THỰC TRẠNG AN TOÀN THÔNG TIN MẠNG HIỆN NAY Ở VIỆT NAM VÀ GIẢI PHÁP PHÒNG CHỐNG VI PHẠM PHÁP LUẬT TRÊN KHÔNG GIAN MẠNG

● LÂM ĐÔNG HỒ - NGUYỄN XUÂN HOÀNG

TÓM TẮT:

An toàn thông tin (ATTT) là an toàn kỹ thuật cho các hoạt động của các cơ sở hạ tầng thông tin, trong đó bao gồm: an toàn phần cứng và phần mềm theo tiêu chuẩn kỹ thuật do Nhà nước ban hành; duy trì các tính chất bí mật, toàn vẹn, sẵn sàng của thông tin trong lưu trữ, xử lý và truyền dẫn trên mạng. Bài viết đã nêu rõ thực trạng ATTT mạng hiện nay ở Việt Nam, đồng thời cũng đưa ra giải pháp phòng chống vi phạm pháp luật trên không gian mạng.

Từ khóa: thực trạng, an toàn thông tin mạng, giải pháp, phòng chống vi phạm.

1. Đặt vấn đề

Luật An toàn thông tin được ban hành năm 2015 đã thể chế hóa các chủ trương, đường lối, chính sách của Đảng và Nhà nước về ATTT, đáp ứng yêu cầu phát triển bền vững kinh tế - xã hội, bảo vệ thông tin và hệ thống thông tin, góp phần bảo đảm quốc phòng, an ninh, chủ quyền và lợi ích quốc gia trên không gian mạng. Theo đó: "ATTT mạng là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin".

Trải qua 35 năm đổi mới, hệ thống thông tin của Việt Nam có sự phát triển mạnh mẽ, phục vụ đắc lực sự lãnh đạo, quản lý, điều hành của Đảng, Nhà nước, đáp ứng nhu cầu thông tin của xã hội, góp phần đảm bảo quốc phòng, an ninh của đất nước. Lĩnh vực viễn thông, Internet, tần số vô tuyến điện có sự phát triển mạnh mẽ, đạt được mục tiêu số hóa hoàn toàn mạng lưới, phát triển nhiều dịch vụ mới, phạm vi phục vụ được mở rộng, bước đầu hình thành những doanh nghiệp mạnh, có khả năng vươn tầm khu vực, quốc tế. Hệ thống bưu chính chuyển phát, báo chí, xuất bản phát triển nhanh cả về số lượng, chất lượng và kỹ thuật nghiệp vụ, có đóng góp quan trọng cho sự phát triển kinh tế - xã hội; đảm bảo quốc phòng, an ninh, đối ngoại của đất nước.

Tuy nhiên, tình hình an ninh thông tin ở Việt Nam đã và đang có những diễn biến phức tạp. Các cơ quan đặc biệt nước ngoài, các thế lực thù địch, phản động tăng cường hoạt động tình báo, gián điệp, khủng bố, phá hoại hệ thống thông tin; tán

phát thông tin xấu, độc hại nhằm tác động chính trị nội bộ, can thiệp, hướng lái chính sách, pháp luật của Việt Nam. Gia tăng hoạt động tấn công mạng nhằm vào hệ thống thông tin quan trọng quốc gia, hệ thống thông tin quan trọng về an ninh quốc gia. Theo thống kê, trung bình mỗi năm, 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. 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.

2. Nội dung

2.1. An toàn, an toàn thông tin

Theo từ điển tiếng Việt: An toàn được hiểu là trạng thái mà con người, thiết bị, môi trường được bảo vệ, phòng chống lại những tác nhân nguy hại có thể phát sinh (hoặc tiềm ẩn) do các nguyên nhân chủ quan, khách quan trong cuộc sống.

An toàn thông tin mạng "là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin".

An ninh mạng "là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân".

2.2. Tội phạm sử dụng công nghệ cao

Hiện nay luật pháp của nhiều nước trên thế giới như Australia, Mỹ, Anh đã có định nghĩa liên quan đến tội phạm này, như: tội phạm công nghệ cao (high-tech crime), tội phạm máy tính (computer crime), tội phạm liên quan đến máy tính (computer-related crime), tội phạm mạng (cybercrime),...

Trong Luật Hình sự của Australia, tội phạm công nghệ cao (high-tech crime) được định nghĩa là "sự xâm nhập máy tính một cách trái phép; sự sửa đổi trái phép dữ liệu bao gồm việc phá hủy dữ liệu; tấn công từ chối dịch vụ (DoS); tấn công từ chối dịch vụ phân tán (DDoS); tạo ra và phân phối phần mềm độc hại".

Theo Từ điển Luật học Blacks Law, tội phạm máy tính (computer crime) được định nghĩa là: "tội phạm đòi hỏi về kiến thức công nghệ máy tính, chẳng hạn như phá hoại hoặc ăn cắp dữ liệu máy tính hay sử dụng máy tính để thực hiện một số tội phạm khác".

Tại Việt Nam, theo khoản 1 Điều 3 Nghị định số 25/2014/NĐ-CP của Chính phủ ngày 07 tháng 4 năm 2014 quy định: "Tội phạm sử dụng công nghệ cao là hành vi nguy hiểm cho xã hội được quy định trong Bộ luật Hình sự có sử dụng công nghệ cao".

Theo khoản 1 Điều 3 của Luật Công nghệ cao năm 2008 quy định: "Công nghệ cao là công nghệ có hàm lượng cao về nghiên cứu khoa học và phát triển công nghệ; được tích hợp từ thành tựu khoa học và công nghệ hiện đại; tạo ra sản phẩm có chất lượng, tính năng vượt trội, giá trị gia tăng cao, thân thiện với môi trường; có vai trò quan trọng đối với việc hình thành ngành sản xuất, dịch vụ mới hoặc hiện đại hóa ngành sản xuất, dịch vụ hiện có".

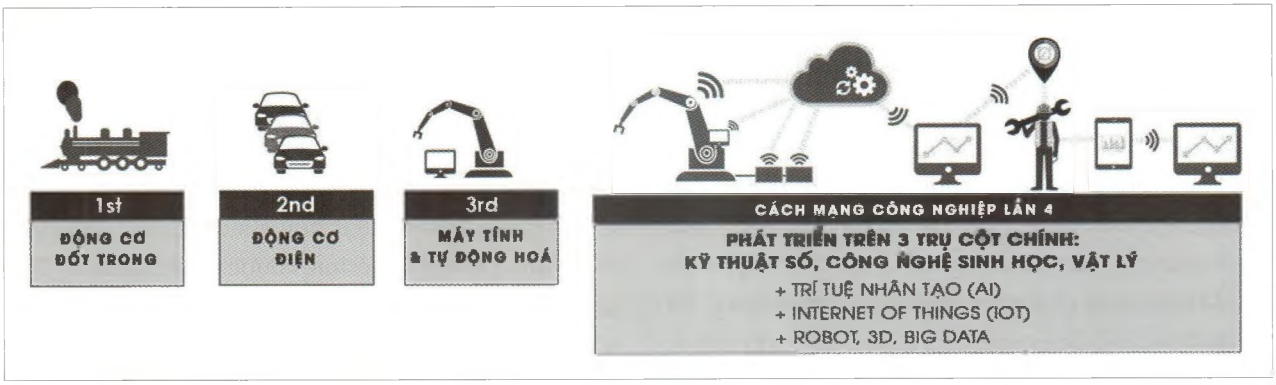
2.3. Thực trạng an toàn thông tin mạng trên thế giới và tại Việt Nam

2.3.1. Thực trạng an toàn thông tin mạng trên thế giới

Trong cuộc CMCN 4.0, thông tin là một dạng tài nguyên. Chính vì thế, đảm bảo an ninh, ATTT là nhiệm vụ quan trọng và cấp thiết. Tuy nhiên, hiện nay, các mối đe dọa từ không gian mạng không ngừng tăng lên và thay đổi nhanh chóng.

Tình hình ATTT mạng diễn biến phức tạp, liên tục xảy ra các vụ tấn công, xâm nhập, đánh cắp dữ liệu trên hệ thống mạng của các cơ quan chính phủ, các cơ sở an ninh quốc phòng, tập đoàn kinh tế, cơ quan truyền thông của nhiều quốc gia. Ví dụ như các vụ tấn công vào hệ thống thư điện tử của Bộ Ngoại giao Mỹ, hệ thống máy tính của Nhà trắng, Hạ viện Đức, Bộ Ngoại giao Australia,...

Tài chính là mục tiêu lớn nhất thúc đẩy tin tặc



hành động, với 73% số lượng các cuộc tấn công mạng; chính trị, tình báo là mục tiêu lớn thứ hai, với 21% các cuộc tấn công.

2.3.2. Thực trạng an toàn thông tin ở Việt Nam

Năm 2011, có trên 1.500 cổng thông tin Việt Nam bị tin tặc sử dụng mã độc gián điệp dưới hình thức tập tin hình ảnh xâm nhập, kiểm soát, cài mã độc thay đổi giao diện trang chủ.

Trong năm 2012 - 2013, Bộ Công an đã phát hiện gần 6.000 lượt cổng thông tin, trang tin điện tử của Việt Nam (trong đó có hơn 300 trang của cơ quan nhà nước) bị tấn công, chỉnh sửa nội dung và cài mã độc.

Năm 2014, sau sự kiện giàn khoan HD 981 hạ đặt trái phép trong vùng đặc quyền kinh tế Việt Nam, tin tặc nước ngoài đã tấn công hơn 700 trang mạng Việt Nam và hơn 400 trang trong dịp Quốc khánh (2/9) để chèn các nội dung xuyên tạc chủ quyền của Việt Nam với quần đảo Hoàng Sa.

Vào cuối năm 2014, tin tặc cũng đã mở đợt tấn công vào trung tâm dữ liệu của VCCorp khiến nhiều tờ báo mà công ty này đang vận hành kỹ thuật như Soha, Kenh14... bị tê liệt.

Năm 2015, có trên 2.460 website của các cơ quan, doanh nghiệp bị xâm nhập. Nguy cơ từ mã độc và Internet of Things (IoT) bùng nổ tạo "thị trường" lớn cho hacker là những nguy cơ an ninh mạng mà người dùng phải đối mặt.

Nổi bật trong năm 2016 là cuộc tấn công mạng vào một số màn hình hiển thị thông tin chuyến bay tại khu vực làm thủ tục chuyến bay của các sân bay quốc tế Tân Sơn Nhất, sân bay quốc tế Nội Bài, sân bay quốc tế Đà Nẵng, sân bay Phú Quốc. Các màn hình của sân bay đã bị chèn những hình ảnh và nội dung xuyên tạc về biển Đông.

Năm 2017, mã độc tống tiền (ransomware) có tên là Wanna Cry trở thành mối nguy hiểm. Tại Việt Nam, ghi nhận hơn 100 máy tính bị nhiễm độc. Wanna Cry là một loại mã nhiễm độc tấn công vào máy nạn nhân qua tệp tin đính kèm email hoặc đường link độc hại.

Năm 2018, thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam đã lên mức kỷ lục 14.900 tỷ đồng, tương đương 642 triệu USD, nhiều hơn 21% so với mức thiệt hại của năm 2017.

Theo số liệu của Bộ Thông tin và Truyền thông, trong tổng số 3.159 cuộc tấn công mạng vào các hệ thống thông tin tại Việt Nam trong 6 tháng đầu năm 2019, có 968 cuộc tấn công thay đổi giao diện, 635 cuộc tấn công cài mã độc (Malware) và 1.556 cuộc tấn công lừa đảo.

Trong 4 tháng đầu năm 2020, tổng cộng 1.056 cuộc tấn công mạng vào các hệ thống thông tin tại Việt Nam dẫn đến sự cố (553 Phishing, 280 Deface, 223 Malware). Hơn 73.000 camera IP trên thế giới, trong đó có gần 1.000 camera tại Việt Nam đang bị theo dõi. Nguyên nhân là do người dùng chưa có thói quen quan tâm đến an ninh của những thiết bị này, không thay đổi mật khẩu mặc định của hệ thống trước khi kết nối Internet. Bảo mật các thiết bị IoT là rất quan trọng, đặc biệt khi người dùng chưa có thói quen quan tâm đến an ninh cho các thiết bị này.

Trong năm 2019, số cuộc tấn công mạng vào

các hệ thống thông tin Việt Nam có chiều hướng giảm (khoảng 45,9%) so với cùng kỳ năm 2018.

Trong 4 tháng đầu năm 2020, số cuộc tấn công mạng vào các hệ thống thông tin tại Việt Nam đã giảm (khoảng 51,4%) so với cùng kỳ năm 2019.

Đạt được những kết quả trên cho thấy việc nâng cao nhận thức, kỹ năng về đảm bảo an toàn, an ninh mạng cho các cơ quan, tổ chức và người dùng, thông qua các hội nghị, hội thảo cũng như các chương trình tập huấn, diễn tập. Bên cạnh đó, các quy định, chế tài pháp luật đã đầy đủ và có tính răn đe hơn như sự ra đời của Luật An ninh mạng có hiệu lực từ ngày 01/01/2019. Sự phối hợp và tuân thủ của các tổ chức Internet lớn trên thế giới với luật pháp Việt Nam cũng tốt hơn. Đặc biệt, nhận thức về ATTT của tổ chức, cá nhân đã được nâng cao, các biện pháp phòng vệ chủ động đã tốt hơn, công tác đánh giá an toàn thông tin được thực hiện nhiều hơn.

Trong Chỉ thị 01/CT-BTTTT ngày 03/01/2020 về định hướng phát triển ngành Thông tin và Truyền thông năm 2020, Bộ trưởng Bộ Thông tin và Truyền thông đã nhấn mạnh: "An toàn, an ninh mạng là điều kiện tiên quyết để phát triển Chính phủ điện tử và chuyển đổi số, do đó phải đi trước một bước."

Chỉ thị 01 nêu rõ các chỉ tiêu cần đạt được trong năm 2020 của lĩnh vực an toàn, an ninh mạng như: 100% cơ quan, tổ chức tại Việt Nam triển khai bảo vệ an toàn, an ninh mạng theo mô hình 4 lớp; 100% bộ, ngành, địa phương triển khai các giải pháp điều hành, giám sát an toàn, an ninh mạng, phòng chống mã độc tập trung, kết nối chia sẻ thông tin với Trung tâm giám sát an toàn không gian mạng quốc gia của Bộ Thông tin và Truyền thông.

2.3.3. Sự nguy hiểm của mã độc và một số vấn đề cần lưu ý khi sử dụng các ứng dụng trực tuyến

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. Đặc biệt khi dư luận xã hội quan tâm nhiều tới tình hình diễn biến của dịch bệnh Covid-19 và các thông báo, hướng dẫn về phòng dịch của cơ quan chức năng, các tổ chức y tế thì tin tặc đã gia tăng giả mạo các thông báo, hướng dẫn này để phát tán mã độc và thực hiện các cuộc tấn công lừa đảo. Hơn nữa, khi các quốc gia trên thế giới triển khai các biện pháp cách ly, giảm giao tiếp xã hội để hạn chế lây lan dịch bệnh, nhiều cơ quan, tổ chức, doanh nghiệp chuyển sang làm việc trên môi trường mạng trong thời gian ngắn dẫn đến một số hạn chế, như:

(1) Tin tặc can thiệp vào dữ liệu trực tuyến như thay đổi nội dung, chèn các nội dung không phù hợp;

(2) Nhà sản xuất ứng dụng thu thập trái phép dữ liệu cá nhân của người dùng và chia sẻ với các bên thứ ba mà người dùng không biết;

(3) Dữ liệu bí mật nhà nước, bí mật kinh doanh, bí mật nội bộ của các cơ quan, tổ chức, doanh nghiệp bị lộ khi người dùng trao đổi qua các ứng dụng trực tuyến;

(4) Tin tặc thông qua tấn công các ứng dụng trực tuyến để kiểm soát camera, micro trên thiết bị của người dùng;

(5) Lượng người dùng tăng đột biến nhưng nhà sản xuất không kịp thời nâng cấp phần mềm, hạ tầng kỹ thuật phù hợp dẫn đến chất lượng dịch vụ giảm.

3. Giải pháp phòng, chống vi phạm pháp luật trên không gian mạng

3.1. Cơ sở pháp lý

Bộ luật Hình sự năm 2015 sửa đổi bổ sung năm 2017 (Gọi tắt là Bộ luật Hình sự) có hiệu lực thi hành từ ngày 01/01/2018 (gồm 26 Chương và 526 Điều), trong đó các hành vi vi phạm pháp luật trên không gian mạng được quy định tại Mục 2. Tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông Chương XII gồm các Điều 285 đến 294.

Luật An toàn thông tin 2015 có hiệu lực thi hành từ ngày 01/7/2016 (gồm 8 Chương và 54 Điều).

Luật An ninh mạng 2018 có hiệu lực thi hành từ ngày 01/01/2019 (gồm 7 Chương, 43 Điều) [6].

3.2. Các biện pháp:

Thứ nhất: Giáo dục nâng cao nhận thức về bảo vệ chủ quyền quốc gia, các lợi ích và sự nguy hại đến từ không gian mạng.

Ngày nay, quan niệm về lãnh thổ, chủ quyền, biên giới của một quốc gia không chỉ là đất liền, hải đảo, vùng biển và vùng trời, mà cả lãnh thổ không gian mạng, chủ quyền không gian mạng. Theo đó, lãnh thổ không gian mạng là một bộ phận hợp thành lãnh thổ quốc gia, nơi xác định biên giới mạng và thực thi chủ quyền quốc gia trên không gian mạng.

Thứ hai: Tuyên truyền, phổ biến, giáo dục các quy định của pháp luật về quản lý không gian mạng.

Các hình thức giáo dục cần được vận dụng đa dạng, phong phú và linh hoạt như: phối hợp giữa cơ quan chức năng với các cơ quan, địa phương, đơn vị, doanh nghiệp, cơ sở giáo dục tổ chức nói chuyện chuyên đề, phổ biến pháp luật; tuyên tuyền Luật An ninh mạng; các cuộc thi tìm hiểu về ATTT; góp ý xây dựng chương trình giáo dục ATTT mạng của các cơ sở giáo dục hoặc tham gia biên soạn các tài liệu liên quan đến ATTT mạng.

Thứ ba: Bồi dưỡng kỹ năng nhận diện các âm mưu, thủ đoạn tấn công mạng và các hình thái phát sinh trên không gian mạng.

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; cài gắm 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 (theo tệp đính kèm trong email hoặc ẩn trong quảng cáo Skype); 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,...

Thứ tư: Nâng cao ý thức phòng tránh, tự vệ và sử dụng biện pháp kỹ thuật để khắc phục hậu quả trong trường hợp bị tấn công trên không gian mạng.

Nêu cao ý thức chính trị, trách nhiệm, nghĩa vụ công dân đối với nhiệm vụ bảo vệ không gian mạng quốc gia. Tuân thủ quy định của pháp luật về bảo vệ an ninh mạng; kịp thời cung cấp thông tin liên quan đến an ninh mạng, nguy cơ đe dọa an ninh mạng và các hành vi xâm phạm khác, thực hiện yêu cầu và hướng dẫn của cơ quan quản lý nhà nước có thẩm quyền; giúp đỡ, tạo điều kiện cho người có trách nhiệm tiến hành các biện pháp bảo vệ an ninh mạng.

Thứ năm: Phát huy vai trò, trách nhiệm của các cơ quan chuyên trách an ninh mạng, lãnh đạo, quản lý các địa phương, cơ quan, đơn vị, doanh nghiệp, nhà trường trong giáo dục nâng cao ý thức làm chủ và bảo vệ không gian mạng.

4. Kết luận

Trong thời đại cách mạng công nghiệp 4.0, an ninh thông tin ngày càng trở thành một nội dung quan trọng của an ninh quốc gia. Nghiên cứu về an ninh thông tin, bảo đảm an ninh thông tin luôn là một yêu cầu bức thiết. Ngày nay, an ninh thông tin dần trở thành một bộ phận quan trọng của an ninh quốc gia. Nguy cơ gây mất an ninh thông tin là mối đe dọa lớn và ngày càng gia tăng đối với an ninh quốc gia. Bài viết tập trung phân tích, làm rõ tình hình an ninh thông tin ở Việt Nam trong điều kiện hiện nay, chỉ rõ những vấn đề đang đặt ra trong bảo đảm an ninh thông tin và các giải pháp trọng tâm nhằm nâng cao hiệu quả bảo đảm an ninh thông tin của Việt Nam thời gian tới ■

TÀI LIỆU THAM KHẢO:

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. Bộ Công an (2018), *Báo cáo số 403/BC-A68-P1 ngày 13/3/2018 "Báo cáo sơ kết 04 năm thực hiện Chỉ thị số 28-CT/TW của Ban Bí thư về tăng cường công tác bảo đảm an ninh, an toàn thông tin mạng trong tình hình mới"*.

3. Học viện Cảnh sát nhân dân - Hội đồng lý luận Bộ Công an (2019). *Bộ từ điển nghiệp vụ Công an nhân dân Việt Nam,* Nhà xuất bản Công an nhân dân.

4. Học viện Cảnh sát nhân dân, (2015). *Giáo trình Những vấn đề cơ bản về phòng, chống tội phạm sử dụng công nghệ cao,* Nhà xuất bản Công an nhân dân.

5. Trường Đại học Kỹ thuật - Hậu cần Công an nhân dân, (2020). *Giáo trình An toàn dịch vụ mạng,* Nhà xuất bản Công an nhân dân.

6. Quốc hội (2015), *Luật An toàn thông tin mạng 2015.*

7. Quốc hội (2018), *Luật An ninh mạng 2018.*

8. Bộ Chính trị (2018), Nghị quyết 30-NQ/TW ngày 25/07/2018 về Chiến lược an ninh mạng quốc gia.

9. Chính phủ (2019), *Nghị quyết 22/NQ-CP ngày 18/2/2019 về ban hành Chương trình hành động thực hiện Nghị quyết số 30-NQ/TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược An ninh mạng quốc gia.*

10. Chính phủ (2018), *Chỉ thị 02/CT-TTg ngày 4/7/2018 về công tác bảo vệ bí mật nhà nước trên không gian mạng.*

Ngày nhận bài: 27/8/2022
Ngày phản biện đánh giá và sửa chữa: 16/9/2022
Ngày chấp nhận đăng bài: 11/10/2022

Thông tin tác giả:
2. ThS. LÂM ĐÔNG HỒ
2. ThS. NGUYỄN XUÂN HOÀNG
Trường Đại học Kiên Giang

THE CURRENT SITUATION OF INFORMATION SECURITY IN VIETNAM AND SOLUTIONS TO PREVENT VIOLATIONS OF LAW IN CYBERSPACE

● Master. **LAM DONG HO**[1]
● Master. **NGUYEN XUAN HOANG**[1]
[1]Kien Giang University

ABSTRACT:

Information security is the practice of protecting information, ensuring confidentiality, integrity and availability of information, and securing information transmission and information infrastructure. Information security includes hardware and software security according to technical standards promulgated by the state. This paper provides an overview on information security in Vietnam and proposes solutions to prevent violations of law in cyberspace.

Keywords: current situation, network information security, solutions, violation prevention.