# CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

**Độc lập - Tự do - Hạnh phúc**

*Hà Nội, ngày 30 tháng 10 năm 2019*

# BÁO CÁO KẾT QUẢ TỰ ĐÁNH GIÁ

**NHIỆM VỤ KHOA HỌC VÀ CÔNG NGHỆ CẤP QUỐC GIA**

1. **Thông tin chung về nhiệm vụ:**
	1. Tên nhiệm vụ, mã số:

Nghiên cứu, phát triển hệ thống phân tích vết truy cập dịch vụ cho phép phát hiện, cảnh báo hành vi bất thường và nguy cơ mất an toàn thông tin trong Chính phủ điện tử.

Mã số đề tài, dự án: KC.01.05/16-20 2. Mục tiêu

 (1) nghiên cứu, đề xuất giải pháp thu thập và phân tích vết truy cập các máy chủ tại các cơ quan cấp Tỉnh/Thành phố/Bộ, nhằm trích xuất các thông tin có giá trị hỗ trợ phát hiện, cảnh báo hành vi bất thường và đảm bảo an toàn thông tin;

(2) xây dựng, phát triển hệ thống phân tích nhật ký vết truy cập dịch vụ hỗ trợ phát hiện, cảnh báo hành vi bất thường và nguy cơ mất an toàn thông tin và triển khai thử nghiệm tại cơ quan cấp Tỉnh/Thành phố/Bộ.

Các mục tiêu cụ thể của đề tài như sau:

3.Chủ nhiệm nhiệm vụ:

Họ và tên: Hoàng Xuân Dậu

 4. Tổ chức chủ trì nhiệm vụ: Học viện Công nghệ Bưu chính Viễn thông

5. Tổng kinh phí thực hiện: 5.490 triệu đồng.

|  |  |  |  |
| --- | --- | --- | --- |
| **Số TT** | **Họ và tên** | **Chức danh khoa****học, học vị** | **Cơ quan công tác** |
| 1 | Hoàng Xuân Dậu | TS | Học viện Công nghệ Bưu chính Viễn thông |
| 2 | Nguyễn Ngọc Điệp | TS | Học viện Công nghệ Bưu chính Viễn thông |
| 3 | Phạm Hoàng Duy | TS | Học viện Công nghệ Bưu chính Viễn thông |
| 4 | Nguyễn Mạnh Sơn | ThS | Học viện Công nghệ Bưu chính Viễn thông |
| 5 | Ngô Quốc Dũng | TS | Học viện Công nghệ Bưu chính Viễn thông |
| 6 | Đỗ Xuân Chợ | TS | Học viện Công nghệ Bưu chính Viễn thông |
| 7 | Hoàng Đăng Hải | PGS.TSKH | Học viện Công nghệ Bưu chính Viễn thông |
| 8 | Trần Mạnh Thắng | ThS | Cục An toàn thông tin |
| 9 | Nguyễn Ngọc Quân | ThS | Tập đoàn Bưu chính Viễn thông Việt Nam |
| 10 | Nguyễn Thị Thanh Thủy | ThS | Học viện Công nghệ Bưu chính Viễn thông |

6. Thời gian thực hiện theo Hợp đồng: Bắt đầu: 10/2017 Kết thúc: 9/2019

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

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

* 1. Về sản phẩm khoa học:
	2. 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 | Hệ thống thu thập và phân tích vết (log) truy cập dịch vụ trong Chính phủ điện tử |  | ✔ |  |  | ✔ |  |
| 2 | Bộ tài liệu đặc tả toàn bộ giải pháp thu thập và phân tích log truy cập các máy chủ tại các cơ quan cấp Tỉnh/Thành Phố/Bộ, nhằm trích xuất các thông tin có giá trị hỗ trợ phát hiện và cảnh báo hành vi bất thường và đảm bảo an toàn thông tin |  | ✔ |  |  | ✔ |  |
| 3 | Bộ tài liệu phân tích và thiết kế chi tiết hệ thống phân tích log truy cập dịch vụ |  | ✔ |  |  | ✔ |  |
| 4 | Bộ tài liệu thử nghiệm và đánh giá hệ thống phân tích log truy cập dịch vụ |  | ✔ |  |  | ✔ |  |
| 5 | Bộ tài liệu hướng dẫn triển khai, cài đặt và hướng dẫn sử dụng |  | ✔ |  |  | ✔ |  |
| 6 | Bài báo tạp chí khoa học quốc tế (ISI hoặc Scorpus) |  | ✔ |  |  | ✔ |  |
| 7 | Bài báo hội nghị khoa học quốc tế | ✔ |  |  |  | ✔ |  |
| 8 | Tham gia đào tạo Thạc sỹ | ✔ |  |  |  | ✔ |  |
| 9 | Tham gia đào tạo Tiến sỹ (Góp phần đào tạo) |  | ✔ |  |  | ✔ |  |

* 1. 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 | Hệ thống thu thập và phân tích vết (log) truy cập dịch vụ trong Chính phủ điện tử | 2020 | Sở TT-TT tỉnh Sóc Trăng và Sở TT-TT tỉnh Quảng Nam | Hệ thống chỉnh sửa rút gọn cho phù hợp |

* 1. Về những đóng góp mới của nhiệm vụ:

Trong lĩnh vực KHCN, đề tài có tác động và lợi ích mang lại không chỉ cho ngành an toàn thông tin mà cả ngành khoa học máy tính và công nghệ thông tin, với việc đã xuất bản 02 công trình khoa học trên các tạp chí có uy tín của quốc tế và 03 công trình nghiên cứu báo cáo trong các Hội nghị khoa học quốc tế. Đề tài cũng góp phần đào tạo 05 thạc sỹ và 01 nghiên cứu sinh.

Đối với lĩnh vực an toàn thông tin, đề tài đề xuất các kỹ thuật, giải pháp mới cho phát hiện các hành vi truy cập bất thường, các dấu hiệu xuất hiện botnet, các dạng tấn công DoS/DDoS và các dạng tấn công thường gặp lên ứng dụng web. Các kỹ thuật, giải pháp đề xuất giúp tăng độ chính xác phát hiện, giảm cảnh báo sai và nhờ vậy nâng cao hiệu quả việc giám sát, đảm bảo an toàn thông tin.

Đối với lĩnh vực khoa học máy tính và công nghệ thông tin, các kỹ thuật và giải pháp đề xuất cho xử lý dữ liệu lớn, xây dựng tập luật dựa trên học máy, khai phá dữ liệu, thống kê và ứng dụng trong lĩnh vực an toàn thông tin là những đóng góp đáng kể ở Việt Nam và cả trên thế giới.

* 1. Về hiệu quả của nhiệm vụ:
	2. Hiệu quả kinh tế

Hệ thống phần mềm của đề tài được phát triển dựa trên các kỹ thuật, công nghệ tiên tiến hiện nay, có chi phí thấp và đáp ứng nhiều chức năng tương đương với nhiều sản phẩm thương mại khác.

Các kết quả nghiên cứu của đề tài sẽ tạo cơ hội kinh doanh cho Trung tâm tư vấn và hỗ trợ nghiệp vụ an toàn thông tin thuộc Cục An toàn thông tin. Trung tâm có thể liên kết với Học viện để phối hợp triển khai kết quả đề tài phục vụ phát hiện các hành vi truy cập bất thường và cảnh báo các nguy cơ mất an toàn thông tin đối với hệ thống mạng chính phủ điện tử tại các cơ quan, tổ chức cấp tỉnh, thành phố, hoặc cấp bộ.

* 1. Hiệu quả xã hội

Trong lĩnh vực khoa học và công nghệ, đề tài có tác động và lợi ích mang lại không chỉ cho ngành an toàn thông tin mà cả ngành khoa học máy tính và công nghệ thông tin,… Đề tài đã xuất bản 05 công trình khoa học trên các tạp chí có uy tín quốc tế và các Hội nghị khoa học quốc tế. Đề tài cũng góp phần

đào tạo các thạc sỹ và nghiên cứu sinh. Các nội dung đề tài đã trở thành chủ đề luận văn, góp phần hướng dẫn học viên cao học thực hiện thực hiện luận văn tốt nghiệp và nghiên cứu sinh thực hiện luận án tiến sỹ.

Các kết quả đề tài là các bài báo khoa học đăng trên tạp chí và hội thảo quốc tế uy tín góp phần nâng cao thương hiệu, uy tín khoa học cho Học viện. Các kết quả đào tạo sau đại học góp phần tăng số lượng các học viên sau đại học được đào tạo tại Học viện. Đồng thời, nội dung các đề tài luận văn Thạc sỹ liên quan đến các hướng công nghệ nghiên cứu của đề tài này làm phong phú các luận văn thạc sỹ của Học viện, cũng như góp phần bổ sung vào cơ sở dữ liệu tham khảo quan trọng cho sinh viên, giảng viên, nghiên cứu viên của Học viện.

Đối với các đơn vị phối hợp của đề tài, gồm Trung tâm Tư vấn và Hỗ trợ nghiệp vụ an toàn thông tin (Nay là Trung tâm giám sát an toàn không gian mạng quốc gia) - Cục An toàn thông tin, Sở Thông tin Truyền thông tỉnh Quảng Nam và Sở Thông tin Truyền Thông tỉnh Sóc Trăng, việc triển khai thử nghiệm thành công hệ thống thu thập, xử lý và phân tích log truy cập phục vụ phát hiện các hành vi truy cập bất thường và cảnh báo các nguy cơ mất an toàn thông tin của hệ thống mạng chính phủ điện tử tại mỗi đơn vị là tiền đề quan trọng cho khả năng triển khai hệ thống hoạt động lâu dài, ổn định trong tương lai. Đây là một giải pháp quan trọng trong nhóm các giải pháp đảm bảo cho hệ thống mạng chính phủ điện tử hoạt động thông suốt, an toàn.

# 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* |

1. Về kết quả thực hiện nhiệm vụ:
	* *Xuất sắc*
	* *Đạt *
	* *Không đạt*

Giải thích lý do: Các sản phẩm đạt các yêu cầu khoa học đề ra trong Thuyết minh được duyệt, đáp ứng đầy đủ các yêu cầu về số lượng và chất lượng

.

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**(*Học hàm, học vị, Họ, tên và chữ ký*) | **THỦ TRƯỞNG****TỔ CHỨC CHỦ TRÌ NHIỆM VỤ**(*Họ, tên, chữ ký và đóng dấu*) |

# TS. Hoàng Xuân Dậu