Tác động của an ninh mạng đến an ninh lương thực quốc gia trong kỷ nguyên số

ThS. TRẦN XUÂN QUỲNH
Học viện Phụ nữ Việt Nam; Email: xuanquynh@vwa.edu.vn

Tóm tắt: *An ninh lương thực và an ninh mạng có mối quan hệ ngày càng chặt chẽ trong bối cảnh Cách mạng công nghiệp 4.0. Việc ứng dụng các công nghệ số như IoT, AI, dữ liệu lớn và tự động hóa giúp nâng cao năng suất nhưng đồng thời tạo ra nhiều lỗ hổng bảo mật, khiến chuỗi cung ứng lương thực dễ trở thành mục tiêu tấn công. Các cuộc tấn công mạng có thể gây gián đoạn sản xuất, chế biến, vận chuyển và giao dịch, dẫn tới thiệt hại kinh tế, xã hội và đe dọa an ninh quốc gia. Bài viết đề xuất chiến lược toàn diện kết hợp kỹ thuật, chính sách và hợp tác công - tư nhằm bảo vệ hệ thống lương thực bền vững trong kỷ nguyên số.*

Từ khóa: *an ninh mạng; an ninh lương thực; chuỗi cung ứng lương thực, chính sách quốc gia; kỷ nguyên số.*

1. Đặt vấn đề

Theo Liên Hợp Quốc, dân số thế giới sẽ tăng từ 7,5 tỷ người hiện nay lên khoảng 10 tỷ người vào năm 2050, kéo theo sản xuất nông nghiệp sẽ cần phải tăng thêm 70% để đáp ứng nhu cầu về lương thực của con người vào thời điểm đó. Việc đảm bảo an ninh lương thực là vấn đề cấp thiết, nhất là trong bối cảnh tình trạng xung đột và bất ổn chính trị, dịch bệnh và biến đổi khí hậu kéo theo các nguy cơ về thảm họa thiên nhiên và ô nhiễm môi trường, khan hiếm nguồn nước đang diễn biến ngày càng phức tạp, khó lường[1]. Tổ chức Lương thực và Nông nghiệp Liên Hợp Quốc (FAO) đã đặt ra vấn đề an ninh lương thực trong bối cảnh gia tăng dân số, đặc biệt ở các nước kém phát triển, suy thoái môi trường, biến đổi khí hậu, sản xuất lương thực tăng trưởng chậm, giá lương thực tăng nhanh, sản xuất □xăng□sinh học và khủng hoảng kinh tế. Các vấn đề này sẽ gây ra mối đe doạ suy dinh dưỡng và đói trên quy mô lớn, làm bất ổn về xã hội, đặc biệt ở các nước nghèo và có điều kiện tự nhiên khắc nghiệt[2].

Quá trình chuyển dịch từ mô hình an ninh lương thực (ANLT) truyền thống sang hệ thống ngày càng phụ thuộc vào công nghệ đã hình thành một mối liên hệ mới giữa ANLT và an ninh mạng (ANM). Những tiến bộ khoa học - công nghệ trong bối cảnh Cách mạng công nghiệp lần thứ tư đã thúc đẩy việc ứng dụng hàng loạt công nghệ mới như cảm biến, Internet vạn vật (IoT), trí tuệ nhân tạo (AI), dữ liệu lớn, hệ thống nhúng, mạng truyền thông và robot trong lĩnh vực nông nghiệp và thực phẩm. Việc tích hợp các công nghệ này vào chu trình quản lý nông trại được kỳ vọng sẽ góp phần gia tăng cả năng suất và chất lượng nông sản, qua đó nâng cao hiệu quả của hệ thống lương thực. Giai đoạn phát triển này thường được gọi là Nông nghiệp 4.0. Trong mô hình nông nghiệp mới, nông trại thông minh được xem là một hệ thống vật lý - không gian mạng, trong đó các hoạt động sản xuất có thể được giám sát và điều khiển thông qua các hệ thống máy tính và truyền thông, với sự tham gia của các tác nhân được kết nối mạng như cảm biến, bộ truyền động, đơn vị xử lý điều khiển và thiết bị truyền thông. Như Zanella và cộng sự đã chỉ ra, việc khai thác các công nghệ mới nổi

trong nông nghiệp thông minh đồng thời làm gia tăng mức độ phức tạp của hệ thống, khiến các rủi ro và lỗ hổng an ninh vốn tồn tại trong các công nghệ này được tích hợp trực tiếp vào nông trại, qua đó làm gia tăng tính dễ tổn thương trước các mối đe dọa an ninh[3].

2. Cơ sở lý thuyết

ANLT là một khái niệm đa chiều, theo Tổ chức Lương thực và Nông nghiệp Liên Hợp Quốc (FAO), ANLT tồn tại khi "tất cả mọi người, vào mọi thời điểm, đều có quyền tiếp cận về vật chất, xã hội và kinh tế đối với đủ lương thực, an toàn và bổ dưỡng để đáp ứng nhu cầu ăn uống và sở thích thực phẩm cho một cuộc sống năng động và khỏe mạnh"[4]. Còn theo quan điểm của Lê Anh Thực (2018) "An ninh lương thực quốc gia là sự bảo đảm có đầy đủ và ổn định của mỗi quốc gia về nguồn lương thực cho người dân để họ tiếp cận và tiêu dùng đáp ứng một cuộc sống năng động, khỏe mạnh; hạn chế và đẩy lùi tình trạng thiếu lương thực, nạn đói và tình trạng phụ thuộc vào nguồn lương thực nhập khẩu; đảm bảo phát huy lợi thế cạnh tranh trong sản xuất lương thực (nếu có) và thu nhập của người sản xuất lương thực"[5].

Tương tự, an ninh mạng là hoạt động bảo vệ các hệ thống máy tính, mạng, dữ liệu và thiết bị khỏi các cuộc tấn công và truy cập trái phép[6]. Vai trò của ANM là đảm bảo tính bảo mật, toàn vẹn và khả dụng của các hệ thống thông tin. Thực tiễn cho thấy tội phạm mạng đang ngày càng gia tăng cả về quy mô lẫn mức độ thiệt hại, với khoảng một nửa số vụ tội phạm liên quan đến tài sản toàn cầu có nguồn gốc từ không gian mạng, thiệt hại kinh tế do các cuộc tấn công này ước tính vượt quá 1% GDP hằng năm của nhiều quốc gia và trong một số trường hợp tấn công nhằm vào cơ sở hạ tầng trọng yếu, mức tổn thất có thể lên tới 6% GDP[7].

Từ góc độ lý thuyết truyền thông, đặc biệt là lý thuyết Sử dụng và Hài lòng, các chủ thể tham gia vào hệ thống nông nghiệp số được xem là những người sử dụng truyền thông số một cách chủ động nhằm thỏa mãn các nhu cầu thông tin và chức năng. Mức độ hài lòng của người sử dụng phụ thuộc vào khả năng của hệ thống truyền thông trong việc cung cấp thông tin chính xác, hỗ trợ ra quyết định và nâng cao hiệu quả hoạt động[8], [9]. Trong môi trường truyền thông số, các nhu cầu này được mở rộng sang các yêu cầu về khả năng kiểm soát, độ tin cậy và mức độ an toàn của hệ thống truyền thông[10]. Trong bối cảnh nông nghiệp thông minh, các hệ thống Internet vạn vật (IoT) đóng vai trò là hạ tầng truyền thông cốt lõi nhưng đồng thời cũng làm gia tăng các thách thức về an ninh mạng, có thể ảnh hưởng trực tiếp đến độ tin cậy của thông tin và hiệu quả vận hành của hệ thống nông nghiệp[11]. Do đó, an ninh mạng trở thành điều kiện nền tảng để các hệ thống truyền thông nông nghiệp số đáp ứng được các nhu cầu sử dụng, góp phần bảo đảm an ninh lương thực quốc gia trong kỷ nguyên số.

Bên cạnh đó, việc triển khai các giải pháp AI trong môi trường thực tế là một thách thức khác được ghi nhận trong lĩnh vực nông nghiệp. Phần lớn các giải pháp an ninh, chẳng hạn như hệ thống phát hiện phần mềm độc hại, tấn công DoS/DDoS và phát hiện xâm nhập cho UAV, vẫn chưa được triển khai. Những giải pháp này rất quan trọng để phát hiện và giảm thiểu các mối đe dọa an ninh mạng đối với trang trại. Việc triển khai các giải pháp AI cũng có thể làm lộ ra các vấn đề về khả năng mở rộng và tính ổn định có thể phát sinh trong quá trình sử dụng. Ngoài ra, các hiện tượng như trôi dữ liệu và trôi mô hình có thể xảy ra khi triển khai các mô hình, điều này cũng đòi hỏi phải chú ý để sử dụng AI như một công cụ hỗ trợ ra quyết định[12].

3. Mối đe dọa an ninh mạng đối với chuỗi cung ứng lương thực

Các nghiên cứu cho thấy quá trình số hóa và sự hội tụ giữa công nghệ thông tin (IT) và công nghệ vận hành (OT) đã làm gia tăng đáng kể mức độ dễ tổn thương của chuỗi cung ứng lương thực trước các mối đe dọa an ninh mạng. Việc ứng dụng rộng rãi các hệ thống số trong toàn bộ chuỗi, từ sản xuất đến phân phối, khiến hệ thống lương thực trở thành mục tiêu tiềm năng của các cuộc tấn công mạng có khả năng gây tác động lan tỏa.

Ở cấp độ sản xuất, các trang trại hiện đại ngày

càng phụ thuộc vào các hệ thống tự động hóa và Internet vạn vật (IoT) như cảm biến môi trường, hệ thống tưới tiêu tự động và máy móc nông nghiệp kết nối mạng. Theo các nghiên cứu về an ninh nông nghiệp số, các cuộc tấn công mạng có thể làm gián đoạn hoạt động của thiết bị thông qua mã độc tống tiền hoặc làm sai lệch dữ liệu môi trường, dẫn đến các quyết định canh tác không phù hợp và gây thiệt hại trực tiếp cho mùa vụ[13]. Dù các sự cố quy mô lớn ở cấp độ này chưa phổ biến, những vụ tấn công nhằm vào các doanh nghiệp nông nghiệp toàn cầu đã được ghi nhận, cho thấy mức độ rủi ro là không thể xem nhẹ [14].

Ở khâu chế biến và sản xuất thực phẩm, các nhà máy sử dụng phổ biến các hệ thống điều khiển công nghiệp SCADA/ICS để giám sát dây chuyền sản xuất và bảo quản. Các nghiên cứu chỉ ra rằng đây là một trong những mắt xích dễ bị tổn thương nhất trong chuỗi cung ứng lương thực. Một cuộc tấn công ransomware có thể khiến hoạt động sản xuất bị tê liệt trong thời gian dài. Trường hợp tấn công vào Tập đoàn JBS S.A. năm 2021 là minh chứng điển hình, khi nhiều nhà máy chế biến thịt tại Mỹ buộc phải tạm thời đóng cửa, gây gián đoạn nguồn cung và ảnh hưởng đến thị trường thực phẩm[15].

Ở cấp độ logistics và phân phối, các hệ thống quản lý chuỗi cung ứng, vận tải và kho bãi thông minh phụ thuộc chặt chẽ vào hạ tầng công nghệ thông tin. Các nghiên cứu về an ninh logistics cho thấy, tấn công mạng vào hệ thống điều phối có thể gây gián đoạn vận chuyển, làm chậm quá trình đưa thực phẩm ra thị trường, đặc biệt là các mặt hàng tươi sống. Sự cố tấn công Colonial Pipeline tại Mỹ, dù không trực tiếp liên quan đến lương thực, đã cho thấy rõ tác động dây chuyền của việc gián đoạn logistics đối với các chuỗi cung ứng thiết yếu và tâm lý xã hội [16].

Ở cấp độ thị trường, các sàn giao dịch nông sản và hệ thống thanh toán điện tử cũng đối mặt với nguy cơ bị tấn công mạng nhằm gây gián đoạn giao dịch hoặc thao túng giá cả. Những tác động này không chỉ gây thiệt hại kinh tế cho doanh nghiệp mà còn ảnh hưởng đến khả năng tiếp cận lương thực của người tiêu dùng, qua đó đặt ra thách thức đối với ổn định xã hội trong bối cảnh hệ thống lương thực ngày càng phụ thuộc vào các nền tảng số.

4. Đánh giá các tác động của nguy cơ an ninh mạng lên an ninh lương thực quốc gia

Khi chuỗi cung ứng lương thực trở thành mục tiêu tấn công mạng, rủi ro không dừng ở sự cố kỹ thuật mà chuyển hóa thành các tác động trực tiếp đến an ninh lương thực quốc gia thông qua ba cơ chế chính: gián đoạn vận hành, suy giảm độ tin cậy của thông tin và đứt gãy khả năng tiếp cận lương thực.

Trước hết, tác động kinh tế thể hiện rõ ở cả chi phí trực tiếp và gián tiếp. Chi phí trực tiếp bao gồm khôi phục hệ thống, ứng cứu sự cố và chi phí phát sinh từ tấn công mã độc tống tiền. Trường hợp JBS S.A. cho thấy doanh nghiệp có thể phải chi khoản tiền chuộc lớn để sớm khôi phục hoạt động; riêng vụ việc này được ghi nhận ở mức 11 triệu USD[17]. Tuy nhiên, phần thiệt hại đáng kể hơn thường nằm ở chi phí gián tiếp như gián đoạn sản xuất, đứt nhịp phân phối, thất thu doanh thu, tổn hại uy tín và biến động giá lương thực khi nguồn cung bị thu hẹp trong ngắn hạn. Các yếu tố này cộng hưởng sẽ làm suy giảm □tính sẵn có□ và □tính ổn định□ của nguồn lương thực - hai thành tố then chốt của an ninh lương thực.

Tiếp đến, tác động xã hội xuất hiện khi đứt gãy vận hành chuyển thành đứt gãy khả năng tiếp cận. Chỉ cần một mắt xích quan trọng như nhà máy chế biến, kho lạnh hoặc vận tải bị tê liệt, thị trường có thể nhanh chóng chứng kiến thiếu hụt cục bộ, đặc biệt ở các đô thị phụ thuộc cao vào hệ thống phân phối tập trung. Từ thiếu hụt cục bộ có thể dẫn tới tâm lý lo ngại, hành vi mua gom và làm trầm trọng thêm cú sốc cung. Sự kiện Colonial Pipeline dù xảy ra trong lĩnh vực nhiên liệu vẫn là ví dụ cho thấy tấn công mạng có thể kích hoạt hiệu ứng dây chuyền về logistics và tâm lý xã hội, tạo ra làn sóng tích trữ trên diện rộng[18]. Với lương thực, hiệu ứng này thường nhạy cảm hơn vì liên quan trực tiếp đến nhu cầu thiết yếu hằng ngày.

Ngoài ra, trong bối cảnh quản trị số, tấn công

mạng nhằm vào hạ tầng thông tin của cơ quan nhà nước cũng có thể làm suy giảm năng lực hỗ trợ sản xuất và ứng phó rủi ro. Các nền tảng cung cấp dữ liệu canh tác, nguồn lực và dịch vụ công cho cộng đồng nông nghiệp (ví dụ các cổng thông tin hỗ trợ ra quyết định, hỗ trợ thiên tai, hay công cụ tiếp cận nguồn lực) có vai trò rút ngắn độ trễ thông tin và nâng cao hiệu quả điều hành. Vì vậy, nếu hạ tầng này bị tấn công hoặc gián đoạn, việc chia sẻ nguồn lực và cung cấp dịch vụ cho nông dân có thể bị chậm trễ làm giảm hiệu quả điều phối và năng lực chống chịu của hệ thống lương thực[19].

Cuối cùng, ở cấp độ chính trị và an ninh quốc gia, một cuộc tấn công thành công vào chuỗi cung ứng lương thực có thể bị xem như hành vi phá hoại có chủ đích, nhất là khi nhắm vào các mắt xích trọng yếu (chế biến quy mô lớn, kho lạnh, vận tải, hệ thống dữ liệu điều phối). Nhận thức về mối liên hệ giữa an ninh mạng và an ninh lương thực đã thúc đẩy nhiều quốc gia, đặc biệt là Hoa Kỳ tăng cường khung chính sách nhằm giảm thiểu lỗ hổng trong chuỗi cung ứng thực phẩm; chẳng hạn FSMA do FDA thực thi đã ghi nhận bối cảnh rủi ro mới, trong đó có các mối đe dọa mạng gia tăng[20]. Điều này cho thấy bảo đảm an ninh lương thực trong kỷ nguyên số không thể tách rời yêu cầu quản trị rủi ro an ninh mạng, đòi hỏi cơ chế phòng ngừa, giám sát và phối hợp ứng phó giữa nhà nước, doanh nghiệp và các chủ thể trong chuỗi.

5. Thách thức trong bảo đảm an ninh mạng cho chuỗi cung ứng lương thực

Việc bảo đảm an ninh mạng cho chuỗi cung ứng lương thực hiện nay đang đối mặt với nhiều thách thức mang tính cấu trúc. Trước hết, mức độ số hóa và năng lực bảo vệ an ninh mạng không đồng đều giữa các chủ thể trong chuỗi, đặc biệt giữa doanh nghiệp lớn và doanh nghiệp quy mô nhỏ, làm gia tăng nguy cơ xuất hiện các □điểm yếu hệ thống□ Các nghiên cứu cho thấy các doanh nghiệp nhỏ trong lĩnh vực nông nghiệp - thực phẩm thường thiếu nguồn lực tài chính, nhân sự chuyên môn và khung quản trị an ninh mạng chuẩn hóa, khiến chúng dễ trở thành mục tiêu của các cuộc tấn công mạng[21].

Bên cạnh đó, cơ chế phối hợp và chia sẻ thông tin về mối đe dọa mạng giữa khu vực công và khu vực tư còn hạn chế, làm suy giảm khả năng phát hiện sớm và ứng phó kịp thời với các sự cố an ninh mạng. Thực tế từ vụ tấn công ransomware vào JBS Foods cho thấy các lỗ hổng trong phối hợp ứng phó có thể gây gián đoạn nghiêm trọng chuỗi cung ứng lương thực ở quy mô lớn[22].

Ngoài ra, yếu tố con người tiếp tục là thách thức đáng kể khi nhận thức và kỹ năng an toàn thông tin của đội ngũ quản lý và người lao động chưa theo kịp mức độ tinh vi ngày càng gia tăng của các hình thức tấn công mạng, đặc biệt trong bối cảnh ứng dụng rộng rãi các công nghệ nông nghiệp thông minh và IoT[23], [24]. Cuối cùng, việc tích hợp an ninh mạng vào các chiến lược an ninh lương thực quốc gia vẫn chưa được chú trọng đầy đủ, dẫn đến thiếu sự gắn kết giữa mục tiêu bảo đảm an ninh thông tin và mục tiêu ổn định, bền vững của hệ thống lương thực [25], [26].

6. Khuyến nghị tăng cường an ninh mạng nhằm bảo đảm an ninh lương thực quốc gia

Trên cơ sở các thách thức an ninh mạng đối với chuỗi cung ứng lương thực, bài viết đề xuất một số khuyến nghị trọng tâm nhằm tăng cường bảo đảm an ninh lương thực quốc gia trong bối cảnh chuyển đổi số. Trước hết, Nhà nước cần hoàn thiện khung chính sách và pháp lý về an ninh mạng cho chuỗi cung ứng lương thực, đồng thời tích hợp an ninh mạng như một nội dung cốt lõi trong chiến lược an ninh lương thực quốc gia, nhằm nâng cao tính ổn định và bền vững của hệ thống lương thực

Bên cạnh đó, các doanh nghiệp và chủ thể tham gia chuỗi cung ứng cần nâng cao năng lực quản trị an ninh mạng, thông qua áp dụng các khung quản trị rủi ro phù hợp, đầu tư cho đào tạo nguồn nhân lực và xây dựng quy trình ứng phó sự cố thay vì chỉ tiếp cận an ninh mạng ở góc độ kỹ thuật đơn lẻ. Đồng thời, tăng cường hợp tác công - tư và cơ chế chia sẻ thông tin về mối đe dọa mạng là yếu tố then chốt nhằm nâng cao năng lực cảnh báo sớm và giảm thiểu gián đoạn chuỗi cung ứng lương thực, như đã được minh chứng qua các sự cố an

ninh mạng trong ngành thực phẩm toàn cầu[27].

Về lâu dài, an ninh mạng cần được nhìn nhận như một yếu tố nền tảng của hệ thống lương thực hiện đại, gắn chặt với mục tiêu ổn định, bền vững và nâng cao khả năng chống chịu của an ninh lương thực quốc gia trong kỷ nguyên số, đặc biệt trong bối cảnh ứng dụng ngày càng rộng rãi các công nghệ nông nghiệp thông minh và Internet vạn vật.

7. Kết luận

Trong bối cảnh Cách mạng công nghiệp 4.0, an ninh lương thực ngày càng gắn bó chặt chẽ với an ninh mạng khi các công nghệ số như IoT, AI, dữ liệu lớn và tự động hóa được ứng dụng rộng rãi trong toàn bộ chuỗi cung ứng lương thực. Mặc dù góp phần nâng cao hiệu quả và chất lượng, quá trình số hóa cũng làm gia tăng các rủi ro an ninh mạng, trong đó các cuộc tấn công có thể gây gián đoạn chuỗi cung ứng, thiệt hại kinh tế và tác động tiêu cực đến ổn định xã hội cũng như an ninh quốc gia. Do đó, bảo đảm an ninh mạng cần được xem là một cấu phần không thể tách rời của chiến lược an ninh lương thực quốc gia, đòi hỏi cách tiếp cận tổng thể kết hợp giữa giải pháp kỹ thuật, khuôn khổ chính sách và năng lực quản trị, cùng với việc thúc đẩy hợp tác công - tư và áp dụng các chuẩn mực an ninh mạng quốc tế nhằm nâng cao khả năng chống chịu của hệ thống lương thực trong kỷ nguyên số./.

(1), (25) Trần Thị Ngọc Lan (2019), *Tác động của an ninh lương thực đến nền kinh tế Việt Nam*. Khoa Quản trị Kinh doanh, Trường Đại học Công nghiệp Thực phẩm TP. HCM.

(2) Nguyễn Văn Sánh (2009), *An ninh lương thực quốc gia: nhìn từ khía cạnh nông dân trồng lúa và giải pháp liên kết vùng và tham gia □4 nhà□ tại vùng ĐBSCL*, Tạp chí Khoa học, Trường Đại học Cần Thơ, 2009(12), 171-181.

(3), (12), (19, (20), (21) Ajay, K., Wang, Y., Gopinath, M., Sobien, D., Rahman, A., & Batarseh, F. A, (2024), *A review of cybersecurity incidents in the food and agriculture sector*. Computers and Electronics in Agriculture, 226, https://doi.org/10.1016/j.compag.2024.109401

(4) Food and Agriculture Organization of the United Nations, (2009), *The state of food insecurity in the world 2009*. Retrieved September 10, 2025,

from https://www.fao.org/3/i0876e/i0876e.pdf

(5), (26) Lê Anh Thực (2018), *An ninh lương thực trong bối cảnh toàn cầu hoá: Kinh nghiệm quốc tế và gợi ý đối với Việt Nam* (Luận án tiến sĩ, Trường Đại học Kinh tế - Đại học Quốc gia Hà Nội).

(6), (13) Schneier, B (2003), *Secrets and lies: Digital security in a networked world*

DOI:10.1108/146366903322008296.

(7) Phan Chung Thủy và cộng sự (2021), *Rủi ro an ninh mạng trong hoạt động ngân hàng số: Trường hợp Việt Nam*, Tạp chí Ngân hàng.

(8) Katz, E., Gurevitch, M., & Haas, H. (1973). *On the use of the mass media for important things*. American Sociological Review, 38(2), 164-181.

(9) Ruggiero, T. E (2000). *Uses and gratifications theory in the 21st century. Mass Communica. tion & Society*, 3(1), 3-37.

https://doi.org/10.1207/S15327825MCS0301_02

(10) Sundar, S. S., & Limperos, A. M (2013). *Uses and grats 2.0: New gratifications for new media*. Journal of Broadcasting & Electronic Media, 57(4), 504-525.

https://doi.org/10.1080/08838151.2013.845827

(11) Friha, O., Ferrag, M. A., Shu, L., Maglaras, L., & Wang, X (2021). *Internet of Things for smart agriculture: Technologies, practices, and future directions*. IEEE/CAA Journal of Automatica Sinica, 8(4), 718-752.

https://doi.org/10.1109/JAS.2021.1003925

(14), (15), (17), (22), (27) Claroty (2023), *Cyber attack overview: JBS Foods ransomware incident. Retrieved September 12, 2025*, from

https://claroty.com/blog/jbs-attack-puts-food-and-beverage-cybersecurity-to-the-test

(16), (18) Olorunlana, T. J., Mohammed, H, (2025), *Analysis of the Colonial Pipeline cybersecurity incident*. Journal of Next Generation Horizons. DOI: 10.63680/jngh0767as

(23) Schneier, B (2003), *Secrets and lies: Digital security in a networked world*,

DOI:10.1108/146366903322008296.

(24) Friha, O., Ferrag, M. A., Shu, L., Maglaras, L., & Wang, X (2021). *Internet of Things for smart agriculture: Technologies, practices, and future directions. IEEE/CAA Journal of Automatica Sinica*, 8(4), 718-752. DOI: Quốc gia Hà Nội).