), hơn 1,8 triệu máy tính bị mất dữ liệu do sự lan tràn của các loại mã độc mã hóa dữ liệu tống tiền (ransomware), trong đó có nhiều máy chủ chứa dữ liệu của các cơ quan, gây đình trệ hoạt động của nhiều cơ quan, doanh nghiệp [2].

Thứ ba: Tính đến tháng 6/2023, Việt Nam xếp thứ 12 trên thế giới về tỷ lệ người dùng Internet với hơn 77 triệu người (chiếm gần 79% dân số); số lượng thuê bao di động được đăng ký lên đến hơn 156 triệu thuê bao; xếp hạng thứ 25 về chỉ số an toàn, an ninh mạng toàn cầu (do Liên minh Viễn thông quốc tế ITU công bố). Tuy nhiên, theo thống kê của hãng bảo mật quốc tế, Việt Nam nằm trong nhóm 3 quốc gia bị tấn công mạng nhiều nhất tại khu vực châu Á - Thái Bình Dương; chỉ riêng 6 tháng đầu năm 2023, các cơ quan chức năng đã phát hiện gần 17 triệu cảnh báo dấu hiệu hoạt động tấn công mạng (tăng 240% so với cùng kỳ năm 2022), trong đó có 208 hệ thống thông tin của cơ quan Nhà nước, các bộ, ban, ngành bị tin tặc tấn công nhằm mục đích đánh cắp thông tin, dữ liệu, tài liệu bí mật nhà nước thuộc nhiều lĩnh vực. Nổi lên là các chiến dịch tấn công mạng nguy hiểm của các tin tặc có nguồn gốc từ nước ngoài, sử dụng 15 biến thể mã độc nguy hiểm, trong đó có các loại mã độc hiện đại, có khả năng vô hiệu hóa các phần mềm bảo vệ để "nằm vùng" lâu dài, thâm nhập sâu vào các hệ thống, đáng chú ý có sự câu kết, móc nối giữa tin tặc trong và ngoài nước. [3].

***Thứ tư**:* các tin tặc gia tăng hoạt động tấn công mạng có chủ đích nhằm chiếm quyền điều khiển hoặc dùng mã độc để tấn công, nhất là mã độc tống tiền nhằm vào các hệ thống thông tin trọng yếu. Ngoài ra các hoạt động phát tán thông tin xấu, độc hại, thông tin sai sự thật trên không gian mạng tiếp tục tác động đến mọi mặt của đời sống xã hội; xâm phạm nghiêm trọng đến quyền, lợi ích hợp pháp của các tổ chức, cá nhân. Trong thời gian tới, hoạt động này sẽ tiếp tục gia tăng, đòi hỏi người dùng nâng cao

cảnh giác, thận trọng khi tiếp cận với những thông tin trên không gian mạng, tránh trở thành nạn nhân của tin giả.

Thứ năm, tội phạm không gian mạng còn sử dụng nhiều chiêu trò khác nhau để lừa đảo chiếm đoạt tài sản qua mạng, hoạt độngh này ngày càng diễn biến phức tạp với nhiều phương thức, thủ đoạn tinh vi, có tính chất xuyên quốc gia, gây thiệt hại lớn và bức xúc trong nhân dân, chúng thường sử dụng các phương thức: Nhắn tin hoặc gọi điện giả danh cơ quan nhà nước, giả danh các tổ chức kinh tế, chiêu trò khuyến mại, hoặc thông qua các trang mạng xã hội để quảng cáo, giới thiệu sản phẩm, giới thiệu việc nhẹ lương cao... ngoài những phương thức trên, tội phạm trên không giam mạng còn tạo lập các website, sàn giao dịch, ứng dụng kiếm tiền trên mạng, giả mạo các trang quảng cáo, rao bán các mặt hàng trực tuyến sau đó chiếm đoạt số tiền đặt cọc của khách hàng hoặc chuyển mặt hàng không đúng giá trị thực tế như quảng cáo.

Cùng với xu thể hội nhập trong điều kiện toàn cầu hóa, đa phương hóa và từ thực trạng về xâm phạm an ninh mạng ở trong nước và thế giới thì công cuộc đấu tranh, phòng chống tội phạm trên không gian mạng hiện nay ở nước ta là hết sức cần thiết và cập bách. Để thực hiện được nhiệm vụ này trước hết cần thực hiện đồng bộ một số giải pháp cơ bản sau:

Thứ nhất: đối với các cơ quan, tổ chức

Để làm tốt công tác bảo mật thôn tin của cơ quan đơn vị, mỗi coq quan tùy thuộc vào tính chất ngành nghề cần ban hành quy chế, quy định về việc sử dụng mạng, trường hợp nào, bộ phận nào trong cơ quan được kết nối với hệ thống mạng bên ngoài; có thể dùng mạng bảo mật, vận hành mạng máy tính nội bộ, máy tính kết nối Internet, cần tách bạch máy tính lưu giữ liệu với máy tính có kết nối internet; Không nên sử dụng USD, thiết bị ổ cứng rời, thẻ nhớ... đối với các máy tính có chứa thông tin, tài liệu mật; hoặc USB chuyên dụng có mã hóa cơ yếu để sao, chuyển tài liệu mật của cơ quan, đơn vị.

Thứ hai: đối với cá nhân

Mỗi cá nhân luôn phải ý thức được vai trò của công tác bảo mật các dữ liệu thông tin, các dữ liệu cá nhân, đặt mật khẩu có tính bảo mật và có sự thay đổi định kỳ; các dữ liệu luôn chủ động sao lưu ở nhiều ổ cứng, có biện pháp lưu dự phòng đối với thông tin, dữ liệu, tài liệu quan trọng; chủ động mua phần mền uy tín để (diệt virus...) các chương trình máy tính, hệ điều hành nên định kỳ cài đặt lại.

các thông tin cá nhân trước khi đăng hoặc các thông tin mà cá nhân cập nhật trên mạng cần kiểm tra, kiểm duyệt độ chính xá trước khi lưu về máy hoặc chia sẻ cho người khác; Không nên truy cập, mở những đường link, trang «web đen» hay những pop-up quảng cáo nghi ngờ; không nên mở các tệp tin, file lạ, đáng ngờ, không rõ xuất sứ được gửi qua email hay các dịch vụ OTT (zalo, viber, whatsup...); đặc biệt mã (OTP) của cá nhân không được chia sẻ qua các đường link, ứng dụng do người lạ gửi đến..

Thứ ba: hợp tác quốc tế trong công tác bảo mật an ninh mạng

Thực hiện tốt hợp tác quốc tế với các nước tiên tiến có trình độ khoa học kỹ thuật cao về công nghệ thông tin như: Ấn Độ, Pháp, Mỹ, Israel... trong công tác đấu tranh, phòng chống tội phạm trên không gian mạng, thường xuyên trao đổi với các nước để hoạc tập các kỹ năng trong công tác phòng, chống và bảo vệ an ninh mạng quốc gia.

Thứ tư: các cơ quan chức năng bảo vệ an ninh mạng quốc gia cần phối hợp chặt chẽ với các cơ sở đào tạo uy tín trong nước về đào tạo công nghệ thông tin để phối hợp phòng chống các tội phạm liên quan đến an ninh mạng

Trường đại học bách khoa, Trường đại học khoa học tự nhiên, Trường đại học công nghệ thông tin, Trường đại học FPT trong công tác chia sẻ kỹ năng, kinh nghiệm, kiến thức máy tính, kiến thức bảo mật thông tin của khoa học máy tính cũng như công tác

tuyển dụng những sinh viên tốt nghiệp loại giỏi để bổ sung cho nguồn nhân lực quốc gia trong công tác bảo vệ không gian mạng.

Thứ năm: Hoàn thiện chính sách pháp luật về an ninh mạng cũng như chính sách hình sự để đảm bảo công tác quan lý được hiệu quả hơn

Trong quá trình ban hành các Nghị định liên quan đến Luật an ninh mạng cần cụ thể hóa các nội dung như: dữ liệu cá nhân, điều kiện kinh doanh trên không giam mạng, xây dựng rõ các quy định nhằm tạo nền tảng pháp lý trong phòng ngừa, đấu tranh và xử lý các hành vi vi phạm pháp luật, ảnh hưởng tới an ninh mạng quốc gia, quyền và lợi ích hợp pháp của các tổ chức cá nhân trên không gian mạng.

Hiện nay, trong Bộ luật Hình sự chưa xây dựng được một chương riêng để cụ thể hóa các tội phạm liên quan đến an ninh mạng, công nghệ thông tin, mạng viễn thông, bổ sung thêm những tội danh quy định về những hành vi phạm tội mới dự báo sẽ phát sinh trong thời gian tới. Trong Bộ Luật hình sự cần làm, nghiên cứu, ban hành làm rõ thế nào là công cụ, thiết bị, phần mềm có tính năng tấn công mạng máy tính, mạng viễn thông, phương tiện điện tử; làm rõ những vấn đề quy định trong bộ luật hình sự như: Chương trình tin học gây hại cho mạng máy tính, mạng viễn thông là chương trình tự động hóa xử lý thông tin, gây ra hoạt động không bình thường cho mạng máy tính, mạng viễn thông hoặc sao chép, sửa đổi, xóa bỏ thông tin lưu trữ trong máy tính, phương tiện điện tử, cần tăng mức hình phạt tù trong các tội liên quan đến an ninh mạng để đủ sức răn đe, giáo dục.

Thứ sáu: tăng cường công tác tuyên truyền sâu rộng về luật an ninh mạng cũng như quy định của pháp luật hình sự về những hành vi xử dụng không gian mạng không đúng mục đích sẽ bị xử lý hình sự.

Hoạt động giáo dục, phổ biến pháp luật đúng và đầy đủ đối về an ninh mạng, chính sách hình sự về các tội phạm liên quan đến sử dụng không gian mạng sẽ góp phần nêu cao ý thức của công dân, của tổ chức trong đấu tranh, phòng ngừa bảo đảm an ninh mạng quốc gia được sử dụng một cách an toàn là hết sức cần thiết. Để thực hiện hiệu quả công tác tuyên truyền, giáo dục luật an ninh mạng cũng như chính sách hình sự liên quan đến an ninh mạng, trước mắt cần tuyên truyền sâu rộng những hành vi sau đây bị pháp luật ngăn cấm, cụ thể:

- Không sử dụng không gian mạng để thực hiện hành vi: tổ chức, hoạt động, cấu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; không xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc; thông tin sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác; không sử dụng không giam mạng để tổ chức hoạt động mại dâm, tệ nạn xã hội, mua bán người; không đăng tải thông tin dâm ô, mại dâm qua mạng, các hành vi đồi trụy, tội ác; phá hoại thuần phong mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng; xúi giục, lôi kéo, kích động người khác phạm tội.

- Nhà nước, các cơ quan chủ quan về quản lý công nghệ thông tin, tổ chức tuyên truyền để mọi cá nhân, tổ chức ý thức được tác hại của việc sử dụng công nghệ thông tin vào mục đích xấu, không tiếp tai cho các tổ chức quốc tế để sản xuất, tổ chức trong nước đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; không phát tán chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; xâm

nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác.

- Không lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi. Tuyên truyền, giáo dục để mọi người hiểu được những hành vi nào bị nghiêm cấm và xâm phạm đến các quyền con người như: quyền sống, quyền tự do ngôn luận, xâm hại bí mật đời tư; xâm hại danh dự hay uy tín cá nhân; xâm hại đến quyền tự do tư tưởng, tín ngưỡng và tôn giáo của công dân... thì sẽ phải chịu những chế tài do Luật An ninh mạng, chế tài do luật hình sự quy định.

Tóm lại: Cách mạng công nghiệp lần thứ tư của nhân loại đã mang lại cả cơ hội và thách thức cho mỗi quốc gia, dân tộc. Để bắt kịp xu thể phát triển chung về khoa học công nghệ mỗi quốc gia cần phải nắm bắt kịp thời, tận dụng hiệu quả các cơ hội; đồng thời, chủ động phòng ngừa, ứng phó để hạn chế các tác động tiêu cực, bảo đảm quốc phòng, an ninh, an toàn và tính bền vững của quá trình phát triển đất nước. Vì vậy, bảo đảm an toàn thông tin, an ninh mạng, phòng chống tội phạm mạng và các vi phạm pháp luật trên không gian mạng không chỉ là nhiệm vụ của các cơ quan chuyên trách mà là trách nhiệm của các ngành, các cấp, các cơ quan, đoàn thể, doanh nghiệp, công dân. Từ thực trạng của hoạt động xâm phạm không giam mạng của các nước trên thế giới nói chung và ở Việt Nam nói riêng, thiết nghĩ trong điều kiện hiện nay ở nước ta nếu đồng bộ các giải pháp nên trên sẽ góp phần quan trọng trong công tác bảo đảm an ninh mạng quốc gia, góp phần thúc đẩy sự phát triển kinh tế- xã hội, hợp tác quốc tế ngày càng sâu rộng đáp ứng yêu công nghiệp hóa, hiện đại hóa đất nước./.

(1). Lê Văn Thắng (2019), "*An ninh thông tin của Việt Nam trong điều kiện hiện nay: Thực trạng, vấn đề đặt ra và giải pháp*", Đề tài khoa học cấp Nhà nước, Hà Nội.

(2). Tập đoàn BKAV (2019), Báo cáo tổng kết công tác an ninh mạng năm 2019.

(3) Tạp chí khoa học và công nghệ (2023)