

TỘI PHẠM CÔNG NGHỆ CAO LĨNH VỰC TÀI CHÍNH NGÂN HÀNG TRONG BỐI CẢNH CÁCH MẠNG CÔNG NGHIỆP 4.0: THỰC TRẠNG VÀ GIẢI PHÁP

● ĐỖ HỮU VIỆT - BÙI THỊ HẠNH

TÓM TẮT:

Bài viết nhằm khái quát về tội phạm công nghệ cao, nêu rõ thực trạng và những vấn đề đặt ra đối với Việt Nam trong đấu tranh phòng, chống tội phạm công nghệ cao trong lĩnh vực tài chính ngân hàng. Từ kết quả phân tích thực trạng, bài viết đã đưa ra một số giải pháp nhằm ngăn ngừa và giảm thiểu tội phạm công nghệ cao trong lĩnh vực tài chính ngân hàng trong bối cảnh cách mạng công nghiệp 4.0.

Từ khóa: CMCN 4.0, tội phạm công nghệ cao, tài chính ngân hàng, hợp tác, đấu tranh phòng, chống tội phạm.

1. Đặt vấn đề

Cuộc cách mạng công nghiệp 4.0, với sự bùng nổ của khoa học kỹ thuật đã đem lại nhiều thuận lợi cho quá trình giao lưu hợp tác quốc tế, song cũng đã tạo điều kiện cho các loại tội phạm phát triển, đặc biệt là tội phạm công nghệ cao. Sự phát triển của tội phạm không chỉ dừng lại ở phạm vi, mức độ thiệt hại mà hành vi phạm tội cũng ngày một tinh vi hơn khi tội phạm ứng dụng các công nghệ mới trong phương thức thực hiện. Điều này gây ảnh hưởng to lớn cũng như gây ra sự lo ngại cho không chỉ một quốc gia mà cho toàn thể cộng đồng quốc tế. Đặc biệt, tội phạm sử dụng công nghệ cao tấn công vào lĩnh vực tài chính ngân hàng đang có xu hướng ngày càng gia tăng và gây hiệu quả nghiêm trọng. Theo đó, Việt Nam cần tiếp tục hoàn thiện hệ thống pháp luật, hợp tác quốc tế và đưa ra những giải pháp

nhằm ngăn ngừa và giảm thiểu tội phạm công nghệ cao trong lĩnh vực tài chính ngân hàng trong bối cảnh cách mạng công nghiệp 4.0.

2. Khái niệm về tội phạm công nghệ cao

Về mặt thuật ngữ, khái niệm “tội phạm công nghệ cao” trong 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 mạng (*cybercrime*); tội phạm ảo (*Virtual Crime*); tội phạm máy tính/tội phạm tin học (*computer crime*); tội phạm liên quan đến máy tính (*computer-related crime*); tội phạm được kích hoạt/hỗ trợ bởi công nghệ (*Technologically Enabled/Supported Crime*)... Ví dụ như trong Luật Hình sự năm 1995 của Australia và phần 10.7 của Luật Thịnh vượng chung (*Commonwealth Legislation - Part 10.7*:

Computer Offences), tội phạm công nghệ cao (*hi-technology 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*) có sử dụng botnets; tạo ra và phân phối phần mềm độc hại”¹. 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”².

Tại Việt Nam, theo Khoản 1 Điều 3 Nghị định số 25/2014/NĐ-CP của Chính phủ ngày 07/04/2014 quy định: “Tội phạm có 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...”.

Qua nghiên cứu các định nghĩa và các cách tiếp cận trên cho thấy những điểm chung trong nội hàm của các khái niệm này; tất cả đều hướng tới các hành vi liên quan đến việc sử dụng máy tính, thiết bị số, khai thác mạng máy tính, mạng viễn thông một cách bất hợp pháp để gây tổn hại cho lợi ích của các tổ chức, cá nhân và toàn xã hội. Vì vậy, có thể rút ra một định nghĩa chung về tội phạm công nghệ cao như sau: tội phạm công nghệ cao là một dạng thức tội phạm được tiến hành thông qua việc sử dụng tri thức, kỹ năng, công cụ, phương tiện và thành tựu của công nghệ thông tin ở trình độ cao, tác động một cách bất hợp pháp đến thông tin số và các dữ liệu điện tử được lưu trữ, xử lý, truyền tải trong hệ thống máy tính và các thiết bị công nghệ cao, xâm phạm đến trật tự an toàn thông tin, gây tổn hại nghiêm trọng đến quyền và lợi ích hợp pháp của các cá nhân, tổ chức cũng như của các quốc gia và cộng đồng quốc tế.

Khác với những tội phạm truyền thống, tội phạm công nghệ cao có những đặc điểm thể hiện sự khác biệt và phức tạp hơn nhiều so với bất kỳ loại hình tội phạm nào.

Thứ nhất, tội phạm công nghệ cao có đầy đủ các tính chất, đặc điểm giống như mọi tội phạm truyền thống khác, được coi là những hành vi nguy hiểm cho xã hội, sự tương đồng trong các cấu thành cơ bản của một tội phạm... Tuy nhiên, điểm khác biệt cốt lõi giữa chúng với tội phạm khác nằm ở khía cạnh “công nghệ thông tin, máy tính và mạng internet” đóng vai trò, mức độ quyết định trong việc thực hiện, che giấu và gây ra những hậu quả khôn lường đối với xã hội của hành vi phạm tội. Nhìn một cách tổng thể, đối với loại tội phạm công nghệ cao, công nghệ máy tính và mạng luôn là một công cụ quan trọng không thể thiếu trong quá trình thực hiện hành vi phạm tội.

Thứ hai, về chủ thể của tội phạm, tội phạm công nghệ cao được thực hiện bởi các đối tượng có kiến thức cập nhật và am hiểu sâu về máy tính. Để thực hiện hành vi phạm tội, người phạm tội cần có những kiến thức đủ sâu về máy tính để thực hiện hành vi cũng như che giấu bằng chứng. Một vấn đề nữa đáng lưu ý hiện nay đối với chủ thể của nhóm tội phạm này là tình trạng ngày càng “trẻ hóa” của các tin tặc (*hacker*).

Thứ ba, về tính chất của hành vi phạm tội và các hành vi có liên quan đến tội phạm công nghệ cao thường rất tinh vi, tinh xảo. Tính chất này được quyết định bởi rất nhiều yếu tố như: tội phạm công nghệ cao phá hủy hoạt động của các đối tượng tồn tại dưới dạng phi vật chất, như chương trình máy tính hoặc dữ liệu điện tử, mà không phá hủy máy tính hoặc phá hủy mạng thông tin hay các linh kiện của chúng, nên sự hủy hoại này không để lại các dấu vết của sự phá hủy tồn tại dưới dạng vật thể. Tốc độ thực hiện hành vi phạm tội diễn ra tương đối nhanh, kẻ phạm tội có thể chỉ cần thực hiện hành vi trong nháy mắt, chúng có thể thực hiện hành vi phạm tội chỉ trong vòng một phần nghìn, thậm chí một phần triệu giây bằng các máy tính có tốc độ xử lý siêu tốc hoặc bằng những chiếc USB có chứa siêu mã độc. Hơn nữa, tội phạm không bị hạn chế về thời gian, không gian, chúng có thể thực hiện hành vi phạm tội bất cứ khi nào, bất cứ nơi đâu, thậm chí từ từ nước ngoài hoặc một nơi rất xa hiện trường³.

Ngoài các đặc điểm khác biệt cơ bản kể trên,

cũng có thể thấy một số dấu hiệu đặc thù khác so với các nhóm tội phạm thông thường như tính quốc tế, tính xuyên biên giới của loại tội phạm này; tính chất ngày càng tăng về số lượng và hậu quả, tính vi về cách thức tiến hành cùng với sự phát triển của cuộc cách mạng khoa học công nghệ...

2. Thực trạng về tội phạm công nghệ cao trong lĩnh vực tài chính ngân hàng ở Việt Nam

Số lượng vụ án: Năm 2019, lực lượng Công an phát hiện 287 vụ, 437 đối tượng phạm tội, vi phạm pháp luật trong lĩnh vực viễn thông, tin học (nhiều hơn 3,24% so với cùng kỳ năm 2018), trong đó, đã khởi tố 127 vụ, 258 bị can (tăng 4,96% số vụ và giảm 5,84% bị can so với cùng kỳ năm 2018)⁴. Tội phạm công nghệ cao trong lĩnh vực tài chính ngân hàng cũng thường xuyên thay đổi phương thức, thủ đoạn phạm tội nên gây khó khăn cho việc điều tra, phát hiện tội phạm, do đó những vụ việc chưa bị tố giác của tội phạm này là rất lớn, mức độ nguy hiểm và hậu quả của tội phạm gây ra chưa thể thống kê, đánh giá được một cách thực sự chính xác.

Phương thức thực hiện của tội phạm công nghệ cao trong lĩnh vực tài chính ngân hàng thường là đồng phạm và có tổ chức chặt chẽ. Theo đó, tội phạm công nghệ cao trong lĩnh vực tài chính ngân hàng thường sử dụng các thủ đoạn sau: tạo, phát tán vi rút tin học, phần mềm tin học độc hại; sử dụng thẻ ATM giả thanh toán dịch vụ, mua hàng hóa; mua thông tin thẻ tín dụng bị hacker chiếm đoạt rao bán trên các trang web, để sử dụng đặt mua hàng trực tuyến chuyển về Việt Nam tiêu thụ (ship hàng); nhằm ăn cắp cước phí viễn thông; sử dụng mạng máy tính, mạng viễn thông, mạng internet đưa thông tin lên mạng để thực hiện các hoạt động tống tiền; xâm phạm nhân phẩm, tự do cá nhân khác...

Về giới tính và trình độ học vấn: tội phạm công nghệ cao nói chung và trong lĩnh vực tài chính ngân hàng nói riêng chủ yếu là nam giới (chiếm 95,51%; nữ giới chỉ có 4,49%), trong nhiều vụ án không có nữ giới tham gia. Điều này có thể giải thích do đặc thù của loại hình tội phạm này cần sử dụng thành thạo công nghệ thông tin nên nữ giới thường là nạn nhân chứ không phải là người thực hiện.

Về địa bàn thực hiện hành vi phạm tội của tội

phạm công nghệ cao trong lĩnh vực tài chính ngân hàng trong những năm qua chủ yếu tại hai thành phố trực thuộc trung ương là Hà Nội và TP. Hồ Chí Minh, còn lại là ở các thành phố lớn, nông thôn, huyện lỵ, thị xã.

Về quốc tịch của bị cáo, chủ yếu có quốc tịch Việt Nam, bị cáo có quốc tịch nước ngoài cũng chiếm một số ít gồm: Trung Quốc, Malaysia, Hàn Quốc, Nigeria, Rumania, Pakistan.

Trong lĩnh vực thẻ ngân hàng, tình trạng đối tượng là người Trung Quốc và một số nước châu Phi nhập cảnh vào Việt Nam, làm giả thẻ và móc nối với một số cơ quan, tổ chức chấp nhận thanh toán thẻ (POS), tiến hành giao dịch khống để rút tiền mặt, hoặc mua hàng hóa tại các cửa hàng, siêu thị, gây thiệt hại hàng triệu USD; nhiều đối tượng còn lắp đặt thiết bị tại các ATM hoặc máy POS để ăn cắp thông tin thẻ ngân hàng.

Ngoài ra, tình trạng truy cập trái phép vào tài khoản ngân hàng của cá nhân để chiếm đoạt tài sản cũng diễn ra rất phổ biến. Theo đó, người phạm tội sử dụng một số phần mềm để phát hiện lỗi của các website bán hàng qua mạng, ngân hàng thanh toán qua mạng, xâm nhập vào cơ sở dữ liệu lấy quyền quản trị của admin để trộm cắp dữ liệu để lấy địa chỉ email, thông tin khách hàng, thông tin thẻ tín dụng, tài khoản cá nhân, bằng hình thức phát tán virus, phần mềm gián điệp, mã độc hại với nhiều biến thể qua thư điện tử, đường link website, diễn đàn, mạng xã hội hoặc các phần mềm miễn phí, phần mềm được sử dụng phổ biến để thu thập, trộm cắp, thay đổi, phá hủy trái phép cơ sở dữ liệu; Chiếm quyền điều khiển máy chủ, sau đó thay đổi giao diện của trang web bị tấn công, tạo website giả...⁵.

Theo BKAV, năm 2015, Việt Nam có 5.226 website bị hacker xâm nhập và 30% website các ngân hàng Việt Nam có lỗ hổng. Theo Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam, năm 2015 đã phát hiện 5.898 sự cố lừa đảo, 8.850 sự cố thay đổi giao diện, 16.837 sự cố mã độc, ngăn chặn 200 website giả mạo.⁶ Theo báo cáo của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), trong năm 2015, đơn vị này đã ghi nhận được 5.898 sự cố lừa đảo (Phishing), 8.850 sự cố thay đổi giao

diện (Deface), 16.837 sự cố mã độc (Malware) tăng 1,7 lần so với năm ngoái, đã cảnh báo và khắc phục được 3.885 sự cố (trong đó có 87 sự cố liên quan đến các tên miền “.gov.vn”). Nhìn chung, mã độc đa số là các liên kết ẩn được nhúng vào website thực hiện các thao tác không mong muốn. Ví dụ như like fanpage Facebook, ẩn link. VNCERT cũng ghi nhận 1.451.997 lượt địa chỉ IP cả nước bị nhiễm mã độc và nằm trong các mạng Botnet.⁷

3. Giải pháp nhằm ngăn ngừa và giảm thiểu tội phạm công nghệ cao trong lĩnh vực tài chính ngân hàng đặt trong bối cảnh cách mạng công nghiệp 4.0

Thứ nhất về mặt văn bản pháp luật, cần thiết có những quy định rõ ràng, cụ thể về các chính sách, biện pháp trong phát triển các lĩnh vực khoa học - công nghệ nhằm phòng, chống tội phạm sử dụng công nghệ cao trong lĩnh vực tài chính ngân hàng chẳng hạn như việc thu thập, kiểm tra, đánh giá chứng từ điện tử cũng như ban hành văn bản hướng dẫn về đường lối xử lý đối với các tội phạm công nghệ cao trong lĩnh vực tài chính ngân hàng. Đặc biệt hiện nay, đi cùng sự phát triển của công nghệ thông tin và đáp ứng nhu cầu khách hàng ngày càng phức tạp, khác biệt rõ rệt về các nghiệp vụ truyền thống về cách thức vận hành và mức độ rủi ro thì dịch vụ trung gian thanh toán tại một số công ty không phải là ngân hàng đã được thí điểm thực hiện.⁸ Song, toàn bộ các dịch vụ cung ứng hạ tầng thanh toán điện tử và một số dịch vụ hỗ trợ thanh toán vẫn nằm ngoài phạm vi hoạt động được cấp phép của các ngân hàng. Do vậy, các quy định pháp lý này vẫn cần phải hoàn thiện để không hạn chế phạm vi hoạt động của ngân hàng.

Thứ hai, những người tiến hành tố tụng cần nâng cao kiến thức cơ bản về dữ liệu điện tử, về công nghệ thông tin (am hiểu nhất định về đối tượng đang được khai thác)... Để làm tốt điều đó, cần xác định phương hướng cho hoạt động thu thập dữ liệu điện tử đó là: (i) Phải xuất phát từ những thông tin, tài liệu, chứng cứ ban đầu về vụ án đã thu thập được, đây là cơ sở đầu tiên giúp cho cơ quan có thẩm quyền xác định phương hướng thu thập dữ liệu điện tử; (ii) Xuất phát từ quy luật dấu vết điện tử có điểm riêng biệt so với dấu vết hình sự khác,

căn cứ vào nguồn gốc hình thành và đặc điểm của vật mang dấu vết điện tử (phương tiện điện tử, mạng máy tính, mạng viễn thông hoặc trên đường truyền); (iii) Quy luật hoạt động của các đối tượng phạm tội đối với các hệ, loại đối tượng là khác nhau, chẳng hạn như: Quy luật hoạt động của các đối tượng sử dụng công nghệ cao xâm phạm an ninh quốc gia sẽ có những điểm đặc trưng so với quy luật hoạt động của các đối tượng sử dụng công nghệ thông tin để hoạt động lừa đảo chiếm đoạt tài sản....

Thứ ba, nâng cao năng lực cho lực lượng chuyên trách đấu tranh, phòng ngừa tội phạm công nghệ cao trong lĩnh vực tài chính ngân hàng

Một trong những vấn đề cốt lõi để nâng cao vai trò và đảm bảo cho hoạt động đấu tranh, phòng chống tội phạm sử dụng công nghệ cao có hiệu quả là nâng cao năng lực cho các cơ quan chuyên trách. Chính phủ cần có các đề án để đào tạo, bồi dưỡng, tập huấn (kể cả trong và ngoài nước) về pháp luật quốc tế, về kỹ thuật nghiệp vụ và về ngôn ngữ để đáp ứng sự thay đổi của phương thức, thủ đoạn tội phạm sử dụng công nghệ cao trong lĩnh vực tài chính ngân hàng. Cần tập trung phát huy tốt hơn vai trò và tăng cường hoạt động của lực lượng nòng cốt trong phòng, chống tội phạm sử dụng công nghệ cao là Văn phòng INTERPOL Việt Nam và lực lượng an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao.

Thứ tư, xây dựng trang thiết bị, công nghệ tiên tiến trong công tác đấu tranh, phòng ngừa tội phạm công nghệ cao trong lĩnh vực tài chính ngân hàng

Đặc thù của tội phạm công nghệ cao nói chung luôn sử dụng thiết bị, máy móc công nghệ thông tin trong hoạt động phạm tội, do đó đòi hỏi cơ quan chuyên trách như Cục Cảnh sát phòng, chống tội phạm sử dụng công nghệ cao, Cục An ninh mạng (Bộ Công an) cần được quan tâm đầu tư mạnh mẽ về trang thiết bị chuyên dụng hiện đại và xây dựng được một đội ngũ cán bộ có trình độ cao. Hiện nay, mặc dù đã được Đảng, Nhà nước quan tâm đầu tư trang thiết bị, máy móc, nhưng để phòng, chống tội phạm công nghệ cao hiệu quả hơn nữa, các đơn vị chức năng rất cần được trang bị đầy đủ thiết bị kỹ thuật, phương tiện, phần mềm chuyên dụng hiện đại. Vì vậy, Chính phủ cần tiếp tục ban hành các

Đề án đầu tư mua sắm trang thiết bị cho các cơ quan chuyên trách bên cạnh Đề án 5 thuộc Chương trình Quốc gia phòng chống tội phạm về “Đấu tranh, phòng chống tội phạm sử dụng công nghệ cao” đã được thông qua.

4. Kết luận

Cuộc cách mạng công nghiệp 4.0 phát triển mạnh mẽ đã tạo điều kiện thuận lợi cho các loại tội phạm phát triển, đặc biệt là tội phạm sử dụng công nghệ cao. Lĩnh vực tài chính ngân hàng là lĩnh vực xảy ra rất nhiều vụ phạm tội trên thực tiễn nhưng do

thủ đoạn tinh vi mà hiện nay vẫn chưa thể phát hiện và xử lý được hết, làm ảnh hưởng rất nhiều đến các cá nhân, tổ chức và ngân hàng. Qua đó chúng ta thấy được những thách thức về đấu tranh phòng, chống tội phạm công nghệ cao mà cuộc cách mạng công nghiệp 4.0 mang lại. Chính vì vậy, việc tiếp tục hoàn thiện hệ thống pháp luật, hợp tác quốc tế và đưa ra những giải pháp nhằm ngăn ngừa và giảm thiểu tội phạm công nghệ cao trong lĩnh vực tài chính ngân hàng trong bối cảnh cuộc cách mạng công nghiệp 4.0 là điều cần thiết ■

TÀI LIỆU TRÍCH DẪN:

¹Xem <https://www.afp.gov.au/what-we-do/crime-types/cybercrime/high-tech-crime>.

²Black's Law Dictionary, truy cập tại: <https://legal.thomsonreuters.com/en/products/law-books/blacks-law-dictionary>

³Đỗ Quý Hoàng (2023).- Pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao - Những vấn đề đặt ra đối với Việt Nam (Sách chuyên khảo), NXB. Công An Nhân dân, Hà Nội.

⁴Bộ Công An: Phát hiện 287 vụ vi phạm pháp luật về CNTT và viễn thông; <https://ictnews.vietnamnet.vn/cuoc-song-so/bo-cong-an-phat-hien-287-vu-vi-pham-phap-luat-ve-cntt-va-vien-thong-36195.html>

⁵Đinh Thế Hưng, Lê Thị Hồng Xuân (2021), Tội phạm công nghệ cao trong lĩnh vực tài chính, ngân hàng ở Việt Nam hiện nay, Tạp chí Tòa án nhân dân số 7 năm 2019

⁶Hà Loan (2017), Ngại chia sẻ thông tin, ngân hàng khó an toàn bảo mật, truy cập tại: <http://anninhthudo.vn/chinh-tri-xahoi/ngai-chia-se-thong-tin-ngan-hang-kho-an-toan-bao-mat/738308.antd>

⁷Thành Luân (2016), Bảo vệ an toàn không gian mạng tại Việt Nam đang 'nóng', truy cập tại: <https://thanhnien.vn/bao-ve-an-toan-khong-gian-mang-tai-viet-nam-dang-nong-185613583.htm>

⁸Phan Chí Hiếu, Nguyễn Văn Cường (2019), Tlđd, tr.171

TÀI LIỆU THAM KHẢO:

1. Đảng Cộng sản Việt Nam (2021). Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII, NXB. Chính trị Quốc gia - Sự thật, Hà Nội.

2. Đỗ Quý Hoàng (2023). Pháp luật quốc tế trong hợp tác đấu tranh phòng chống tội phạm công nghệ cao - Những vấn đề đặt ra đối với Việt Nam (Sách chuyên khảo), NXB. Công an Nhân dân, Hà Nội.

3. Phan Chí Hiếu, Nguyễn Văn Cường (2019). Cách mạng Công nghiệp lần thứ tư và những vấn đề pháp lý đặt ra (Sách chuyên khảo), NXB Tư pháp, Hà Nội.

4. Đinh Thế Hưng, Lê Thị Hồng Xuân (2021). Tội phạm công nghệ cao trong lĩnh vực tài chính, ngân hàng ở Việt Nam hiện nay, Tạp chí Tòa án nhân dân số 7 năm 2019.

5. Nguyễn Ngọc Anh (2021). Một số quy định của pháp luật về tội phạm công nghệ cao, truy cập tại: <http://csnd.vn/Home/Nghien-cuu-Trao-doi/286/Mot-so-quy-dinh-cua-phap-luat-ve-toi-pham-cong-nghe-cao>.

6. Black's Law Dictionary, truy cập tại: <https://legal.thomsonreuters.com/en/products/law-books/blacks-law-dictionary>.

7. Bộ Thông tin và Truyền thông (2019). Sách trắng Công nghệ thông tin và truyền thông Việt Nam năm 2019, truy cập tại: https://mic.gov.vn/Upload_Moi/FileBaoCao/Sach-Trang2019-Final.pdf.
8. Bộ Công an (2019). Phát hiện 287 vụ vi phạm pháp luật về CNTT và viễn thông, truy cập tại: <https://ictnews.vietnamnet.vn/cuoc-song-so/bo-cong-an-phat-hien-287-vu-vi-pham-phap-luat-ve-cntt-va-vien-thong-36195.html>.
9. Hà Loan (2017). Ngại chia sẻ thông tin, ngân hàng khó an toàn bảo mật, truy cập tại: <http://anninhthudo.vn/chinh-tri-xahoi/ngai-chia-se-thong-tin-ngan-hang-kho-an-toan-bao-mat/738308.antd>.
10. Thành Luân (2016). Bảo vệ an toàn không gian mạng tại Việt Nam đang “nóng”, truy cập tại: <https://thanhnien.vn/bao-ve-an-toan-khong-gian-mang-tai-viet-nam-dang-nong-185613583.htm>.

Ngày nhận bài: 2/3/2024

Ngày phản biện đánh giá và sửa chữa: 15/3/2024

Ngày chấp nhận đăng bài: 28/3/2024

Thông tin tác giả:

1. ĐỖ HỮU VIỆT¹

2. BUI THI HANH²

¹Ngân hàng TMCP Kiên Long

²Công ty TNHH Tư vấn và Phát triển thương hiệu AMC Việt Nam

HIGH-TECH CRIME IN THE BANKING AND FINANCE FIELD IN THE CONTEXT OF INDUSTRY 4.0: CURRENT SITUATION AND SOLUTIONS

● **DO HUU VIET¹**

● **BUI THI HANH²**

¹Kien Long Joint Stock Commercial Bank

²AMC Vietnam Brand Development and Consulting Company Limited

ABSTRACT:

This paper provided an overview of high-tech crimes, clarified the current situation and issues facing Vietnam in the fight against high-tech crimes in the banking and finance sector. Based on the papers findings, some solutions were proposed to prevent and reduce high-tech crimes in the banking and finance sector in the context of the Fourth Industrial Revolution (Industry 4.0).

Keywords: the Fourth Industrial Revolution (Industry 4.0), high-tech crime, finance-banking, cooperation, crime prevention.