CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 25 tháng 02 năm 2021

BÁO CÁO KẾT QUẢ TỰ ĐÁNH GIÁ
NHIỆM VỤ KHOA HỌC VÀ CÔNG NGHỆ CẤP QUỐC GIA

I. Thông tin chung về nhiệm vụ:

1. Tên nhiệm vụ, mã số:

Nghiên cứu, xây dựng hệ thống đánh giá, quản lý rủi ro và hỗ trợ xử lý sự cố an toàn thông tin trong Chính phủ điện tử.

Mã số: KC.01.19/16-20

Thuộc: Chương trình: Chương trình Khoa học và Công nghệ trọng điểm Quốc gia giai đoạn 2016 2020 về "Nghiên cứu công nghệ và phát triển sản phẩm công nghệ thông tin phục vụ Chính phủ điện tử", Mã số: KC.01/16-20.

2. Mục tiêu nhiệm vụ:

Trong đề tài này, chúng tôi hướng đến thực hiện hai mục tiêu đã xác lập trong đặt hàng của Bộ Khoa học và Công nghệ, cụ thể như sau:

1. Xây dựng hệ thống phục vụ hoạt động đánh giá, quản lý rủi ro và hỗ trợ xử lý sự cố an toàn thông tin trong các hệ thống công nghệ thông tin tại các cơ quan nhà nước.

2. Hình thành quy trình đánh giá, quản lý rủi ro và hỗ trợ xử lý sự cố an toàn thông tin trong Chính phủ điện tử Việt Nam, phù hợp với tiêu chuẩn quốc gia và quốc tế về an toàn thông tin.

3. Chủ nhiệm nhiệm vụ:

Họ và tên: Nguyễn Ngọc Hoá Học hàm, học vị: PGS.TS.

Chức danh khoa học: Giảng viên cao cấp

Chức vụ: Chủ nhiệm Bộ môn.

Cơ quan: Trường Đại học Công nghệ - ĐHQGHN

Địa chỉ: E3, 144 Xuân Thủy, Cầu Giấy, Hà Nội

Điện thoại: Tổ chức: 024.37547.813 Mobile: 09.04.10.48.20

E-mail: hoa.nguyen@vnu.edu.vn

4. Tổ chức chủ trì nhiệm vụ:

Trường Đại học Công nghệ - Đại học Quốc gia Hà Nội

Địa chỉ: Nhà E3 – 144 Xuân Thuỷ - Cầu Giấy – Hà Nội

Điện thoại: (84-24) 37547.461 Fax: (84-24) 37547460

Website: http://uet.vnu.edu.vn

5. Tổng kinh phí thực hiện: 6.885 triệu đồng.

Trong đó, kinh phí từ ngân sách SNKH: 6.885 triệu đồng.

Kinh phí từ nguồn khác: 0 triệu đồng.

6. Thời gian thực hiện theo Hợp đồng: 24 tháng

Bắt đầu: 01/2019

Kết thúc: 12/2020

Thời gian thực hiện theo văn bản điều chỉnh của cơ quan có thẩm quyền *(nếu có)*: kéo dài thêm 02 tháng, kết thúc 02/2021

7. Danh sách thành viên chính thực hiện nhiệm vụ nêu trên gồm:

TT	Họ và tên	Chức danh khoa học, học vị	Tổ chức công tác
1	Nguyễn Ngọc Hoá	PGS.TS	Trường Đại học Công nghệ - ĐHQG HN
2	Nguyễn Thị Hậu	TS	Trường Đại học Công nghệ - ĐHQG HN
3	Phùng Văn Ổn	TS	Trung tâm tin học - VPCP
4	Lê Việt Hà	ThS	Trung tâm tin học - VPCP
5	Phùng Văn Thọ	ThS	Trung tâm tin học - VPCP
6	Khuất Hoàng Kiên	KS	Cục CNTT&DLTNMT – Bộ TNMT
7	Trần Văn Trung	TS	Cục CNTT&DLTNMT – Bộ TNMT
8	Ngô Quang Huy	TS	VNCERT – Bộ TTTT
9	Hoàng Minh Tiến	ThS	Cục ATTT – Bộ TTTT
10	Đặng Minh Tuấn	TS	Công ty TNHH Việt Kỳ
11	Tống Minh Đức	TS	HVKTQS – Bộ Quốc phòng
12	Nguyễn Quang Uy	PGS.TS	HVKTQS – Bộ Quốc phòng
13	Hà Quang Thuy	PGS.TS	Trường Đại học Công nghệ - ĐHQG HN
14	Nguyễn Trí Thành	PGS.TS	Trường Đại học Công nghệ - ĐHQG HN
15	Lê Phê Đô	TS	Trường Đại học Công nghệ - ĐHQG HN
16	Nguyễn Đại Thọ	TS	Trường Đại học Công nghệ - ĐHQG HN
17	Trần Trọng Hiếu	TS	Trường Đại học Công nghệ - ĐHQG HN
18	Lê Hồng Hải	TS	Trường Đại học Công nghệ - ĐHQG HN
19	Vũ Bá Duy	ThS	Trường Đại học Công nghệ - ĐHQG HN
20	Dư Phương Hạnh	TS	Trường Đại học Công nghệ - ĐHQG HN
21	Phạm Hải Đăng	ThS	Trường Đại học Công nghệ - ĐHQG HN

II. Nội dung tự đánh giá về kết quả thực hiện nhiệm vụ:

1. Về sản phẩm khoa học:

1.1. Danh mục sản phẩm đã hoàn thành:

Số TT	Tên sản phẩm	Số lượng			Chất lượng		
		Xuất sắc	Đạt	Không đạt	Xuất sắc	Đạt	Không đạt
1.	USB chuyên dụng, được cài sẵn phần mềm thu thập chứng cứ về sự cố mất ATTT		X			Đã tạo được 06 USB chuyên dụng, được cài sẵn phần mềm mềm thu thập chứng cứ về sự cố mất ATTT trên cả Linux lẫn Windows với các thông số kỹ thuật như sau: o Sử dụng chuẩn giao tiếp từ USB 3.0, dung lượng 128GB. o Sử dụng định dạng dữ liệu chuyên biệt chống nguy cơ lây nhiễm ngược đối với thiết bị USB với cơ chế mã hoá, được tổ chức gồm 3 phân vùng chuyên biệt. o *Phân vùng 1*: chống ghi sử dụng cơ chế LUKS trên Linux, chứa các phần mềm công cụ sau: ▪ Hệ điều hành Linux chuyên dụng phục vụ thu thập chứng cứ sự cố ATTT; ▪ Phần mềm công cụ IncidentCollect trên Linux để thu thập chứng cứ trên thiết bị lưu trữ, có cơ chế đảm bảo tính toàn vẹn dữ liệu chứng cứ thu thập được, bao gồm các dữ liệu như Registry, Windows logs, cấu hình hệ thống, lịch sử người dùng, caches trình duyệt, các tệp hệ thống quan trọng của Windows,... o *Phân vùng 2*: chống ghi với cơ chế BitLocker, thiết lập quyền chỉ đọc, chứa phần mềm công cụ IncidentCollector.exe trên Windows phục vụ thu thập chứng cứ với cơ chế đảm bảo tính toàn vẹn: ▪ *từ bộ nhớ chính RAM,* bao gồm: thông tin trạng thái mạng, các cổng được mở, bảng định tuyến; dữ liệu trao đổi qua các cổng mạng được mở; dữ liệu các tiến trình đang hoạt động; dữ liệu các tệp tin được thao tác từ xa; thông tin người dùng và máy tính. ▪ *từ thiết bị lưu trữ,* bao gồm các dữ liệu như:Registry, Windows logs, cấu hình hệ thống, logs người dùng (caches trình duyệt), các tệp hệ thống quan trọng của Windows,... *Phân vùng 3*: để lưu dữ liệu chứng cứ, được cập nhật bởi công cụ phần mềm thu thập chứng cứ được xây dựng trong đề tài.	
2.	Hệ thống đánh giá, quản lý rủi		X			**Hệ thống đánh giá, quản lý rủi ro ATTT, UET.SRA, bao gồm**:	

	ro an toàn thông tin trong các hệ thống công nghệ thông tin					- CSLD tập các nguy cơ rủi ro, lỗ hổng mất an toàn thông tin; sử dụng chuẩn SCAP (Security Content Automation Protocol) của NIST với các loại tập mẫu với số lượng tối thiểu 100.000 CVEs, 270.000 CPEs, 28.000 mẫu OPAL và 9.000 mẫu CERT. - Tập các mẫu rò quét lỗ hổng với số lượng khoảng 60.000 mẫu. - CSDL tập các mô hình mẫu để đánh giá và quản lý rủi ro an toàn thông tin tại cơ quan cấp Bộ, tỉnh, thành phố trực thuộc Trung ương. - 02 phần mềm hỗ trợ phân tích, phát hiện, thu thập các nguy cơ, lỗ hổng dẫn đến rủi ro mất an toàn thông tin: *1. Công cụ vScanner hỗ trợ phân tích, phát hiện, thu thập các nguy cơ, lỗ hổng dẫn đến rủi ro ATTT:* o Dò quét được các lỗ hổng trong các hệ thống CNTT (bao gồm cả thiết bị mạng, hệ điều hành) dựa trên các mẫu rò quét lỗ hổng, o Phân loại mức độ rủi rỏ ảnh hưởng đến hệ thống CNTT theo độ đo CVSS (từ 0 đến 10), o Phát hiện được các Windows policy bị vi phạm trên các máy tính Windows đã được cấp quyền, o Phát hiện được các máy tính Windows chưa thi hành và áp dụng những bản vá lỗ hổng đã được nhà cung cấp khắc phục, o Có khả năng thi hành song song để tăng hiệu năng dò quét, o Có khả năng lưu lại các kết quả dò quét về CSDL chung của hệ thống. *2. Công cụ wScanner dò quét, phân tích, phát hiện (có ứng dụng phương pháp học sâu) và thu thập các nguy cơ, lỗ hổng trong mã nguồn ứng dụng Web được xây dựng bằng các ngôn ngữ PHP, ASP, từ đó gửi về CSDL chung của hệ thống.* - 05 dịch vụ trực tuyến quản lý rủi ro, bao gồm phân tích, đánh giá, đề xuất phương án xử lý, giám sát rủi ro ATTT. Các dịch vụ này có thể hoạt động độc lập và được tích hợp trong một giao diện chính (dashboard) để thuận lợi sử dụng: *1. Dịch vụ quản lý quy trình nghiệp vụ đánh giá, quản lý rủi ro ATTT, với các chức năng:* o Tìm kiếm, tra cứu các mô hình mẫu phục vụ đánh giá ATTT, o Quản lý quy trình đánh giá và quản lý rủi ATTT, o Ước lượng rủi ro ATTT theo độ đo CVSS. *2. Dịch vụ quản lý tác vụ xác định rủi ro ATTT trong các hệ thống CNTT, với các chức năng:* o Quản lý các tiến trình dò quét và phát hiện rủi rỏ ATTT sử dụng vScanner, o Quản lý các tiến trình dò quét lỗ hổng và Webshells sử dụng wScanner, o Lập lịch thi hành tiến trình dò quét rủi ro ATTT sử dụng vScanner hoặc wSanner, o Quản lý danh mục các tác vụ xác định rủi ro ATTT. *3. Dịch vụ quản lý rủi ro ATTT trong các hệ thống CNTT, với các khả năng:* o Quản lý danh mục các kết quả rủi ro ATTT đã được phát hiện,	

						○ Phân tích, đánh giá toàn bộ các rủi ro ATTT đã phát hiện được dựa trên các nguy cơ khai thác các lỗ hổng bảo mật; phân loại theo mức độ ảnh hưởng đến hệ thống CTTT theo tối thiểu 3 mức (Cao, Trung bình, Thấp) dựa trên độ đo CVSS (từ 0 đến 10), ○ Đề xuất phương án xử lý các lỗ hổng, Windows policy vi phạm quy định, cập nhật các bản vá lỗ hổng, ○ Sinh báo cáo, thống kê kết quả phân tích, đánh giá theo những định dạng phổ biến (PDF, HTML, XML, …), ○ Hỗ trợ gợi ý phương án xử lý rủi ro ATTT, ○ Quản lý và hỗ trợ giám sát kết quả xử lý rủi ro ATTT, ○ Tìm kiếm thông tin trong tập dữ liệu rủi ro và phương án xử lý rủi ro ATTT. *4. Dịch vụ quản lý các hệ thống CNTT và các CSDL, với các khả năng:* ○ Quản lý danh mục các hệ thống CNTT (cả các hosts lẫn các ứng dụng) trong cơ quan nhà nước kèm theo các nguy cơ công nghệ tương ứng, ○ Quản lý tập mô hình mẫu để đánh giá và quản lý rủi ro trong cơ quan, ○ Quản lý các bản vá và chính sách áp dụng bản vá tự động tại các thiết bị đầu cuối, ○ Quản lý danh mục các quy định Windows Policy, ○ Quản lý tập dữ liệu CPEs, CVEs và OPAL, các lỗ hổng được các trung tâm ứng cứu khẩn cấp xác lập, ○ Quản lý các mẫu kiểm tra lỗ hổng. *5. Dịch vụ quản trị toàn bộ hệ thống, với các chức năng:* ○ Dashboard để hiển thị các thông tin chính của hệ thống, ○ Quản lý người dùng, ○ Quản lý các tài khoản phục vụ dò quét sâu và vá lỗ hổng, ○ Quản lý cấu hình hệ thống, ○ Điều phối thi hành các bản vá tại các máy Windows được giám sát, ○ Hỗ trợ liên thông với những kết quả giám sát hạ tầng mạng từ các đề tài khác như hệ thống phân tích vết truy cập, hệ thống giám sát hạ tầng mạng, ...	
3.	Hệ thống hỗ trợ xử lý sự cố an toàn thông tin trong các hệ thống công nghệ thông tin		X			**Hệ thống phần mềm trung tâm, UET.SIR, phục vụ phân tích chứng cứ, phát hiện nguyên nhân sự cố, hỗ trợ công tác xử lý sự cố ATTT, gồm bốn phân hệ có các chức năng và yêu cầu khoa học chính sau:** ○ *Phân hệ quản lý quy trình hỗ trợ xử lý sự cố ATTT*, với các chức năng chính: ▪ Quản lý quy trình xử lý sự cố ATTT, ▪ Quản lý các mẫu quy trình thông dụng có thể áp dụng để xử lý sự cố ATTT. ○ *Phân hệ quản lý dữ liệu chứng cứ sự cố ATTT*, với các chức năng: ▪ Quản lý các sự cố ATTT, ▪ Tiếp nhận các dữ liệu chứng cứ đã thu thập được,	

						▪ Hỗ trợ khôi phục dữ liệu từ ảnh ổ đĩa thu thập được, truy xuất dữ liệu bị lỗi bảng định vị tệp tin thông qua sử dụng công cụ autopsy trước khi lấy phân tích, ▪ Quản lý và tra cứu dữ liệu chứng cứ, theo hồ sơ, máy tính bị sự cố, thời gian thu thập và kiểu dữ liệu sự cố. ▪ Tìm kiếm theo từ khoá trong tập bộ dữ liệu chứng cứ, cung cấp chức năng thu hẹp kết quả theo hồ sơ/máy tính/ngày/kiểu dữ liệu sự cố. o *Phân hệ phân tích, xác định nguyên nhân và hỗ trợ công tác xử lý sự cố ATTT,* với các chức năng: ▪ Phân tích, xác định nguyên nhân sự cố ATTT thông qua dò quét mã độc, từ dữ liệu chứng cứ trong bộ nhớ chính (thông tin trạng thái mạng, các cổng được mở, bảng định tuyến; dữ liệu trao đổi qua các cổng mạng được mở; dữ liệu các tiến trình đang hoạt động; dữ liệu các tệp tin được thao tác từ xa; thông tin người dùng và máy tính), từ dữ liệu chứng cứ trên thiết bị lưu trữ (Registry, Windows logs, cấu hình hệ thống, logs người dùng (caches trình duyệt), các tệp hệ thống quan trọng của Windows,...), ▪ Sinh báo cáo, thống kê về sự cố ATTT, ▪ Tư vấn, gợi ý hỗ trợ chuyên gia xây dựng phương án xử lý sự cố ATTT. ▪ Hỗ trợ đánh giá, phân tích sự cố ATTT theo phương pháp xếp chồng, phân tích so khác, duyệt theo dòng thời gian. ▪ Cho phép chuyên gia đánh giá, xác định sự cố ATTT trực tiếp khi thực hiện các chức năng nêu trên. o *Phân hệ quản trị toàn bộ hệ thống*, với các chức năng: ▪ Quản trị người dùng và hệ thống, ▪ Quản lý các công cụ phục vụ phân tích, xác định nguyên nhân sự cố ATTT, ▪ Quản lý, cập nhật hệ điều hình Linux chuyên dụng và các phần mềm thu thập dữ liệu chứng cứ trên USB chuyên dụng.	
4.	Tài liệu đặc tả quy trình đánh giá, quản lý rủi ro ATTT trong Chính phủ điện tử Việt Nam		X			Đặc tả chi tiết quy trình đánh giá, quản lý rủi ro ATTT trong Chính phủ điện tử Việt Nam, phù hợp với tiêu chuẩn quốc gia và quốc tế về an toàn thông tin như ISO/IEC 27001 (TCVN ISO/IEC 27001:2009), ISO/IEC 27005:2011 (TCVN 10295:2014), NIST SP30r1, NIST SP800-39, NIST SP 800-53 Rev. 4 và ISO/IEC 15408:2017.	
5.	Tài liệu đặc tả quy trình chung phục vụ đánh		X			- Làm rõ được quy trình chung phục vụ đánh giá, xử lý, chấp nhận và giám sát rủi ro an toàn thông tin tại cơ quan nhà nước cấp Bộ, tỉnh, thành phố trực thuộc Trung ương. - Có các mô hình mẫu để có thể triển khai, đánh giá và quản lý rủi ro ATTT tại 01 Bộ TNMT.	

	giá, xử lý, chấp nhận và giám sát rủi ro ATTT tại cơ quan nhà nước cấp Bộ, tỉnh, thành phố trực thuộc Trung ương.						
6.	Tài liệu đặc tả quy trình thu thập chứng cứ và hỗ trợ xử lý sự cố ATTT		X			Đặc tả chi tiết quy trình thu thập chứng cứ và hỗ trợ xử lý sự cố ATTT trong Chính phủ điện tử Việt Nam, phù hợp với tiêu chuẩn quốc gia và quốc tế, cụ thể là ISO/IEC 27035-2011 (TCVN 11239:2015), NIST SP800-61r1.	
7.	Tài liệu phân tích, thiết kế toàn bộ hệ thống đánh giá và quản lý rủi ro ATTT		X			Đặc tả chi tiết quá trình phân tích, thiết kế toàn bộ hệ thống đánh giá và quản lý rủi ro an toàn thông tin với các nội dung chính sau: - Mô hình kiến trúc hệ thống - Nền tảng thư viện hệ thống kèm các lược đồ CSDL - Phần mềm dò quét, phát hiện thu thập các lỗ hổng trong các hệ thống CNTT, các Windows policy chưa đáp ứng quy định, thông tin về các bản vá trên Windows chưa được cập nhật (vScanner) - Phần mềm phân tích, phát hiện các nguy cơ, lỗ hổng trong mã nguồn ứng dụng Web sử dụng ngôn ngữ PHP, ASP (wScanner) - Năm dịch vụ trực tuyến quản lý rủi ro, bao gồm phân tích, đánh giá, đề xuất phương án xử lý, giám sát rủi ro ATTT: • Dịch vụ quản lý quy trình nghiệp vụ phục vụ công tác đánh giá, quản lý rủi ro ATTT, • Dịch vụ trực tuyến quản lý tác vụ dò quét xác định rủi ro ATTT, • Dịch vụ trực tuyến hỗ trợ phân tích, đánh giá các rủi ro ATTT đã được xác định được, đề xuất phương án xử lý và giám sát kết quả xử lý rủi ro ATTT, • Dịch vụ các hệ thống CNTT và các CSDL mẫu trong hệ thống quản lý rủi ro, Dịch vụ quản trị toàn bộ hệ thống.	
8.	Tài liệu phân tích, thiết kế		X			Tài liệu phân tích, thiết kế toàn bộ hệ thống hỗ trợ xử lý sự cố ATTT, bao gồm các thành phần chính: - Mô hình kiến trúc hệ thống,	

	toàn bộ hệ thống hỗ trợ xử lý sự cố ATTT					- Chức năng, nhiệm vụ của USB chuyên dụng phục vụ thu thập dữ liệu chứng cứ, - Công cụ phần mềm phục vụ thu thập thu thập dữ liệu chứng cứ, cả trong bộ nhớ chính lẫn trong các thiết bị lưu trữ, - Vai trò, chức năng, nhiệm vụ của phần mềm trung tâm phục vụ phân tích chứng cứ, phát hiện nguyên nhân sự cố, hỗ trợ công tác xử lý sự cố ATTT, với các phân hệ: • Phân hệ quản lý quy trình hỗ trợ xử lý sự cố ATTT, • Phân hệ quản lý dữ liệu chứng cứ sự cố ATTT, • Phân hệ phân tích, xác định nguyên nhân và hỗ trợ công tác xử lý sự cố ATTT, Phân hệ quản trị toàn bộ hệ thống.	
9.	Tài liệu hướng dẫn quản lý, vận hành, khai thác và sử dụng hệ thống đánh giá, quản lý rủi ro và hỗ trợ xử lý sự cố ATTT		X			- Có đầy đủ thông tin để hướng dẫn quản lý, vận hành, khai thác và sử dụng hệ thống đánh giá, quản lý rủi ro ATTT, dựa trên quy trình đánh giá, quản lý rủi ro trong Chính phủ điện tử Việt Nam - Có đầy đủ thông tin để hướng dẫn quản lý, vận hành, khai thác và sử dụng hệ thống hỗ trợ xử lý sự cố ATTT, dựa trên quy trình xử lý sự cố ATTT đã được xây dựng.	
10.	Báo cáo kết quả triển khai, đánh giá thử nghiệm hệ thống đánh giá, quản lý rủi ro và hỗ trợ xử lý sự cố ATTT tại Bộ TNMT		X			Trình bày đầy đủ quá trình thử nghiệm tại Cục CNTT và dữ liệu TNMT – Bộ TNMT, với những nội dung chính gồm: - Kịch bản thử nghiệm gồm 14 bài kiểm tra cho hệ thống đánh giá, quản lý rủi ro ATTT; 06 bài kiểm tra đối với hệ thống hỗ trợ xử lý sự cố. Các kết quả thử nghiệm tương ứng với những kịch bản cho cả hai hệ thống phần mềm sản phẩm của đề tài.	
11.	Báo cáo giải pháp hữu ích sản phẩm của đề tài		X			Đã xây dựng được 02 giải pháp nộp Bộ KHCN để xin cấp bằng sáng chế/giải pháp hữu ích: 1. "*Phương pháp phát hiện đoạn mã độc trong mã nguồn ứng dụng Web sử dụng ngôn ngữ PHP*". Mã số đơn 1-2020-06834 (26/11/2020) đã được Cục Sở hữu trí tuệ Bộ KH&CN chấp nhận đơn hợp lệ theo Quyết định số 1494w/QĐ-SHTT ngày 29/01/2021. 2. "*Phương pháp phát hiện đoạn mã độc trong mã nguồn ứng dụng Web sử dụng ngôn ngữ ASP*". Mã số đơn 1-2021-00205 đã được Cục Sở hữu trí tuệ Bộ KH&CN nhận hồ từ 15/01/2021.	

12.	Báo cáo tổng kết và tóm tắt kết quả đề tài		X			Tổng hợp được toàn bộ những kết quả thu được từ các nội dung đã thực hiện trong nhiệm vụ này	
13.	Bài báo khoa học		X			*Đã công bố được 06 công trình, gồm:* **04 bài tạp chí (03 trên tạp chí quốc tế thuộc danh mục Scopus, WoS; 01 bài trên tạp chí uy tín trong nước)** 1. Nguyễn Kim Sao, Nguyen Ngoc Hoa, Pham Van At (2020), An effective reversible data hiding method based on pixel-value-ordering, Journal of Computer Science and Cybernetics, V.36, N.2 (2020). 2. Tran, Nghi Phu and Hoang, Dang Kien and Ngo, Quoc Dung and Nguyen, Dai Tho and Nguyen, Ngoc Binh, *A Novel Framework to Classify Malware in MIPS Architecture-based IoT Devices*. Hindawi Security and Communication Networks. Volume 2019, Article ID 4073940 (SCI-E, Scopus). 3. Phuong-Hanh DU, Ngoc Son DUONG, Ngoc-Cuong NGUYEN and Ngoc-Hoa NGUYEN, *A Fast Computation of the Betweenness Centrality in Social Networks*, International Journal on Emerging Technologies, 11(2):370–377 (WoS, Scopus), 2020 4. Ha LE Viet, On PHUNG Van and Hoa NGUYEN Ngoc, "Information Security Risk Management by a Holistic Approach: a Case Study for Vietnamese e-Government", IJCSNS International Journal of Computer Science and Network Security, Vol. 20, No. 6, pp.72-82, 2020 (WoS-ESCI). 5. Ha V. Le, Tu N. Nguyen, Hoa N. Nguyen, "Hybrid ASP.NET Webshell Detection Using Static Analysis and Deep Learning", submitted to Computers & Security Journal, 2021. **02 bài trên Kỷ yếu Hội nghị quốc tế (danh mục Scopus/WoS)** 1. Ngoc-Hoa NGUYEN, Viet-Ha LE, Van-On PHUNG, and Phuong-Hanh DU. 2019. Toward a Deep Learning Approach for Detecting PHP Webshell. In the Tenth International Symposium on Information and Communication Technology (SoICT 2019), December 4–6, 2019, Hanoi - Ha Long Bay, Viet Nam. ACM, New York, NY, USA, (WoS, Scopus). 2. C. N. Van, V. A. Phan, V. L. Cao and K. D. T. Nguyen, "IoT Malware Detection based on Latent Representation," *2020 12th International Conference on Knowledge and Systems Engineering (KSE)*, Can Tho, Vietnam, 2020, pp. 177-182.	

14.	Đào tạo thạc sỹ		X			Đã đào tạo được 06 thạc sỹ 1. Nguyễn Văn Cường, Thạc sỹ HTTT, HVTKQS, 2021. Người hướng dẫn: TS. Phan Việt Anh. 2. Lã Xuân Kiên, Thạc sỹ ATTT, 2021. Người hướng dẫn: TS. Nguyễn Đại Thọ. 3. Trần Quang Chung, Thạc sỹ ATTT, 2020. Người hướng dẫn: TS. Nguyễn Đại Thọ. 4. Đỗ Bá Sơn, Thạc sỹ HTTT, 2020. Người hướng dẫn: PGS. Nguyễn Ngọc Hoá. 5. Vũ Việt Dũng, Thạc sỹ HTTT, 2020. Người hướng dẫn: PGS. Nguyễn Ngọc Hoá. 6. Nguyễn Thành Văn, Thạc sỹ HTTT, 2019. Người hướng dẫn: PGS. Nguyễn Ngọc Hoá.	
15.	Tham gia đào tạo tiến sỹ		X			Đã hỗ trợ đào tạo 02 NCS: - NCS. Lê Việt Hà, "*Nghiên cứu một số phương pháp học sâu trong phát hiện đoạn mã độc*", bắt đầu từ 2019. - NCS. Nguyễn Kim Sao, "*Phát triển một số phương pháp giấu tin thuận nghịch trên ảnh đa cấp xám*", bảo vệ 2020.	

1.2. Danh mục sản phẩm khoa học dự kiến ứng dụng, chuyển giao (nếu có):

Số TT	Tên sản phẩm	Thời gian dự kiến ứng dụng	Cơ quan dự kiến ứng dụng	Ghi chú
1	Quy trình đánh giá, quản lý rủi ro ATTT trong các hệ thống CNTT của CPĐT	2021	Bộ TT&TT	Hiện đang ở bước xin ý kiến chuẩn bị ban hành
2	Quy trình hỗ trợ xử lý sự cố ATTT đối với các hệ thống trong CPĐT	2021	Bộ TT&TT	Hiện đang ở bước xin ý kiến chuẩn bị ban hành
3	Hệ thống đánh giá, quản lý rủi ro an toàn thông tin UET.SRA	2021	Các bộ ngành, tỉnh, thành phố trực thuộc Trung ương; cơ quan tổ chức, doanh nghiệp khác có nhu cầu	Hiện đã triển khai tại Bộ TNMT
4	Hệ thống hỗ trợ xử lý sự cố an toàn thông tin UET.SIR	2021	Các bộ ngành, tỉnh, thành phố trực thuộc Trung ương; cơ quan tổ chức, doanh nghiệp khác có nhu cầu	Hiện đã triển khai tại Bộ TNMT

2. Về những đóng góp mới của nhiệm vụ:

Những đóng góp có tính mới, sáng tạo của nhóm đề tài gồm:

- Đã xây dựng được (i) quy trình đánh giá, quản lý rủi ro ATTT trong CPĐT với sự kết hợp cả phương pháp đánh giá, quản lý rủi ro của ISO/IEC 27005-2011, NIST SP800-39 và NIST SP800-53r4; và (ii) quy trình hỗ trợ xử lý sự cố ATTT trong CPĐT theo phương pháp của ISO/IEC 27035-2011 và NIST SP800-61r1.
- Đã xây dựng được hệ thống phần mềm UET.SRA cho phép thực hiện được các nghiệp vụ quản lý rủi ro ATTT theo quy trình đề xuất; bao gồm cả chức năng dò quét sâu lỗ hổng hệ thống, Website, bản vá chưa áp dụng, chính sách không tuân thủ, dò quét mã nguồn ứng dụng Web, đánh giá tổng thể theo CVSS/OWASP, xây dựng phương án xử lý rủi ro theo NIST SP800-53r4.
- Đã xây dựng được hệ thống phần mềm UET.SIR với USB chuyên dụng chứa công cụ thu thập được những dữ liệu chứng cứ sự cố ATTT quan trọng, cung cấp các chức năng để phân tích dữ liệu sự cố (dò quét mã độc, phân tích theo kiểu xếp chồng, so khác, …).
- Đã thử nghiệm được toàn bộ hai quy trình đề xuất cũng như hai hệ thống UET.SRA, UET.SIR thực tế tại Bộ TNMT. Các kết quả bước đầu thu được đã minh chứng tính khả

thi của sản phẩm, hỗ trợ hiệu quả cho công tác đảm bảo ATTT tại cơ quan cấp Bộ thông qua những chức năng của hai hệ thống đã xây dựng được.

- Đã xây dựng được 02 phương pháp xin cấp bằng Sáng chế/Giải pháp hữu ích của Bộ KHCN và đã được chấp nhận đơn hợp lệ.

Hiện nay, trong các cơ quan nhà nước, với số lượng dịch vụ công triển khai trực tuyến trên nền Web rất lớn, việc đánh giá, xác định các rủi ro ATTT từ bên trong mã nguồn các dịch vụ trên nền Web đó sẽ cho phép phát hiện sớm những nguy cơ, lỗ hổng mà các đơn vị xây dựng phần mềm có thể bỏ sót trước khi triển khai. Đây cũng là một trong những điểm nhấn thể hiện tính độc đáo của hệ thống đánh giá, quản lý rủi ro ATTT của đề tài. Ngoài ra, việc cung cấp thêm khả năng phát hiện những Windows Policy vi phạm quy định của cơ quan nhà nước, phát hiện những máy tính Windows chưa cập nhật những bản vá lỗ hổng quan trọng, … cũng cho phép nâng cao được khả năng phát hiện rủi ro ATTT trong hệ thống phần mềm của chúng tôi.

Đối với công tác hỗ trợ xử lý sự cố ATTT, hiện thách thức ATTT do các phần mềm độc hại, do tấn công mạng, … ngày càng tăng. Vì thế, làm chủ được nghiên cứu công nghệ, kỹ thuật trong việc thu thập dữ liệu chứng cứ lẫn xây dựng hệ thống quản lý, phân tích, xác định nguyên nhân sự cố, từ đó đưa ra được những tư vấn, gợi ý hỗ trợ chuyên gia xây dựng phương án khắc phục tại Việt Nam cũng là một điểm thể hiện được tính mới của sản phẩm trong đề tài này.

Cuối cùng, thông qua việc nghiên cứu, xây dựng các quy trình đánh giá rủi ro ATTT và hỗ trợ xử lý sự cố trong các cơ quan nhà nước; chuyên biệt hoá cho các cơ quan cấp Bộ/Ngành và cơ quan cấp Tỉnh/Thành trực thuộc trung ương, sản phẩm của đề tài sẽ góp phần tích cực trong việc nâng cao nhận thức về đảm bảo ATTT nói chung tại các cơ quan nhà nước. . Từ đó có thể giảm thiểu rủi ro ATTT và hỗ trợ xử lý sự cố ATTT trong Chính phủ điện tử Việt Nam.

3. Về hiệu quả của nhiệm vụ:

3.1. Hiệu quả kinh tế

Các quy trình và hệ thống đánh giá, quản lý rủi ro và hỗ trợ xử lý sự cố an toàn thông tin trong Chính phủ điện tử Việt Nam được xây dựng trong đề tài có phạm vi áp dụng tại các cơ quan nhà nước cấp Bộ, tỉnh, thành phố trực thuộc Trung ương.

Hai hệ thống phần mềm sản phẩm của đề tài là UET.SRA và UET.SIR đa được triển khai ứng dụng tại Bộ TNMT để hỗ trợ công tác đảm bảo ATTT tại Bộ này. Ngoài ra, tại Bộ Thông tin và Truyền thông, các hệ thống phần mềm này hoàn toàn có thể triển khai, vận hành tại các đơn vị của Bộ, cụ thể có thể được ứng dụng tại Cục ATTT và Trung tâm thông tin – Bộ TTTT. Ngoài ra, hai hệ thống phần mềm cũng hoàn toàn có thể tuỳ biến để triển khai tại các cơ quan cấp Bộ, tỉnh, thành phố trực thuộc Trung ương. Từ đó, các sản phẩm của đề tài cho phép giảm thiểu chi phí trong việc mua các sản phẩm tương tự của nước ngoài để đánh giá, quản lý rủi ro và hỗ trợ công tác xử lý sự cố ATTT (chẳng hạn như sản phẩm tương tự của hãng Rapid7,

Tenable, Qualys, IBM Security Operations and Response, … đều có giá thành rất cao).

Ngoài tác động về giảm chi phí đầu tư, các chức năng hỗ trợ đánh giá và quản lý rủi ro ATTT của UET.SRA cho phép giảm thiểu được những nguy cơ mất ATTT thông qua việc chủ động phát hiện các lỗ hổng rủi ro. Từ đó giảm thiểu được những chi phí mất mát thông tin, dữ liệu từ các sự cố mất ATTT. Ngoài ra, các chức năng của hệ thống UET.SIR trong hoạt động hỗ trợ xử lý sự cố mất ATTT cũng góp phần nâng cao hiệu quả công tác ứng cứu sự cố ATTT của các chuyên gia, sớm phát hiện được nguyên nhân sự cố và góp phần giảm thiểu được những thiệt hại cả về kinh tế, danh tiếng lẫn thông tin, dữ liệu của các hệ thống trong Chính phủ điện tử, kinh tế số hiện nay.

3.2. Hiệu quả xã hội

Ngoài những tác động về kinh tế nêu trên, các kết quả, sản phẩm của đề tài cũng có những tác động tích cực đối với xã hội như liệt kê dưới đây:

- Nâng cao được nhận thức về việc đảm bản ATTT nói chung của cán bộ trong các cơ quan nhà nước thông qua những quy trình, tiêu chuẩn về quản lý rủi ro nói chung. Từ đó góp phần giảm thiểu được những nguy cơ, rủi ro mất ATTT trong các cơ quan đó.
- Tạo cơ sở vững chắc để các cơ quan nhà nước làm chủ khả năng tự đảm bảo những vấn đề ATTT nói chung thông qua những sản phẩm của đề tài; tránh thêm được một phần những rủi ro mất ATTT khi sử dụng những dịch vụ tương tự từ các tổ chức/doanh nghiệp khác.
- Đảm bảo được những vấn đề an toàn phần mềm khi triển khai những hệ thống đảm bảo ATTT nói chung trong cơ quan nhà nước. Đây cũng là một trong những lợi điểm nổi bật nhất khi các sản phẩm của đề tài được các nhóm nghiên cứu từ các trường Đại học, cơ sở nghiên cứu của Nhà nước xây dựng và phát triển; từ đó góp phần giảm thiểu cũng như tránh được những nguy cơ mất ATTT từ chính những sản phẩm ngoài nước trong việc đánh giá, quản lý rủi ro và hỗ trợ công tác xử lý sự cố ATTT.

Ngoài ra, sản phẩm của đề tài hoàn toàn có thể được mở rộng, ứng dụng cho các doanh nghiệp, tổ chức khác. Khi đó, toàn bộ những tác động nêu trên còn có phổ lan toả rộng hơn nữa, từ đó minh chứng rõ nét hơn những tác động tích cực và hữu ích của các sản phẩm đề tài trong kinh tế - xã hội.

Sau khi hoàn thiện, phát triển thêm các tính năng chuyên biệt, hai hệ thống phần mềm trong nhiệm vụ này có thể triển khai phục vụ công tác nghiệp vụ trong các đơn vị có nhiệm vụ đảm bảo an ninh xã hội, quốc phòng như Cục CNTT, Cục An ninh mạng - Bộ Công an, Bộ Tư lệnh 86 – Bộ Quốc phòng.

III. Tự đánh giá, xếp loại kết quả thực hiện nhiệm vụ

1. Về tiến độ thực hiện: *(đánh dấu ✓ vào ô tương ứng*):

- *Nộp hồ sơ đúng hạn* ☒
- *Nộp chậm từ trên 30 ngày đến 06 tháng* ☐
- *Nộp hồ sơ chậm trên 06 tháng* ☐

2. Về kết quả thực hiện nhiệm vụ:

- *Xuất sắc* ☐
- *Đạt* ☒
- *Không đạt* ☐

Giải thích lý do:

Đề tài KC.01.19/16-20 đã hoàn thành mục tiêu nghiên cứu, đã hoàn thành đầy đủ các sản phẩm, đáp ứng được các yêu cầu về số lượng, chất lượng, khối lượng đã đặt ra trong thuyết minh và hợp đồng đã ký.

Cam đoan nội dung của Báo cáo là trung thực; Chủ nhiệm và các thành viên tham gia thực hiện nhiệm vụ không sử dụng kết quả nghiên cứu của người khác trái với quy định của pháp luật.

CHỦ NHIỆM NHIỆM VỤ	**THỦ TRƯỞNG TỔ CHỨC CHỦ TRÌ NHIỆM VỤ**
Nguyễn Ngọc Hoá	