BÁO CÁO KINH TẾ - KỸ THUẬT

**DỰ ÁN: XÂY DỰNG HỆ THỐNG**

**HỖ TRỢ SĂN TÌM MỐI NGUY CƠ**

ĐÀ NẴNG - 2025

**MỤC LỤC**

[I. THÔNG TIN CHUNG 5](#_Toc193950966)

[1. Căn cứ pháp lý 5](#_Toc193950967)

[2. Tên dự án 6](#_Toc193950968)

[3. Đơn vị sử dụng ngân sách 6](#_Toc193950969)

[4. Địa điểm thực hiện 6](#_Toc193950970)

[5. Tổ chức, đơn vị lập Báo cáo kinh tế - kỹ thuật 6](#_Toc193950971)

[II. SỰ CẦN THIẾT ĐẦU TƯ 6](#_Toc193950972)

[1. Hiện trạng ứng dụng CNTT 6](#_Toc193950973)

[2. Sự cần thiết thực hiện hoạt động ứng dụng công nghệ thông tin 6](#_Toc193950974)

[III. ĐÁNH GIÁ SỰ PHÙ HỢP VỚI QUY HOẠCH CÓ LIÊN QUAN THEO QUY ĐỊNH CỦA PHÁP LUẬT VỀ QUY HOẠCH 7](#_Toc193950975)

[1. Căn cứ pháp lý 7](#_Toc193950976)

[2. Đánh giá sự phù hợp 7](#_Toc193950977)

[IV. PHÂN TÍCH, XÁC ĐỊNH MỤC TIÊU, NHIỆM VỤ, KẾT QUẢ ĐẦU RA CỦA DỰ ÁN; PHÂN TÍCH, LỰA CHỌN QUY MÔ HỢP LÝ; XÁC ĐỊNH PHÂN KỲ ĐẦU TƯ; LỰA CHỌN HÌNH THỨC ĐẦU TƯ 8](#_Toc193950978)

[1. Phân tích, xác định mục tiêu, nhiệm vụ 8](#_Toc193950979)

[2. Phân tích, xác định kết quả đầu ra của dự án 8](#_Toc193950980)

[3. Phân tích, lựa chọn quy mô 8](#_Toc193950981)

[4. Xác định phân kỳ đầu tư 9](#_Toc193950982)

[5. Lựa chọn hình thức đầu tư 9](#_Toc193950983)

[V. PHÂN TÍCH CÁC ĐIỀU KIỆN TỰ NHIÊN, ĐIỀU KIỆN KINH TẾ - KỸ THUẬT, LỰA CHỌN ĐỊA ĐIỂM ĐẦU TƯ 9](#_Toc193950984)

[1. Phân tích các điều kiện tự nhiên, điều kiện kinh tế - kỹ thuật 9](#_Toc193950985)

[1.1. Điều kiện tự nhiên 9](#_Toc193950986)

[1.2. Điều kiện kinh tế - kỹ thuật 9](#_Toc193950987)

[2. Lựa chọn địa điểm đầu tư 10](#_Toc193950988)

[VI. PHÂN TÍCH, LỰA CHỌN PHƯƠNG ÁN, GIẢI PHÁP KỸ THUẬT, CÔNG NGHỆ ĐỀ XUẤT 10](#_Toc193950989)

[1. Danh mục quy chuẩn kỹ thuật, tiêu chuẩn công nghệ thông tin được áp dụng 10](#_Toc193950990)

[1.1. Tiêu chuẩn kỹ thuật CNTT 10](#_Toc193950991)

[1.2. Các tiêu chuẩn khác 18](#_Toc193950992)

[1.3. Yêu cầu chức năng tối thiểu của Hệ thống hỗ trợ săn tìm mối nguy cơ 19](#_Toc193950993)

[2. Phân tích, lựa chọn phương án, giải pháp kỹ thuật, công nghệ 21](#_Toc193950994)

[3. Phân tích, lựa chọn phương án, giải pháp kết nối, liên thông, chia sẻ dữ liệu với các hệ thống hạ tầng kỹ thuật, phần mềm, cơ sở dữ liệu liên quan 21](#_Toc193950995)

[4. Thuyết minh giải pháp kỹ thuật, công nghệ 22](#_Toc193950996)

[4.1. Tên phần mềm 22](#_Toc193950997)

[4.2. Các tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin theo quy định của Nhà nước 22](#_Toc193950998)

[4.3. Các yêu cầu chung về Hệ thống hỗ trợ săn tìm mối nguy cơ 23](#_Toc193950999)

[4.4. Thiết kế giao diện Hệ thống hỗ trợ săn tìm mối nguy cơ 23](#_Toc193951000)

[4.5. Các quy trình nghiệp vụ cần được tin học hóa 24](#_Toc193951001)

[4.6. Các yêu cầu phi chức năng 27](#_Toc193951002)

[4.7. Yêu cầu năng lực của cán bộ tham gia phát triển, nâng cấp, chỉnh sửa phần mềm 34](#_Toc193951003)

[4.8. Yêu cầu về bảo hành phần mềm 34](#_Toc193951004)

[4.9. Yêu cầu về đào tạo và chuyển giao công nghệ 35](#_Toc193951005)

[4.10. Yêu cầu về kiểm thử, vận hành thử 36](#_Toc193951006)

[VII. PHƯƠNG ÁN TỔ CHỨC QUẢN LÝ, KHAI THÁC, SỬ DỤNG DỰ ÁN 37](#_Toc193951007)

[VIII. ĐÁNH GIÁ TÁC ĐỘNG MÔI TRƯỜNG VÀ GIẢI PHÁP BẢO VỆ MÔI TRƯỜNG 37](#_Toc193951008)

[IX. PHƯƠNG ÁN TỔNG THỂ ĐỀN BÙ, GIẢI PHÓNG MẶT BẰNG, TÁI ĐỊNH CƯ 37](#_Toc193951009)

[X. DỰ KIẾN TIẾN ĐỘ THỰC HIỆN DỰ ÁN; CÁC MỐC THỜI GIAN CHÍNH THỰC HIỆN ĐẦU TƯ 37](#_Toc193951010)

[XI. XÁC ĐỊNH TỔNG MỨC ĐẦU TƯ, CƠ CẤU NGUỒN VỐN, PHƯƠNG ÁN HUY ĐỘNG VỐN 38](#_Toc193951011)

[XII. XÁC ĐỊNH CHI PHÍ VẬN HÀNH, BẢO DƯỠNG, DUY TU, SỬA CHỮA LỚN TRONG GIAI ĐOẠN KHAI THÁC DỰ ÁN 38](#_Toc193951012)

[XIII. TỔ CHỨC QUẢN LÝ DỰ ÁN, BAO GỒM XÁC ĐỊNH CHỦ ĐẦU TƯ, PHÂN TÍCH LỰA CHỌN HÌNH THỨC TỔ CHỨC QUẢN LÝ THỰC HIỆN DỰ ÁN, MỐI QUAN HỆ VÀ TRÁCH NHIỆM CỦA CÁC CHỦ THỂ LIÊN QUAN ĐẾN QUÁ TRÌNH THỰC HIỆN DỰ ÁN, TỔ CHỨC BỘ MÁY QUẢN LÝ KHAI THÁC DỰ ÁN 38](#_Toc193951013)

[1. Chủ đầu tư 38](#_Toc193951014)

[2. Phân tích lựa chọn hình thức tổ chức quản lý thực hiện dự án 39](#_Toc193951015)

[XIV. CÁC ĐỀ XUẤT, KIẾN NGHỊ 39](#_Toc193951016)

[XV. PHỤ LỤC: THUYẾT MINH DỰ TOÁN 40](#_Toc193951017)

[1. Cơ sở lập dự toán chi tiết 40](#_Toc193951018)

[2. Dự toán chi tiết 40](#_Toc193951019)

[2.1. Tổng hợp dự toán 40](#_Toc193951020)

[2.2. Dự toán chi tiết 41](#_Toc193951021)

[3. Thuyết minh diễn giải chi tiết dự toán 42](#_Toc193951022)

[3.1. Bảng danh sách tác nhân (Actors) 42](#_Toc193951023)

[3.2. Bảng danh sách các yêu cầu chức năng của phần mềm 43](#_Toc193951024)

[3.3. Bảng chuyển đổi yêu cầu chức năng sang trường hợp sử dụng (usecase) 45](#_Toc193951025)

[3.4. Bảng tính toán điểm các tác nhân (actors) tương tác, trao đổi thông tin với phần mềm 48](#_Toc193951026)

[3.5. Bảng tính toán điểm các trường hợp sử dụng 49](#_Toc193951027)

[3.6. Bảng tính toán hệ số phức tạp kỹ thuật – công nghệ 49](#_Toc193951028)

[3.7. Bảng tính toán hệ số tác động môi trường và nhóm làm việc, hệ số phức tạp về môi trường, xác định độ ổn định kinh nghiệm và nội suy thời gian lao động 54](#_Toc193951029)

[3.8. Bảng tính toán chi phí trực tiếp xây dựng, phát triển, mở rộng phần mềm nội bộ 55](#_Toc193951030)

[3.9. Chi phí đầu tư xây dựng, phát triển hình thành dịch vụ công nghệ thông tin 56](#_Toc193951031)

[3.10. Bảng diễn giải cách tính giờ công H 58](#_Toc193951032)

# I. THÔNG TIN CHUNG

## 1. Căn cứ pháp lý

* Luật Công nghệ thông tin số 67/2006/QH11 ngày 29/6/2006;
* Luật Ngân sách nhà nước số 83/2015/QH13 ngày 25/06/2015;
* Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015;
* Luật Tiếp cận thông tin số 104/2016/QH13 ngày 06/4/2016;
* Nghị định 163/2016/NĐ-CP ngày 21/12/2016 của Chính phủ quy định chi tiết và hướng dẫn thi hành Luật Ngân sách nhà nước;
* Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;
* Nghị định 82/2024/NĐ-CP ngày 10/07/2024 sửa đổi, bổ sung Nghị định 73/2019/NĐ-CP ngày 05/09/2019 của Chính phủ quy định quản lý đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước;
* Nghị định 42/2022/NĐ-CP ngày 24/06/2022 của Chính phủ quy định về việc cung cấp thông tin và dịch vụ công trực tuyến của cơ quan nhà nước trên môi trường mạng;
* Thông tư 39/2017/TT-BTTTT ngày 15/12/2017 của Bộ Thông tin và Truyền thông ban hành Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước;
* Thông tư 03/2020/TT-BTTTT ngày 24/02/2020 của Bộ Thông tin và Truyền thông quy định về lập đề cương và dự toán chi tiết đối với hoạt động ứng dụng công nghệ thông tin sử dụng kinh phí chi thường xuyên thuộc nguồn vốn ngân sách nhà nước;
* Thông tư 26/2020/TT-BTTTT ngày 23/9/2020 của Bộ Thông tin và Truyển thông quy định việc áp dụng tiêu chuẩn, công nghệ hỗ trợ người khuyết tật tiếp cận, sử dụng sản phẩm, dịch vụ thông tin và truyền thông;
* Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;
* Thông tư 22/2023/TT-BTTTT ngày 31/12/2023 của Bộ Thông tin và Truyền thông quy định cấu trúc, bố cục, yêu cầu kỹ thuật cho cổng thông tin điện tử và trang thông tin điện tử của cơ quan nhà nước;
* Quyết định 129/QĐ-BTTTT ngày 03/02/2021 của Bộ Thông tin và Truyền thông hướng dẫn xác định đơn giá nhân công trong quản lý chi phí đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước;
* Quyết định số 671/QĐ-BTTTT ngày 26/04/2024 của Bộ Thông tin và Truyền thông về việc Hướng dẫn xác định chi phí phần mềm nội bộ;

## 2. Tên dự án

Xây dựng hệ thống hỗ trợ săn tìm mối nguy cơ trên mạng máy tính quân sự.

## 3. Đơn vị sử dụng ngân sách

Trung tâm 386 - Bộ Tư lệnh 86.

## 4. Địa điểm thực hiện

- Trung tâm 386 - Bộ Tư lệnh 86.

- Địa chỉ: Số 39 Phan Tứ, Mỹ An, Ngũ Hành Sơn, Đà Nẵng

- Thời gian thực hiện: 12 tháng.

- Thời gian thực hiện nhiệm vụ: Năm 2025.

## 5. Tổ chức, đơn vị lập Báo cáo kinh tế - kỹ thuật

Trung tâm 386 - Bộ Tư lệnh 86.

# II. SỰ CẦN THIẾT ĐẦU TƯ

## 1. Hiện trạng ứng dụng CNTT

Hiện nay, lực lượng tác chiến mạng đang tiến hành các hoạt động săn tìm mối nguy cơ trên các hệ thống giám sát tập trung, nổi bật là FMS. Đây là hệ thống hỗ trợ mạnh mẽ cho nhiệm vụ săn tìm mối nguy cơ với tính năng thống kê, giám sát chặt chẽ các hoạt động, truy vấn bất thường từ máy tính, máy chủ trong mạng. Mặc dù rất hữu ích trong nhiệm vụ săn tìm mối nguy cơ, tuy nhiên các tính năng lại hỗ trợ gián tiếp và chưa thực sự rõ nét. Hệ thống chỉ mang tính cảnh báo, thông báo các hành vi, hoạt động đáng ngờ, các truy vấn của máy tính đến các địa chỉ, IP độc hại. Chưa hỗ trợ nhiều trong phân tích, xác định chiến dịch tấn công, thống kê và trực quan hóa các hành vi đáng ngờ của máy tính trong mạng. Các nhiệm vụ săn tìm, phát hiện mối nguy cơ vẫn đang tiêu tốn rất nhiều sức lực, nhân lực, chưa thể có một cái nhìn nhanh chóng và tổng quan đối với các hạ tầng mạng mà đơn vị giám sát, quản lý.

## 2. Sự cần thiết thực hiện hoạt động ứng dụng công nghệ thông tin

Mặc dù trên thế giới đã có nhiều hệ thống, phần mềm quản lý, trực quan hóa, so sánh dữ liệu, tuy nhiên đều rất khó để cấu hình và sử dụng cho mục đích đặc thù của nhiệm vụ Săn tìm mối nguy cơ trong Quân đội.

Ở trong nước, đặc biệt là Quân đội, hiện chưa có nhiều nghiên cứu, hệ thống cung cấp các chức năng hỗ trợ tốt cho nhiệm vụ săn tìm mối nguy cơ, ứng dụng vào các hoạt động tác chiến mạng.

Bài toán đặt ra cho nhiệm vụ tác chiến mạng là xây dựng một hệ thống có thể quản lý, trực quan hóa dữ liệu giám sát, bên cạnh đó cung cấp các tính năng hữu ích, tự động hóa một số công đoạn trong nhiệm vụ săn tìm mối nguy cơ trên mạng máy tính quân sự.

Vì vậy, nhiệm vụ xây dựng hệ thống hỗ trợ săn tìm mối nguy cơ, để phục vụ trong các nhiệm vụ tác chiến của đơn vị nói riêng và của Bộ Tư lệnh nói chung là vô cùng cần thiết.

# III. ĐÁNH GIÁ SỰ PHÙ HỢP VỚI QUY HOẠCH CÓ LIÊN QUAN THEO QUY ĐỊNH CỦA PHÁP LUẬT VỀ QUY HOẠCH

## 1. Căn cứ pháp lý

Dự án “Hệ thống Săn tìm mối nguy cơ trên mạng máy tính quân sự tại địa bàn miền Trung – Tây Nguyên” được xây dựng trên cơ sở các quy định pháp luật về quy hoạch ngành, lĩnh vực công nghệ thông tin, an ninh mạng và quốc phòng, cụ thể:

- Nghị quyết số 29-NQ/TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược bảo vệ Tổ quốc trên không gian mạng;

- Luật An ninh mạng số 24/2018/QH14 ngày 12/6/2018;

- Luật Quy hoạch số 21/2017/QH14 ngày 24/11/2017;

- Thông tư số 03/2020/TT-BTTTT ngày 24/02/2020 của Bộ TT&TT về lập, thẩm định, phê duyệt đề cương và dự toán chi tiết hoạt động ứng dụng CNTT sử dụng kinh phí chi thường xuyên;

- Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số ban hành kèm Quyết định số 942/QĐ-TTg ngày 15/6/2021 của Thủ tướng Chính phủ.

## 2. Đánh giá sự phù hợp

Dự án phù hợp với các quy hoạch, định hướng, kế hoạch sau:

- Phù hợp với Chiến lược bảo vệ Tổ quốc trên không gian mạng, đặc biệt là nội dung phát triển năng lực tự chủ về công nghệ, kỹ thuật trong giám sát, phát hiện và phòng ngừa tấn công mạng.

- Phù hợp với quy hoạch phát triển ứng dụng CNTT trong hoạt động quân sự, đảm bảo định hướng hiện đại hóa lực lượng tác chiến mạng, tăng cường khả năng phát hiện sớm, chủ động ứng phó với các mối đe dọa mạng.

- Gắn liền với nhu cầu thực tiễn tại địa phương (miền Trung – Tây Nguyên) và sự chỉ đạo của Bộ Tư lệnh 86 về triển khai các nhiệm vụ trọng điểm trên không gian mạng năm 2024 theo Kế hoạch số 2012/KH-BTL ngày 31/12/2023.

# IV. PHÂN TÍCH, XÁC ĐỊNH MỤC TIÊU, NHIỆM VỤ, KẾT QUẢ ĐẦU RA CỦA DỰ ÁN; PHÂN TÍCH, LỰA CHỌN QUY MÔ HỢP LÝ; XÁC ĐỊNH PHÂN KỲ ĐẦU TƯ; LỰA CHỌN HÌNH THỨC ĐẦU TƯ

## 1. Phân tích, xác định mục tiêu, nhiệm vụ

* Mục tiêu: Nghiên cứu xây dựng hệ thống hỗ trợ săn tìm mối nguy cơ triển khai trên nền tảng web. Hệ thống cho phép thu thập, phân tích, đánh giá và cảnh báo các hành vi đáng ngờ, phục vụ nhiệm vụ tác chiến mạng tại Trung tâm 386 và các đơn vị thuộc Bộ Tư lệnh 86.
* Nhiệm vụ:

+ Phân tích nghiệp vụ săn tìm mối nguy cơ của lực lượng tác chiến mạng;

+ Đề xuất giải pháp công nghệ, thiết kế hệ thống hỗ trợ thu thập, phân tích, cảnh báo các hành vi, truy vấn bất thường trong mạng MTQS;

+ Xây dựng phần mềm với các chức năng: thu thập dữ liệu từ FMS, phân tích và gán nhãn truy vấn, thống kê – trực quan hóa – sao lưu dữ liệu, quản lý chỉ số độc hại, người dùng, nhật ký;

+ Kiểm thử, hoàn thiện và bàn giao hệ thống cho đơn vị sử dụng;

+ Đảm bảo vận hành hệ thống hoạt động tốt trong thực tế. Kết hợp hỗ trợ kỹ thuật, đào tạo sử dụng sau bàn giao.

## 2. Phân tích, xác định kết quả đầu ra của dự án

Sau khi triển khai thực hiện nhiệm vụ xây dựng hệ thống hỗ trợ săn tìm mối nguy cơ, hệ thống dự kiến đạt được các kết quả, cụ thể như sau:

- Hệ thống hỗ trợ săn tìm mối nguy cơ: Yêu cầu hệ thống đáp ứng được các chức năng như trong phần mô tả. Có thể triển khai hoạt động tốt tại các đơn vị trong Bộ Tư lệnh 86.

- Tài liệu phân tích thiết kế hệ thống: Yêu cầu phân tích thiết kế mô hình hệ thống theo tiêu chuẩn, các sơ đồ UML, các mô đun, chức năng của hệ thống

- Tài liệu hướng dẫn sử dụng hệ thống: Yêu cầu tài liệu chi tiết, tỉ mỉ trong việc cài đặt, triển khai và sử dụng hệ thống

## 3. Phân tích, lựa chọn quy mô

Dự án được triển khai xây dựng với **quy mô phần mềm nội bộ**, áp dụng tại **Cụm 31 – Trung tâm 386 – BTL 86**, đồng thời **mở rộng khả năng triển khai tại các đơn vị khác thuộc BTL 86** nếu có nhu cầu.

Hệ thống được xây dựng trên nền tảng web, triển khai **trong mạng nội bộ quân sự**, phục vụ cho cán bộ thực hiện nhiệm vụ săn tìm mối nguy cơ trên không gian mạng. Phần mềm sẽ tích hợp với hệ thống FMS, cơ sở dữ liệu máy chủ độc hại, đồng thời hỗ trợ các tính năng phân tích, cảnh báo, thống kê và trực quan hóa thông tin.

## 4. Xác định phân kỳ đầu tư

Dự án được thực hiện đầu tư trong 01 năm:

* Thực hiện chuẩn bị đầu tư: Năm 2025
* Hoàn thành dự án: Năm 2025

## 5. Lựa chọn hình thức đầu tư

Mua sắm trang thiết bị công nghệ thông tin (phần mềm nội bộ).

# V. PHÂN TÍCH CÁC ĐIỀU KIỆN TỰ NHIÊN, ĐIỀU KIỆN KINH TẾ - KỸ THUẬT, LỰA CHỌN ĐỊA ĐIỂM ĐẦU TƯ

## 1. Phân tích các điều kiện tự nhiên, điều kiện kinh tế - kỹ thuật

### 1.1. Điều kiện tự nhiên

Dự án “Xây dựng hệ thống hỗ trợ săn tìm mối nguy cơ” có đặc thù là một dự án sử dụng công nghệ thông tin, cho nên không chịu ảnh hưởng của điều kiện tự nhiên.

### 1.2. Điều kiện kinh tế - kỹ thuật

**Cụm 31 – Trung tâm 386 – Bộ Tư lệnh 86** là đơn vị có đủ điều kiện về kinh tế – kỹ thuật để tổ chức triển khai dự án phần mềm nội bộ, bao gồm:

**- Hạ tầng công nghệ thông tin ổn định**, có hệ thống máy chủ, mạng nội bộ quân sự được bảo vệ và kiểm soát chặt chẽ theo các quy định hiện hành về an toàn thông tin và bảo mật quân sự.

**- Nguồn nhân lực kỹ thuật có trình độ**, lực lượng cán bộ chuyên trách về tác chiến mạng, an toàn thông tin có đủ năng lực để tiếp nhận, vận hành và khai thác hệ thống phần mềm nội bộ sau khi hoàn thiện.

**- Kinh nghiệm triển khai các dự án công nghệ thông tin chuyên ngành**, đã từng tham gia các nhiệm vụ xây dựng, thử nghiệm, tích hợp hệ thống an ninh mạng trong Quân đội.

**- Có sự phối hợp chặt chẽ với các đơn vị nghiệp vụ và cơ quan quản lý cấp trên**, đảm bảo quá trình triển khai dự án đúng tiến độ, đúng quy định, hiệu quả và tiết kiệm ngân sách.

Với các điều kiện thuận lợi về tổ chức, kỹ thuật và con người, Trung tâm đủ năng lực triển khai thành công dự án xây dựng hệ thống hỗ trợ săn tìm mối nguy cơ trên mạng máy tính quân sự.

## 2. Lựa chọn địa điểm đầu tư

* Trung tâm 386/Bộ Tư lệnh 86.
* Trụ sở: Số 39 Phan Tứ, Mỹ An, Ngũ Hành Sơn, Đà Nẵng

# VI. PHÂN TÍCH, LỰA CHỌN PHƯƠNG ÁN, GIẢI PHÁP KỸ THUẬT, CÔNG NGHỆ ĐỀ XUẤT

## 1. Danh mục quy chuẩn kỹ thuật, tiêu chuẩn công nghệ thông tin được áp dụng

### 1.1. Tiêu chuẩn kỹ thuật CNTT

Hệ thống khi thiết kế, triển khai đảm bảo tuân thủ danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nước công bố kèm theo Thông tư 39/2017/TT-BTTTT ngày 15/12/2017 của Bộ Thông tin và Truyền thông, cụ thể:

| **TT** | **Loại tiêu chuẩn** | **Ký hiệu tiêu chuẩn** | **Tên đầy đủ của tiêu chuẩn** | **Quy định áp dụng** |
| --- | --- | --- | --- | --- |
| **1** | **Tiêu chuẩn về kết nối** | | | |
| 1.1 | Truyền siêu văn bản | HTTP v1.1 | Hypertext Transfer Protocol version 1.1 | Bắt buộc áp dụng |
| HTTP v2.0 | Hypertext Transfer Protocol version 2.0 | Khuyến nghị áp dụng |
| 1.2 | Truyền tệp tin | FTP | File Transfer Protocol | Bắt buộc áp dụng một hoặc cả hai tiêu chuẩn |
| HTTP v1.1 | Hypertext Transfer Protocol version 1.1 |
| HTTP v2.0 | Hypertext Transfer Protocol version 2.0 | Khuyến nghị áp dụng |
| WebDAV | Web-based Distributed Authoring and Versioning | Khuyến nghị áp dụng |
| 1.3 | Truy cập thư mục | LDAP v3 | Lightweight Directory Access Protocol version 3 | Bắt buộc áp dụng |
| 1.4 | Dịch vụ Web dạng SOAP | SOAP v1.2 | Simple Object Access Protocol version 1.2 | Bắt buộc áp dụng một, hai hoặc cả ba tiêu chuẩn |
| WSDL V2.0 | Web Services Description Language version 2.0 |
| UDDI v3 | Universal Description, Discovery and Integration version 3 |
| 1.5 | Dịch vụ Web dạng RESTful | RESTful web service | Representational state transfer | Khuyến nghị áp dụng |
| 1.6 | Dịch vụ đặc tả Web | WS BPEL v2.0 | Web Services Business Process Execution Language Version 2.0 | Khuyến nghị áp dụng |
| WS-I Simple SOAP Binding Profile Version 1.0 | Simple SOAP Binding Profile Version 1.0 | Khuyến nghị áp dụng |
| WS- Federation v1.2 | Web Services Federation Language Version 1.2 | Khuyến nghị áp dụng |
| WS- Addressing v1.0 | Web Services Addressing 1.0 | Khuyến nghị áp dụng |
| WS-Coordination Version 1.2 | Web Services Coordination Version 1.2 | Khuyến nghị áp dụng |
| WS-Policy v1.2 | Web Services Coordination Version 1.2 | Khuyến nghị áp dụng |
| OASIS Web Services Business Activity Version 1.2 | Web Services Business Activity Version 1.2 | Khuyến nghị áp dụng |
| WS- Discovery Version 1.1 | Web Services Dynamic Discovery Version 1.1 | Khuyến nghị áp dụng |
| WS- MetadataExc hange | Web Services Metadata Exchange | Khuyến nghị áp dụng |
| **2** | **Tiêu chuẩn về tích hợp dữ liệu** | | | |
| 2.1 | Ngôn ngữ định dạng văn bản | XML v1.0 (5th Edition) | Extensible Markup Language version 1.0 (5th Edition) | Bắt buộc áp dụng một trong hai tiêu chuẩn |
| XML v1.1 (2nd Edition) | Extensible Markup Language version 1.1 |
| 2.2 | Ngôn ngữ định dạng văn bản cho giao dịch điện tử | ISO/TS 15000:2014 | Electronic Business Extensible Markup Language (ebXML) | Bắt buộc áp dụng |
| 2.3 | Định nghĩa các lược đồ trong tài liệu XML | XML Schema V1.1 | XML Schema version 1.1 | Bắt buộc áp dụng |
| 2.4 | Biến đổi dữ liệu | XSL | Extensible Stylesheet Language | Bắt buộc áp dụng phiên bản mới nhất. |
| 2.5 | Mô hình hóa đối tượng | UML v2.5 | Unified Modelling Language version 2.5 | Khuyến nghị áp dụng |
| 2.6 | Mô tả tài nguyên dữ liệu | RDF | Resource Description Framework | Khuyến nghị áp dụng |
| OWL | Web Ontology Language | Khuyến nghị áp dụng |
| 2.7 | Trình diễn bộ kí tự | UTF-8 | 8-bit Universal Character Set (UES)/Unicode Transformation Format | Bắt buộc áp dụng |
| 2.8 | Trao đổi dữ liệu đặc tả tài liệu XML | XMI v2.4.2 | XML Metadata Interchange version 2.4.2 | Khuyến nghị áp dụng |
| 2.9 | Định dạng trao đổi dữ liệu mô tả đối tượng dạng kịch bản JavaScript | JSON RFC 7159 | JavaScript Object Notation | Khuyến nghị áp dụng |
| 2.10 | Ngôn ngữ mô hình quy trình nghiệp vụ | BPMN 2.0 | Business Process Model and Notation version 2.0 | Khuyến nghị áp dụng |
| **3** | **Tiêu chuẩn về truy cập thông tin** | | | |
| 3.1 | Chuẩn nội dung Web | HTML v4.01 | Hypertext Markup Language version 4.01 | Bắt buộc, áp dụng |
| WCAG 2.0 | W3C Web Content Accessibility Guidelines (WCAG) 2.0 | Khuyến nghị áp dụng |
| HTML 5 | Hypertext Markup Language version 5 | Khuyến nghị áp dụng |
| 3.2 | Chuẩn nội dung Web mở rộng | XHTML v1.1 | Extensible Hypertext Markup Language version 1.1 | Bắt buộc áp dụng |
| 3.3 | Giao diện người dùng | CSS2 | Cascading Style Sheets Language Level 2 | Bắt buộc áp dụng một trong ba tiêu chuẩn |
| CSS3 | Cascading Style Sheets Language Level 3 |
| XSL | Extensible Stylesheet Language version |
| 3.4 | Văn bản | (.txt) | Định dạng Plain Text (.txt): Dành cho các tài liệu cơ bản không có cấu trúc | Bắt buộc áp dụng |
| (.rtf) v1.8, v1.9.1 | Định dạng Rich Text (.rtf) phiên bản 1.8, 1.9.1: Dành cho các tài liệu có thể trao đổi giữa các nền khác nhau | Bắt buộc áp dụng |
| (.docx) | Định dạng văn bản Word mở rộng của Microsoft (.docx) | Khuyến nghị áp dụng |
| (.pdf) v1.4, v1.5, v1.6, v1.7 | Định dạng Portable Document (.pdf) phiên bản 1.4, 1.5, 1.6, 1.7: Dành cho các tài liệu chỉ đọc | Bắt buộc áp dụng một, hai hoặc cả ba tiêu chuẩn |
| (.doc) | Định dạng văn bản Word của Microsoft (.doc) |
| (.odt) v1.2 | Định dạng Open Document Text (.odt) phiên bản 1.2 |
| 3.5 | Bộ ký tự và mã hóa | ASCII | American Standard Code for Information Interchange | Bắt buộc áp dụng |
| 3.6 | Bộ ký tự và mã hóa cho tiếng Việt | TCVN 6909:2001 | TCVN 6909:2001 “Công nghệ thông tin - Bộ mã ký tự tiếng Việt 16-bit” | Bắt buộc áp dụng |
| 3.7 | Chuẩn kết nối ứng dụng cổng thông tin điện tử | JSR 168 | Java Specification Requests 168 (Portlet Specification) | Bắt buộc áp dụng |
| JSR286 | Java Specification Requests 286 (Portlet Specification) | Khuyến nghị áp dụng |
| WSRP v1.0 | Web Services for Remote Portlets version 1.0 | Bắt buộc áp dụng |
| WSRP v2.0 | Web Services for Remote Portlets version 2.0 | Khuyến nghị áp dụng |
| **4** | **Tiêu chuẩn về an toàn thông tin** | | | |
| 4.1 | An toàn truyền tệp tin | HTTPS | Hypertext Transfer Protocol Secure | Bắt buộc áp dụng |
| FTPS | File Transfer Protocol Secure | Khuyến nghị áp dụng |
| SFTP | SSH File Transfer Protocol | Khuyến nghị áp dụng |
| 4.2 | Giải thuật chữ ký số | PKCS #1 V2.2 | RSA Cryptography Standard - version 2.2 | Bắt buộc áp dụng, sử dụng lược đồ RSASSA-PSS để ký |
| ECDSA | Elliptic Curve Digital Signature Algorithm | Khuyến nghị áp dụng |
| 4.3 | Giải thuật băm cho chữ ký số | SHA-2 | Secure Hash Algorithms-2 | Khuyến nghị áp dụng |
| 4.4 | An toàn trao đổi bản tin XML | XML Encryption Syntax and Processing | XML Encryption Syntax and Processing | Bắt buộc áp dụng |
| XML Signature Syntax and Processing | XML Signature Syntax and Processing | Bắt buộc áp dụng |
| 4.5 | Quản lý khóa công khai bản tin XML | XKMS v2.0 | XML Key Management Specification version 2.0 | Khuyến nghị áp dụng |
| 4.6 | Hạ tầng khóa công khai | | | Khuyến nghị áp dụng |
| Cú pháp thông điệp mật mã cho ký, mã hóa | PKCS#7 v1.5 (RFC 2315) | Cryptographic message syntax for file-based signing and encrypting version 1.5 |  |
| Cú pháp thông tin thẻ mật mã | PKCS#15 v1.1 | Cryptographic token information syntax version 1.1 |
| Cú pháp thông tin khóa riêng | PKCS#8 V1.2 (RFC 5958) | Private-Key Information Syntax Standard version 1.2 |
| Giao diện thẻ mật mã | PKCS#11 v2.20 | Cryptographic token interface standard version 2.20 |
| Cú pháp trao đổi thông tin cá nhân | PKCS#12 v1.1 | Personal Information Exchange Syntax version 1.1 |
| Khuôn dạng danh sách chứng thư số thu hồi | RFC 5280 | Certificate Revocation List Profile |
| Khuôn dạng chứng thư số | RFC 5280 | Public Key Infrastructure Certificate |
| Cú pháp yêu cầu chứng thực | PKCS#10 v1.7 (RFC 2986) | Certification Request Syntax Specification version 1.7 |
| Giao thức trạng thái chứng thư trực tuyến | RFC 6960 | On-line Certificate status protocol |
| Giao thức gắn tem thời gian | RFC 3161 | Time stamping protocol |
| Dịch vụ tem thời gian | ISO/EEC 18014-1:2008  ISO/EEC 18014-2:2009  ISO/EEC 18014-3:2009  ISO/EEC 18014-4:2015 | Information technology Security techniques - Time stamping services  Part 1: Framework  Part 2: Mechanisms producing independent tokens  Part 3: Mechanisms producing linked tokens  Part 4: Traceability of time sources |

### 1.2. Các tiêu chuẩn khác

Hệ thống đảm bảo tuân thủ các tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin theo các tiêu chuẩn khác như sau:

* Nghị định số 85/2016/NĐ-CP ngày 0/07/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Tiêu chuẩn TCVN 11930:2017 yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ;
* Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ;
* Thông tư số 24/2011/TT-BTTTT ngày 20/09/2011 quy định về việc tạo lập, sử dụng và lưu trữ dữ liệu đặc tả trên trang thông tin điện tử hoặc cổng thông tin điện tử của cơ quan nhà nước.
* Thông tư số 22/2023/TT-BTTTT ngày 31/12/2023 quy định cấu trúc, bố cục, yêu cầu kỹ thuật cho cổng thông tin điện tử và trang thông tin điện tử của cơ quan nhà nước
* Thông tư số 13/2017/TT-BTTTT ngày 23/6/2017 của Bộ Thông tin và Truyền thông quy định các yêu cầu kỹ thuật về kết nối các hệ thống thông tin, cơ sở dữ liệu với cơ sở dữ liệu quốc gia
* Quyết định 742/QĐ-BTTTT ngày 22/04/2022 của Bộ Thông tin và Truyền thông ban hành Yêu cầu an toàn cơ bản đối với Phần mềm nội bộ.
* Thông tư 26/2020/TT-BTTTT quy định việc áp dụng tiêu chuẩn, công nghệ hỗ trợ người khuyết tật tiếp cận, sử dụng sản phẩm, dịch vụ thông tin và truyền thông.

### 1.3. Yêu cầu chức năng tối thiểu của Hệ thống hỗ trợ săn tìm mối nguy cơ

#### 1.3.1. Yêu cầu về chức năng đối với phần mềm

|  |  |  |
| --- | --- | --- |
| **STT** | **TÊN CHỨC NĂNG** | **MÔ TẢ** |
| 1 | Đối chiếu và phân loại cảnh báo | Trích xuất thông tin quan trọng từ dữ liệu thu thập được |
| So khớp dữ liệu thu thập được với cơ sở dữ liệu địa chỉ máy chủ |
| Gán nhãn cho dữ liệu dựa trên kết quả so sánh |
| Hiển thị cảnh báo |
| 2 | Sao lưu dữ liệu | Sao lưu dữ liệu định kỳ |
| Xuất file sao lưu |
| Nhập dữ liệu từ file sao lưu |
| Tìm kiếm, trích xuất dữ liệu |
| 3 | Quản lý đăng nhập | Phân quyền người dùng |
| Quản lý cơ sở dữ liệu người dùng |
| Mã hóa dữ liệu đăng nhập |
| Quản lý phiên đăng nhập |
| 4 | Thu thập dữ liệu | Thiết lập kết nối tới máy chủ lưu trữ cơ sở dữ liệu FMS |
| Trích xuất dữ liệu |
| Khởi tạo bộ nhớ tạm để lưu trữ dữ liệu |
| Quản lý dữ liệu thu thập |
| 5 | Quản lý địa chỉ máy chủ | Thêm địa chỉ máy chủ |
| Sửa thông tin địa chỉ máy chủ |
| Xóa địa chỉ máy chủ |
| 6 | Trực quan hóa dữ liệu | Biểu diễn dữ liệu dưới dạng biểu đồ |
| Biểu diễn dữ liệu dưới dạng bảng |
| Biểu diễn tình trạng an toàn thông tin theo thời gian |
| 7 | Thống kê báo cáo | Thống kê theo nhóm hành vi |
| Thống kê theo khoảng thời gian |
| Thống kê theo từng máy tính |
| Thống kê theo từng đơn vị |
| Xuất báo cáo theo định dạng PDF/Excel |

#### 1.3.2. Yêu cầu phi chức năng

|  |  |
| --- | --- |
| **TT** | **YÊU CẦU** |
| 1 | Cho phép cài đặt trong hệ thống mạng có phân vùng bảo mật nhiều lớp. |
| 2 | Sẵn sàng hỗ trợ địa chỉ Internet thế hệ mới IPv6, DNSSEC. Triển khai HTTPS sử dụng giao thức TLS v1.2 trở lên với các bộ mã hóa an toàn trong xác thực người sử dụng và truyền nhận các thông tin nhạy cảm (thông tin cá nhân, thông tin thanh toán). |
| 3 | Các định dạng tập tin (tập tin nhập vào hệ thống, tập tin được xuất ra từ hệ thống, tập tin lưu trữ trong hồ sơ điện tử...) tuân thủ theo các định dạng tập tin (về văn bản, hình ảnh...) được quy định tại Thông tư số [39/2017/TT-BTTTT](https://thuvienphapluat.vn/van-ban/cong-nghe-thong-tin/thong-tu-39-2017-tt-btttt-tieu-chuan-ky-thuat-ve-ung-dung-cong-nghe-thong-tin-trong-co-quan-370857.aspx" \t "_blank) ngày 15/12/2017 của Bộ Thông tin và Truyền thông. |
| 4 | Chuẩn hóa dữ liệu để lưu trữ theo chuẩn ký tự Unicode. |
| 5 | Tương thích với các trình duyệt thông dụng hiện nay: Chrome, Firefox, Safari. |
| 6 | Hỗ trợ hiển thị tiếng Việt theo chuẩn Unicode. |
| 7 | Tuân thủ các quy định về chuẩn nội dung web theo Thông tư số [39/2017/TT-BTTTT](https://thuvienphapluat.vn/van-ban/cong-nghe-thong-tin/thong-tu-39-2017-tt-btttt-tieu-chuan-ky-thuat-ve-ung-dung-cong-nghe-thong-tin-trong-co-quan-370857.aspx" \t "_blank) ngày 15/12/2017 của Bộ Thông tin và Truyền thông. |
| 8 | Cho phép sử dụng chữ ký số cho các đối tượng trong hệ thống như người sử dụng, máy chủ. Sử dụng chữ ký số bảo đảm hoạt động được trên máy tính và các thiết bị cầm tay thông minh. |
| 9 | Cho phép xem trực tiếp trên trình duyệt các tệp đính kèm với một số định dạng phổ biến (ví dụ: .doc; .docx; .xls; .xlsx; .rtf, pdf). |
| 10 | Áp dụng tiêu chuẩn WCAG tối thiểu là phiên bản 2.0. |

#### 1.3.3. Yêu cầu về hiệu năng

Hệ thống phải đáp ứng các yêu cầu về hiệu năng như sau:

- Xử lý dữ liệu theo thời gian gần thực: Tính năng giám sát phải bảo đảm khả năng xử lý, phân tích dữ liệu log thu thập từ hệ thống FMS trong thời gian ngắn, phục vụ việc cảnh báo mối nguy kịp thời.

- Khả năng truy xuất dữ liệu nhanh chóng: Truy vấn dữ liệu trong cơ sở dữ liệu phải đảm bảo tốc độ phản hồi nhanh, đặc biệt là đối với các yêu cầu thống kê, lọc truy vấn phổ biến.

- Khả năng mở rộng: Thiết kế hệ thống theo hướng có thể mở rộng quy mô triển khai tại các đơn vị khác, đảm bảo hiệu năng vẫn ổn định khi khối lượng dữ liệu và người dùng tăng.

- Tối ưu sử dụng tài nguyên: Phần mềm cần tối ưu về bộ nhớ và CPU, phù hợp với môi trường mạng nội bộ quân sự, sử dụng thiết bị phần cứng hiện có mà không yêu cầu nâng cấp lớn.

## 2. Phân tích, lựa chọn phương án, giải pháp kỹ thuật, công nghệ

Phần mềm được xây dựng theo mô hình client-server, hoạt động trên nền tảng web, sử dụng các công nghệ:

- Ngôn ngữ lập trình: Python (Back-end), JavaScript/HTML/CSS (Front-end).

- Framework: Flask cho phía máy chủ (server-side), Bootstrap cho giao diện người dùng (UI).

- Kiến trúc hệ thống: Thiết kế hướng dịch vụ (modular), dễ dàng mở rộng và bảo trì.

Lựa chọn công nghệ này giúp đảm bảo hệ thống có hiệu năng tốt, dễ triển khai trong mạng nội bộ quân sự, đồng thời đáp ứng yêu cầu bảo mật, ổn định và tiết kiệm chi phí.

## 3. Phân tích, lựa chọn phương án, giải pháp kết nối, liên thông, chia sẻ dữ liệu với các hệ thống hạ tầng kỹ thuật, phần mềm, cơ sở dữ liệu liên quan

Dựa trên phân tích đặc thù nghiệp vụ, nhóm phát triển đề xuất sử dụng MongoDB – một hệ quản trị cơ sở dữ liệu NoSQL mạnh mẽ, có khả năng mở rộng cao và hiệu năng xử lý tốt. MongoDB lưu trữ dữ liệu dưới dạng tài liệu JSON (hoặc BSON), phù hợp với kiểu dữ liệu log thu thập từ hệ thống FMS, các chỉ số tấn công (IOC), mẫu mã độc, mối quan hệ giữa các đối tượng và kết quả phân tích.

Ngoài ra, MongoDB hỗ trợ khả năng **truy vấn linh hoạt, tích hợp tốt với ngôn ngữ lập trình Python**, phù hợp với kiến trúc back-end của hệ thống. Việc sử dụng MongoDB giúp giảm thiểu chi phí triển khai, đồng thời đảm bảo khả năng mở rộng quy mô dữ liệu và tích hợp với các giải pháp phân tích nâng cao trong tương lai, góp phần tăng cường hiệu quả nhiệm vụ giám sát và phòng thủ không gian mạng quân sự.

## 4. Thuyết minh giải pháp kỹ thuật, công nghệ

### 4.1. Tên phần mềm

Hệ thống hỗ trợ săn tìm mối nguy cơ

### 4.2. Các tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin theo quy định của Nhà nước

Hệ thống phải tuân thủ các tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin theo quy định của Nhà nước như sau:

* Nghị định số 85/2016/NĐ-CP ngày 0/07/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Tiêu chuẩn TCVN 11930:2017 yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ;
* Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ;
* Tuân thủ tiêu chuẩn kết nối, tiêu chuẩn về tích hợp dữ liệu, tiêu chuẩn về truy cập thông tin, tiêu chuẩn về an toàn thông tin, tiêu chuẩn về dữ liệu đặc tả được công bố kèm theo Danh mục tiêu chuẩn về ứng dụng CNTT trong cơ quan nhà nước được ban hành theo Thông tư số 39/2017/TT-BTTTT ngày 15/12/2017 của Bộ trưởng Bộ Thông tin và Truyền thông.
* Thông tư số 24/2011/TT-BTTTT ngày 20/09/2011 quy định về việc tạo lập, sử dụng và lưu trữ dữ liệu đặc tả trên trang thông tin điện tử hoặc cổng thông tin điện tử của cơ quan nhà nước.
* Thông tư số 22/2023/TT-BTTTT ngày 31/12/2023 quy định cấu trúc, bố cục, yêu cầu kỹ thuật cho cổng thông tin điện tử và trang thông tin điện tử của cơ quan nhà nước
* Thông tư số 13/2017/TT-BTTTT ngày 23/6/2017 của Bộ Thông tin và Truyền thông quy định các yêu cầu kỹ thuật về kết nối các hệ thống thông tin, cơ sở dữ liệu với cơ sở dữ liệu quốc gia
* Quyết định 742/QĐ-BTTTT ngày 22/04/2022 của Bộ Thông tin và Truyền thông ban hành Yêu cầu an toàn cơ bản đối với Phần mềm nội bộ.

### 4.3. Các yêu cầu chung về Hệ thống hỗ trợ săn tìm mối nguy cơ

Hệ thống phần mềm được xây dựng nhằm phục vụ nhiệm vụ chuyên biệt trong quân đội, do đó cần đảm bảo các yêu cầu chung sau:

- Phù hợp với môi trường mạng nội bộ quân sự, bảo đảm hoạt động ổn định, liên tục trong điều kiện không có kết nối internet và có phân vùng bảo mật cao.

- Giao diện thân thiện, dễ sử dụng, phù hợp với cán bộ kỹ thuật trong đơn vị. Bố cục các chức năng rõ ràng, dễ thao tác, hỗ trợ tìm kiếm, lọc và truy xuất dữ liệu nhanh chóng.

- Hiệu năng cao, xử lý tốt các khối lượng dữ liệu log lớn từ hệ thống FMS, hỗ trợ trực quan hóa các truy vấn và cảnh báo mối nguy một cách kịp thời.

- Tính bảo mật cao: Hệ thống yêu cầu xác thực người dùng bằng mật khẩu, có cơ chế phân quyền rõ ràng giữa quản trị viên và người dùng thường. Mật khẩu được mã hóa lưu trữ dưới dạng băm (hash), đảm bảo an toàn thông tin.

- Dễ triển khai và bảo trì: Hệ thống hoạt động độc lập, gọn nhẹ, không yêu cầu hạ tầng phức tạp. Có thể triển khai trên máy chủ hiện có của đơn vị. Việc cập nhật phần mềm, sao lưu và phục hồi dữ liệu dễ dàng.

- Tính mở và khả năng tích hợp: Hệ thống thiết kế mở, dễ tích hợp với các hệ thống giám sát, phân tích mã độc hoặc nền tảng threat intelligence khác trong tương lai.

- Tuân thủ các tiêu chuẩn kỹ thuật trong lĩnh vực an toàn thông tin, dữ liệu và phần mềm nội bộ theo quy định hiện hành của Bộ Thông tin và Truyền thông, Bộ Quốc phòng và các văn bản pháp luật liên quan.

### 4.4. Thiết kế giao diện Hệ thống hỗ trợ săn tìm mối nguy cơ

Giao diện hệ thống được thiết kế theo hướng đơn giản, rõ ràng, tập trung vào tính tiện dụng và tối ưu thao tác cho cán bộ kỹ thuật trong quá trình thực hiện nhiệm vụ giám sát và săn tìm mối nguy cơ mạng.

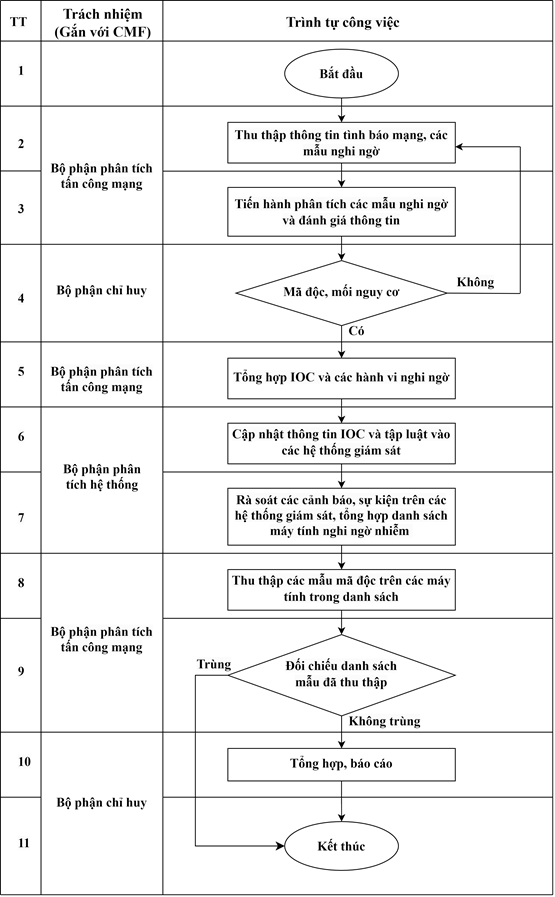
Thiết kế giao diện web hiện đại, dễ sử dụng, sử dụng khung giao diện Bootstrap, hỗ trợ tùy biến linh hoạt và tương thích tốt trên các trình duyệt hiện đại như Chrome, Firefox, Edge.

Bố cục chức năng được phân vùng rõ ràng, hiển thị theo thanh điều hướng ngang hoặc dọc, bao gồm các mục chính như: Giám sát – Cơ sở dữ liệu – Quản lý người dùng –Trang chủ– Trực quan hóa.

Màu sắc giao diện sử dụng tông màu trắng sáng, chuyên nghiệp, phù hợp môi trường quân sự và hạn chế gây mỏi mắt khi làm việc kéo dài. Các thành phần được bố trí có khoảng cách rõ ràng, dễ thao tác, tránh nhầm lẫn.

### 4.5. Các quy trình nghiệp vụ cần được tin học hóa

Hiện nay, lực lượng tác chiến mạng đang tiến hành các hoạt động săn tìm mối nguy cơ trên các hệ thống giám sát tập trung, nổi bật là FMS. Đây là hệ thống hỗ trợ mạnh mẽ cho nhiệm vụ săn tìm mối nguy cơ với tính năng thống kê, giám sát chặt chẽ các hoạt động, truy vấn bất thường từ máy tính, máy chủ trong mạng. Mặc dù rất hữu ích trong nhiệm vụ săn tìm mối nguy cơ, tuy nhiên các tính năng lại hỗ trợ gián tiếp và chưa thực sự rõ nét. Hệ thống chỉ mang tính cảnh báo, thông báo các hành vi, hoạt động đáng ngờ, các truy vấn của máy tính đến các địa chỉ, IP độc hại. Chưa hỗ trợ nhiều trong phân tích, xác định chiến dịch tấn công, thống kê và trực quan hóa các hành vi đáng ngờ của máy tính trong mạng. Các nhiệm vụ săn tìm, phát hiện mối nguy cơ vẫn đang tiêu tốn rất nhiều sức lực, nhân lực, chưa thể có một cái nhìn nhanh chóng và tổng quan đối với các hạ tầng mạng mà đơn vị giám sát, quản lý.

****

*Quy trình săn tìm mối nguy cơ*

Từ quy trình săn tìm mối nguy cơ của lực lượng tác chiến mạng, ứng dụng CNTT vào quá trình thực hiện nhiệm vụ:

| **TT** | **Hoạt động** | **Trách nhiệm** | **Mô tả** | **Ứng dụng CNTT** |
| --- | --- | --- | --- | --- |
|  |  |  | Bắt đầu công tác săn tìm các mối nguy cơ trong mạng MTQS thường xuyên. |  |
| B1 | Thu thập thông tin các mẫu nghi ngờ | Bộ phận giám sát, phòng thủ | - Giám sát hoạt động của các máy tính trong mạng MTQS.  - Phát hiện và điều ra các hoạt động bất thường của các máy tính trong mạng MTQS.  - Liên hệ thu thập các thông tin liên quan đến mẫu nghi ngờ kết hợp với công tác kiểm tra ATTT tại các cơ quan, đơn vị. | Tự động rà soát, thu thập hành vi bất thường của các máy tính trong mạng MTQS |
| B2 | Phân tích các mẫu nghi ngờ và đánh giá thông tin | - Phân tích các mẫu nghi ngờ sử dụng công cụ kiểm tra ATTT và phân tích mã độc.  - Phân tích, so sánh (địa chỉ máy chủ độc hại, hành vi) với các mẫu mã độc có trong CSDL.  - Kiểm tra các truy vấn lạ trên hệ thống Virustotal. | Tự động đối chiếu, so sánh các truy vấn nghi ngờ với CSDL |
| B3 | Xác định mối nguy cơ | Bộ phận  chỉ huy | Đánh giá kết quả, xác định mối nguy cơ:  - Có: Chuyển sang bước 4.  - Không: Quay lại bước 1. | Gán nhãn các truy vấn là lành tính, nguy cơ |
| B4 | Tổng hợp  kết quả phân tích | Bộ phận giám sát, phòng thủ | - Tổng hợp địa chỉ máy chủ độc hại và các hành vi nghi ngờ.  - Xây dựng các tập luật dựa trên địa chỉ máy chủ độc hại và các hành vi nghi ngờ. |  |
| B5 | Cập nhật địa chỉ máy chủ động hại và tập luật | Bộ phận giám sát, phòng thủ | Cập nhật địa chỉ máy chủ độc hại và tập luật vào các hệ thống giám sát. | Tự động cập nhật tập luật, địa chỉ máy chủ độc hại vào CSDL |
| B6 | Rà soát, tổng hợp danh sách máy tính nghi nhiễm | - Tiến hành rà soát các cảnh báo và sự kiện dựa trên các thông tin đã cập nhật.  - Tổng hợp danh sách các máy tính có hành vi nghi ngờ nhiễm mã độc. | Tổng hợp các danh sách máy tính xuất hiện các cảnh báo |
| B7 | Tổng hợp báo cáo | Bộ phận  chỉ huy | Tổng hợp báo cáo phát hiện mẫu biến thể mã độc mới trong hệ thống. | Tổng hợp báo cáo theo mẫu |
| B8 | Kết thúc,  Phê duyệt báo cáo | Phê duyệt báo cáo, phát hành báo cáo khi đạt yêu cầu. |  |

### 4.6. Các yêu cầu phi chức năng

#### 4.6.1. Yêu cầu cần đáp ứng đối với cơ sở dữ liệu

* CSDL phải có chế độ backup tự động hoặc bằng tay. Kế hoạch backup tự động có thể định nghĩa được.
* CSDL phải cung cấp khả năng xử lý và lưu trữ dữ liệu lớn.
* Hệ quản trị CSDL cho phép giám sát hoạt động lâu dài, sử dụng giao diện công cụ GUI để dễ dàng thao tác.
* Hệ quản trị CSDL phải hỗ trợ ít nhất nền tảng Windows
* Hệ quản trị CSDL có hỗ trợ sự nhất quán khi đọc nhiều phiên bản.
* Hệ quản trị CSDL có hỗ trợ khả năng chẩn đoán về cả các hoạt động của cơ sở dữ liệu và khả năng phần cứng để cung cấp mối tương quan giữa việc sử dụng cơ sở dữ liệu và hiệu suất phần cứng.
* Hệ quản trị CSDL hỗ trợ cho mức độ truy vấn song song tự động.
* Hệ quản trị CSDL có cung cấp tính năng ghi nhật ký giao dịch, có thể cấu hình được.
* Các bảng mô tả dữ liệu bao gồm:

| **TT** | **TÊN BẢNG MỖ TẢ DỮ LIỆU** |
| --- | --- |
| 1 | Bảng User |
| 2 | Bảng Indicator |
| 3 | Bảng Log |
| 4 | Bảng Statistics |
| 5 | Bảng Chart |
| 6 | Bảng Campaign |
| 7 | Bảng Intrusion\_set |
| 8 | Bảng Malware |
| 9 | Bảng Relationship |

#### 4.6.2. Yêu cầu về an toàn thông tin đối với phần mềm

Đáp ứng yêu cầu về bảo đảm an toàn thông tin của hệ thống thông tin cấp độ 2 theo quy định tại khoản 2 điều 8 Nghị định 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ, Tiêu chuẩn TCVN 11930:2017 yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

Dựa trên việc xác định cấp độ an toàn của hệ thống thông tin đã nêu, Hệ thống Cổng thông tin điện tử của Viện Hàn lâm cần tuân thủ yêu cầu cơ bản đảm bảo an toàn thông tin đối với hệ thống thông tin cấp độ 2, quy định tại Phụ lục 2 - Thông tư số 03/2017/TT-BTTTT ngày 24/04/2017.

Các yêu cầu cơ bản đảm bảo an toàn hệ thống thông tin đối với hệ thống thông tin cấp độ 2 bao gồm:

**- Yêu cầu kỹ thuật:**

+ An toàn hạ tầng mạng:

*(i)* Có phân vùng hạ tầng mạng thành các vùng mạng khác nhau tùy theo yêu cầu, mục đích sử dụng;

*(ii)* Có phương án sử dụng thiết bị có chức năng tường lửa để ngăn chặn truy cập trái phép giữa các vùng mạng với mạng Internet;

*(iii)* Có cơ chế xác thực và mã hóa khi sử dụng mạng không dây (nếu có);

*(iv)* Có phương án xác thực tài khoản quản trị trên các thiết bị mạng quan trọng;

*(v)* Có phương án quản trị các thiết bị từ xa (nếu có) thông qua các giao thức hỗ trợ mã hóa;

+ An toàn máy chủ:

*(i)* Có sử dụng phần mềm phòng, chống mã độc trên máy chủ và có cơ chế tự động cập nhật phiên bản mới hoặc dấu hiệu nhận dạng mã độc mới cho phần mềm này;

*(ii)* Có cơ chế xác thực bằng mật khẩu bảo đảm độ phức tạp cần thiết, yêu cầu thay đổi mật khẩu định kỳ theo quy định của tổ chức và có cơ chế phòng chống dò quét mật khẩu; Các thông tin xác thực phải được lưu trữ trên hệ thống dưới dạng mã hóa;

*(iii)* Có phương án vô hiệu hóa các tài khoản mặc định hoặc không hoạt động trên hệ thống; vô hiệu hóa các dịch vụ, phần mềm không sử dụng trên máy chủ;

*(iv)* Có ghi nhật ký hệ thống đối với hoạt động truy cập, quản trị máy chủ;

*(v)* Có thiết lập cơ chế cập nhật bản vá điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ;

+ An toàn ứng dụng:

*(i)* Có thiết lập yêu cầu bảo đảm mật khẩu trên ứng dụng đủ độ phức tạp cần thiết để hạn chế tấn công dò quét mật khẩu; các thông tin xác thực phải được lưu trữ dưới dạng mã hóa;

*(ii)* Có thiết lập yêu cầu ghi nhật ký truy cập, lỗi phát sinh;

*(iii)* Không sử dụng kết nối mạng không mã hóa trong việc quản trị ứng dụng từ xa.

**- Yêu cầu quản lý:**

+ Chính sách chung:

*(i)* Có chính sách an toàn thông tin cho người sử dụng bao gồm các nội dung: chính sách truy cập và sử dụng mạng và tài nguyên trên Internet; truy cập và sử dụng ứng dụng;

*(ii)* Có chính sách an toàn thông tin cho người quản trị, vận hành hệ thống bao gồm nhưng không giới hạn bởi chính sách quản lý an toàn hạ tầng mạng, an toàn máy chủ, an toàn ứng dụng và an toàn dữ liệu;

+ Tổ chức, nhân sự: Có quy trình, thủ tục để cấp phát, loại bỏ tài khoản, quyền truy cập của cán bộ mới tham gia sử dụng hệ thống, cán bộ thay đổi nhiệm vụ hoặc cán bộ ngừng sử dụng hệ thống;

+ Quản lý thiết kế, xây dựng:

*(i)* Có tài liệu thiết kế, mô tả về các phương án bảo đảm an toàn hệ thống thông tin;

*(ii)* Có phương án kiểm tra, xác minh hệ thống được triển khai tuân thủ theo đúng tài liệu thiết kế và yêu cầu bảo đảm an toàn thông tin trước khi nghiệm thu, bàn giao;

*(iii)* Có hồ sơ cấp độ được thẩm định, phê duyệt bởi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin;

+ Quản lý vận hành:

*(i)* Có quy trình quản lý, vận hành hệ thống phù hợp yêu cầu kỹ thuật cơ bản; quản lý sự thay đổi, di chuyển hệ thống; kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống;

*(ii)* Có phương án ứng cứu sự cố trong tình huống xảy ra sự cố an toàn thông tin;

+ Kiểm tra, đánh giá và quản lý rủi ro:

*(i)* Có phương án định kỳ 02 năm hoặc đột xuất khi cần thiết thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin theo quy định của pháp luật;

*(ii)* Việc kiểm tra, đánh giá an toàn thông tin và đánh giá rủi ro phải do đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin thực hiện hoặc thuê ngoài thực hiện theo quy định của pháp luật.

#### 4.6.3. Các yêu cầu cần đáp ứng về thời gian xử lý, độ phức tạp xử lý của các phần mềm

Phần mềm hỗ trợ săn tìm mối nguy cơ trên mạng máy tính quân sự được xây dựng nhằm đảm bảo khả năng xử lý hiệu quả, nhanh chóng các tập dữ liệu lớn từ hệ thống FMS và các nguồn khác. Vì vậy, hệ thống phải đáp ứng các yêu cầu về thời gian và độ phức tạp xử lý như sau:

- Thời gian phản hồi: Hệ thống phải đảm bảo thời gian phản hồi không quá 2 giây đối với các truy vấn phổ biến như tìm kiếm truy vấn độc hại theo IP, lọc danh sách máy tính nghi nhiễm, hiển thị thống kê theo đơn vị.

- Xử lý dữ liệu theo lô (batch): Khi thực hiện phân tích, đối chiếu dữ liệu log theo lô từ FMS (tối thiểu 10.000 bản ghi), hệ thống cần hoàn tất việc phân loại và cảnh báo trong thời gian không quá 30 giây.

- Phân tích và gán nhãn: Thuật toán gán nhãn hành vi (nguy cơ/cảnh báo/lành tính) phải được tối ưu để xử lý trên tập dữ liệu lớn mà không gây gián đoạn hệ thống.

- Trực quan hóa dữ liệu: Các biểu đồ, bảng thống kê phải được hiển thị tức thời khi người dùng yêu cầu. Hệ thống cần tối ưu hóa xử lý để đảm bảo biểu diễn trực quan không vượt quá 3 giây với dữ liệu ở cấp cụm.

- Độ phức tạp xử lý: Hệ thống được thiết kế theo hướng phân tách luồng xử lý (asynchronous processing), giảm tải tài nguyên và tối ưu hiệu suất. Các tác vụ tính toán phức tạp như đối chiếu pattern, đánh giá mối quan hệ giữa các mẫu mã độc và chiến dịch APT được thực hiện nền (background process).

#### 6.4.4. Các yêu cầu về cài đặt, hạ tầng, đường truyền, an toàn vận hành, khai thác, sử dụng

- Hạ tầng phần cứng: Hệ thống phần mềm được thiết kế để triển khai và vận hành trên máy chủ nội bộ của đơn vị, sử dụng hệ điều hành mã Linux và không yêu cầu phần cứng chuyên dụng. Phần mềm hoạt động ổn định trong điều kiện cấu hình máy chủ hiện có tại Trung tâm 386 – BTL 86. Trước khi đưa vào vận hành chính thức, hệ thống sẽ được kiểm thử đầy đủ trên môi trường thực tế.

- Khả năng tích hợp: Hệ thống dễ dàng tích hợp với các hệ thống giám sát hiện có như FMS, hoặc các nền tảng threat intelligence nội bộ khác thông qua giao tiếp cơ sở dữ liệu hoặc API nội bộ.

- Đường truyền và môi trường vận hành: Phần mềm được cài đặt và vận hành hoàn toàn trong mạng nội bộ quân sự, không yêu cầu kết nối Internet, đảm bảo an toàn, bảo mật. Hệ thống tương thích với hạ tầng mạng LAN, các VLAN phân vùng bảo mật đang được áp dụng tại đơn vị.

- An toàn vận hành và khai thác: Hệ thống có cơ chế phân quyền người dùng rõ ràng, mã hóa dữ liệu quan trọng, bảo đảm không gây ảnh hưởng đến hệ thống chung. Việc vận hành được thực hiện bởi cán bộ chuyên trách của Trung tâm 386, có khả năng khai thác, bảo trì và xử lý sự cố trong quá trình sử dụng.

#### 4.6.5. Các ràng buộc đối với hệ thống gồm: ràng buộc môi trường, sự phụ thuộc vào hệ thống nền tảng

**a) Ràng buộc về môi trường phát triển và vận hành**

Hệ thống phần mềm được phát triển dưới dạng ứng dụng web, triển khai trên máy chủ nội bộ, hoạt động ổn định trong môi trường mạng LAN quân sự không kết nối Internet. Yêu cầu hệ thống vận hành tốt trong môi trường sử dụng các trình duyệt phổ biến như: Chrome (≥ phiên bản 61), Firefox (≥ phiên bản 60), Microsoft Edge (≥ phiên bản 16), Safari (≥ phiên bản 10.1).

**b) Ràng buộc về nền tảng công nghệ**

Hệ thống được xây dựng bằng ngôn ngữ lập trình **Python**, sử dụng **framework Flask** cho phía máy chủ và **Bootstrap** cho giao diện người dùng. Cơ sở dữ liệu sử dụng là **MongoDB**, hoạt động tốt trên các hệ điều hành mã nguồn mở như Ubuntu Server. Phần mềm không phụ thuộc vào nền tảng Windows hay các công nghệ độc quyền khác.

#### 4.6.6. Yêu cầu về tính sẵn sàng với IPv6

Đáp ứng yêu cầu quy định về tính sẵn sáng với Ipv6 tại Thông tư 39/2017/TT-BTTTT ngày 15 tháng 12 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông ban hành Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước.

#### 4.6.7. Yêu cầu về mức độ chịu sự sai hỏng đối với các lỗi cú pháp lập trình, lỗi logic trong xử lý dữ liệu, lỗi kiểm soát tính đúng đắn của dữ liệu đầu vào

* Hiển thị thông báo hoặc không cho nhập khi người dùng nhập dữ liệu không hợp lệ.
* Các ô nhập phải hiển thị dấu thông báo ô nhập là bắt buộc hoặc tùy chọn nhập dữ liệu cho người dùng.
* Các ô nhập cần có định dạng của dữ liệu nhập chuyên biệt ví dụ: Ô nhập ngày tháng, Ô nhập số...
* Thứ tự các ô nhập tuân theo đúng logic của văn bản cần nhập, người dùng hoàn toàn có thể sử dụng bàn phím (không cần chuột) để di chuyển tới các ô nhập này.
* Đối với các ô nhập có dữ liệu cố định như: Danh mục, Ngày tháng, Danh sách cụ thể... cần hỗ trợ hiện thị danh sách để người dùng chọn mà không cần nhập.
* Việc nhập dữ liệu trên hệ thống đảm bảo ràng buộc xử lý logic của chương trình
* Lỗi cú pháp:

+ Lỗi vi phạm khi đặt hoặc gọi tên biến và hàm: Thường xuất hiện trong lúc phát triển mã. Thông thường lập trình viên đọc lại các bảng tham chiếu về ngôn ngữ để tránh sai cú pháp mẫu (prototype) của hàm hoặc/và tránh dùng các ký tự đặc biệt bị cấm không cho dùng trong khi đặt tên.

+ Lập trình viên hạn chế định nghĩa cùng một tên cho nhiều hơn một đối tượng khác nhau và giá trị toàn cục và được hạn chế rất nhiều trong nhiều trường hợp chúng tạo thành lỗi ý nghĩa.

* Logic trong gán sai dữ liệu:

+ Run-time: Các lỗi này xảy ra khi chương trình đang hoạt động và thường xảy ra do dữ liệu truyền vào không hợp lệ hoặc do các biến môi trường không tồn tại. Các lỗi xử lý được thể hiện trên các câu lệnh rẽ nhánh tránh không để cho mã vi phạm các lỗi.

+ Dùng các câu lệnh xử lý các ngoại lệ để xử lý các lỗi do dữ liệu hoặc viết code.

+ Lập trình viên tránh dùng một dữ liệu có kiểu khác với kiểu của biến để gán cho biến đó một cách không chủ ý. Đối với các ngôn ngữ tĩnh hay có kiểu mạnh như Java thì lỗi này dễ tìm thấy và sớm được phát hiện trong khi lập trình.

+ Các lỗi biên được lập trình viên hạn chế khi viết mã, thể hiện qua việc chú ý đến các giá trị ở biên của các biến, các hàm

#### 4.6.8. Yêu cầu về mỹ thuật, kỹ thuật cần đạt được của các giao diện chương trình

* Giao diện với người sử dụng đầu cuối dựa trên nền tảng web, hỗ trợ người sử dụng cuối sử dụng thiết bị cầm tay thông minh (ví dụ: điện thoại thông minh, máy tính bảng...).
* Hệ thống sẽ cung cấp giao diện trực quan, dễ dùng, thân thiện với người sử dụng và phù hợp đối với các nhóm người sử dụng khác nhau.
* Hỗ trợ tối đa sử dụng các chức năng bằng bàn phím máy tính. Các biểu tượng và phím nóng phải được thống nhất trong toàn bộ ứng dụng;
* Dễ dàng tìm thấy dịch vụ: người sử dụng dễ dàng tìm được dịch vụ sau tối đa 03 lần bấm chuột từ trang chủ của cổng thông tin điện tử cung cấp dịch vụ công trực tuyến; dễ dàng tìm được dịch vụ bằng các công cụ tìm kiếm phổ biến. Các giao diện thiết kế một cách đơn giản nhưng hiệu quả cao về thao tác, hiển thị và xử lý hình ảnh nhanh, màu sắc không gây cảm giác nhàm chán cho người sử dụng và theo một chuẩn giao diện thống nhất.
* Hệ thống sẽ cho phép lưu trữ tất cả dữ liệu theo định dạng Unicode, chấp nhận tất cả các ký tự tiếng Việt có dấu.
* Giao diện màn hình, các thông báo lỗi và trợ giúp là ngôn ngữ tiếng Việt theo chuẩn TCVN 6909:2001 dựa trên bảng mã Unicode dựng sẵn (ISO 10646), với trợ giúp của các bộ gõ Unikey, Vietkey.
* Giao diện chương trình dùng các Font chuẩn của hệ thống như Arial hay Times News Romans. Người dùng không phải cài thêm bất cứ font chữ nào.
* Hiển thị ngày giờ theo dạng DD/MM/YYYY và hh:mm:ss và căn giữa.
* Các chức năng phần mềm được xây dựng với một cơ chế thông báo lỗi thân thiện và rõ ràng. Thông báo lỗi phải được Việt hóa tối đa, giúp cho người sử dụng biết được lý do gây ra lỗi để tránh lặp lại các trường hợp tương tự; báo lỗi xác định rõ ràng đâu là lỗi do người sử dụng gây ra và đâu là lỗi do hệ thống gây ra và chỉ ra hướng khắc phục.
* Các thông báo hướng dẫn rõ ràng, tường minh để người dùng có thể thực hiện hỏi đáp một cách dễ dàng.

#### 4.6.9. Các yêu cầu phi chức năng khác

* Yêu cầu về chuẩn tiếng Việt: Phần mềm phải hỗ trợ chuẩn ngôn ngữ Unicode (tiêu chuẩn TCVN 6909); hỗ trợ tiêu chuẩn Unicode về mặt lưu trữ dữ liệu, hỗ trợ nhiều bộ gõ khác nhau.
* Yêu cầu về hệ thống báo lỗi: Hệ thống cung cấp tính năng báo lỗi chi tiết đến từng tình huống; trong các thông báo lỗi nền tảng cũng cho phép xây dựng để đáp ứng cho phép liên kết đến hệ thống trợ giúp cho từng nội dung tương ứng.
* Hệ thống báo lỗi được phân cấp ở nhiều mức, đi từ mức ứng dụng cho đến mức hệ thống. Giúp quản trị hệ thống có thể cấu hình để nắm được thông báo lỗi ở các thành phần khác nhau, cũng như nhận các báo cáo thống kê về quản trị hệ thống.
* Yêu cầu về mỹ thuật, kỹ thuật cần đạt được của các giao diện:

+ Giao diện phải được thiết kế để phù hợp với nhiều độ phân giải màn hình khác nhau, phù hợp với chuẩn thiết kế giao diện, thể hiện được môi trường thân thiện cho người dùng khai thác, sử dụng thuận lợi.

+ Giao diện có thể hiển thị linh hoạt trên các loại tính để bàn, máy xách tay, máy điện thoại thông minh hoặc các máy tính bảng.

+ Có thể truy cập bình thường trên các trình duyệt (với mọi version) thông dụng hiện nay như: IE, Firefox, Chrome, Opera, ... mà không bị vỡ trang hay biến dạng bố cục thông tin trên trang.

+ Ngôn ngữ sử dụng: Phần mềm phải hỗ trợ chuẩn ngôn ngữ Unicode (tiêu chuẩn TCVN 6909); hỗ trợ tiêu chuẩn Unicode về mặt lưu trữ dữ liệu, hỗ trợ nhiều bộ gõ khác nhau.

### 4.7. Yêu cầu năng lực của cán bộ tham gia phát triển, nâng cấp, chỉnh sửa phần mềm

| **STT** | **Vị trí** | **Số lượng** | **Bậc kỹ sư** |
| --- | --- | --- | --- |
| 1 | Cán bộ kiểm thử + đào tạo | 1 | KS1 |
| 2 | Cán bộ triển khai | 1 | KS1 |
| 4 | Quản trị dự án | 1 | KS1 |

### 4.8. Yêu cầu về bảo hành phần mềm

Đơn vị triển khai cung cấp dịch vụ bảo hành miễn phí hạng mục phần mềm như sau:

* Thời gian bảo hành đối với phần mềm là 24 tháng kể từ ngày nghiệm thu bàn giao.

- Đơn vị triển khai nhiệm vụ phải có trách nhiệm bảo hành sản phẩm khi có bất kỳ một đơn vị thụ hưởng nào báo hệ thống có lỗi hoặc không đáp ứng yêu cầu và phải có trách nhiệm cập nhật bản vá lỗi cho tất cả các đơn vị thụ hưởng khác trong thời gian bảo hành. Một khi ứng dụng có sự điều chỉnh mã nguồn do khắc phục lỗi hoặc nâng cấp chức năng của phần mềm. Đơn vị triển khai phải bàn giao CD (2 bản có nội dung giống nhau) mã nguồn và các tài liệu có liên quan đến việc hiệu chỉnh phần mềm cho Chủ đầu tư.

- Thời gian xử lý lỗi tối đa không quá 03 ngày làm việc. Hình thức đơn vị vận hành thông báo phần mềm xuất hiện lỗi có thể bằng: văn bản, thư điện tử, điện thoại, …

### 4.9. Yêu cầu về đào tạo và chuyển giao công nghệ

#### 4.9.1. Đào tạo hướng dẫn sử dụng cho cán bộ

- Mục tiêu đào tạo: Nhằm giúp học viên là các cán bộ trực tiếp sử dụng hệ thống nắm vững các chức năng chính như: thu thập, phân tích log từ FMS, đối chiếu với cơ sở dữ liệu độc hại, trực quan hóa, thống kê, và xuất báo cáo. Đồng thời, học viên hiểu được vai trò vận hành – quản trị hệ thống trong quy trình nghiệp vụ săn tìm mối nguy cơ, xử lý các lỗi logic thường gặp, và khai thác phần mềm hiệu quả phục vụ tác chiến mạng.

- Hình thức đào tạo: Tổ chức theo hình thức kết hợp giữa lý thuyết và thực hành, trong đó thực hành chiếm phần lớn thời lượng. Học viên được hướng dẫn trực tiếp trên phần mềm thật, tại môi trường triển khai thực tế.

- Quy mô khóa đào tạo: 01 lớp học với số lượng khoảng 4–5 học viên/lớp, là cán bộ kỹ thuật thuộc Trung tâm 386 hoặc các đơn vị có liên quan.

- Thời gian đào tạo: 06h/lớp, thực hiện trong giai đoạn chuyển giao hệ thống. Nội dung bao gồm vận hành, quản trị hệ thống và xử lý tình huống thường gặp trong thực tế.

- Người tham gia: Cán bộ kỹ thuật trực tiếp làm nhiệm vụ giám sát, phân tích log và vận hành hệ thống tại đơn vị.

- Địa điểm đào tạo: Tại Trung tâm 386 – Bộ Tư lệnh 86, trên hạ tầng triển khai thực tế của đơn vị.

- Yêu cầu về giảng viên: Mỗi lớp đào tạo có 01 giảng viên chính và 01 trợ giảng, am hiểu hệ thống và trực tiếp tham gia quá trình phát triển phần mềm.

#### 4.9.2. Đào tạo hướng dẫn sử dụng cho cán bộ quản trị hệ thống

- Mục tiêu đào tạo: Giúp học viên nắm vững các chức năng quản trị hệ thống phần mềm, bao gồm: phân quyền người dùng, quản lý cơ sở dữ liệu (indicator, log, campaign...), thiết lập tham số hệ thống, sao lưu/phục hồi dữ liệu, kiểm soát truy cập và đảm bảo an toàn, bảo mật. Qua đó, cán bộ có thể tự tin vận hành, duy trì, xử lý sự cố và hỗ trợ khai thác hệ thống hiệu quả, lâu dài.

- Hình thức đào tạo: Đào tạo tập trung, kết hợp giữa lý thuyết và thực hành ngay trên hệ thống thực tế, với các tình huống mô phỏng sự cố thường gặp trong quá trình quản trị.

- Quy mô khóa đào tạo: Gồm 01 lớp với khoảng 03 học viên/lớp là cán bộ kỹ thuật quản trị tại đơn vị triển khai (Trung tâm 386 hoặc đơn vị được chuyển giao).

- Thời gian đào tạo: 01 ngày/lớp, tổ chức trong giai đoạn chuyển giao và đưa hệ thống vào sử dụng chính thức.

- Người tham gia: Cán bộ kỹ thuật, cán bộ phụ trách vận hành hệ thống và quản trị phần mềm tại đơn vị.

- Địa điểm đào tạo: Tại Trung tâm 386 – Bộ Tư lệnh 86, trên hạ tầng hệ thống đã triển khai thực tế.

- Yêu cầu về giảng viên: Mỗi lớp đào tạo có 01 giảng viên chính và 01 trợ giảng, là người trực tiếp tham gia phát triển và triển khai hệ thống, am hiểu đầy đủ về kỹ thuật, quản trị và vận hành phần mềm.

### 4.10. Yêu cầu về kiểm thử, vận hành thử

Trước khi triển khai vận hành chính thức Hệ thống, đơn vị phát triển phải phối hợp với Chủ đầu tư lập kế hoạch và thực hiện kiểm thử chất lượng, vận hành thử nghiệm phần mềm, đảm bảo phần mềm sau khi đưa vào sử dụng sẽ hoạt động an toàn, ổn định và hiệu quả theo đúng nhu cầu người dùng. Việc kiểm thử phải bao gồm các hạng mục sau:

- Kiểm thử chức năng: Đảm bảo tất cả các chức năng được thiết kế trong phần mềm hoạt động đúng như yêu cầu đặc tả.

- Kiểm thử tích hợp: Đánh giá khả năng tương tác và tích hợp giữa các module trong hệ thống và với các hệ thống liên quan như FMS, cơ sở dữ liệu log, indicator,...

- Kiểm thử bảo mật: Kiểm tra các điểm yếu bảo mật, đánh giá cơ chế phân quyền, xác thực, mã hóa dữ liệu, nhằm đảm bảo hệ thống đáp ứng yêu cầu an toàn thông tin trong môi trường mạng nội bộ quân sự.

- Kiểm thử hiệu năng: Đánh giá khả năng xử lý dữ liệu ở các mức tải khác nhau, bảo đảm phần mềm phản hồi nhanh, không xảy ra tình trạng treo, gián đoạn hoặc tiêu tốn quá nhiều tài nguyên.

Việc thực hiện kiểm thử, vận hành thử thiết bị, phần mềm đảm bảo tuân thủ theo các nội dung hướng dẫn tại Thông tư 24/2020/TT-BTTTT ngày 09/9/2020 của Bộ Thông tin và Truyền thông quy định về công tác triển khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng CNTT sử dụng nguồn vốn ngân sách nhà nước hoặc văn bản hướng dẫn tại thời điểm thực hiện.

# VII. PHƯƠNG ÁN TỔ CHỨC QUẢN LÝ, KHAI THÁC, SỬ DỤNG DỰ ÁN

* Trung tâm 386/Bộ Tư lệnh 86 là đơn vị chịu trách nhiệm quản lý, vận hành và trực tiếp khai thác, sử dụng dự án

# VIII. ĐÁNH GIÁ TÁC ĐỘNG MÔI TRƯỜNG VÀ GIẢI PHÁP BẢO VỆ MÔI TRƯỜNG

Dự án “Xây dựng hệ thống hỗ trợ săn tìm mối nguy cơ” có đặc thù là một dự án sử dụng công nghệ thông tin, bao gồm phần mềm nội bộ và phần mềm thương mại nên không có tác động hay ảnh hưởng xấu tới môi trường.

# IX. PHƯƠNG ÁN TỔNG THỂ ĐỀN BÙ, GIẢI PHÓNG MẶT BẰNG, TÁI ĐỊNH CƯ

Dự án “Xây dựng hệ thống hỗ trợ săn tìm mối nguy cơ” có đặc thù là một dự án sử dụng công nghệ thông tin vì vậy không ảnh hưởng tới công tác đền bù, giải phóng mặt bằng, tái định cư.

# X. DỰ KIẾN TIẾN ĐỘ THỰC HIỆN DỰ ÁN; CÁC MỐC THỜI GIAN CHÍNH THỰC HIỆN ĐẦU TƯ

Thời gian thực hiện: trong vòng 06 tháng kể từ ngày hợp đồng có hiệu lực

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nội dung công việc** | **T6** | **T7** | **T8** | **T9** | **T10** | **T11** |
| Xây dựng thuyết minh nhiệm vụ |  |  |  |  |  |  |
| Tổ chức xây dựng phần mềm |  |  |  |  |  |  |
| Thử nghiệm và hiệu chỉnh hệ thống |  |  |  |  |  |  |
| Phối hợp với các cơ quan, đơn vị giám định chất lượng, kiểm tra an ninh, ATTT phần mềm và thiết bị |  |  |  |  |  |  |
| Viết báo cáo tổng hợp kết quả thực hiện nhiệm vụ |  |  |  |  |  |  |

# XI. XÁC ĐỊNH TỔNG MỨC ĐẦU TƯ, CƠ CẤU NGUỒN VỐN, PHƯƠNG ÁN HUY ĐỘNG VỐN

* Tổng mức đầu tư: 800.000.000 (Bằng chữ: Năm trăm triệu đồng chẵn.)
* Cơ cấu nguồn vốn: Nguồn vốn ngân sách nhà nước
* Phương án huy động vốn: Từ kinh phí nghiệp vụ thường xuyên

# XII. XÁC ĐỊNH CHI PHÍ VẬN HÀNH, BẢO DƯỠNG, DUY TU, SỬA CHỮA LỚN TRONG GIAI ĐOẠN KHAI THÁC DỰ ÁN

Trong giai đoạn khai thác hệ thống, các chi phí phát sinh liên quan đến bảo dưỡng định kỳ, duy tu, sửa chữa nhỏ thuộc phạm vi hợp đồng phát triển phần mềm sẽ do đơn vị triển khai chịu trách nhiệm thực hiện, không làm phát sinh chi phí cho Trung tâm 386.

Đối với các hạng mục sửa chữa lớn, thay đổi kiến trúc hệ thống hoặc nâng cấp mở rộng vượt ngoài phạm vi bảo hành, đơn vị triển khai và Trung tâm 386 – Bộ Tư lệnh 86 sẽ phối hợp trao đổi, thống nhất phương án xử lý và xác định chi phí cụ thể. Khoản chi phí này sẽ do Chủ đầu tư phê duyệt và chi trả theo quy định.

Sau thời gian bảo hành miễn phí (24 tháng), căn cứ theo báo giá của các nhà cung cấp dịch vụ, Trung tâm 386 sẽ lựa chọn đơn vị phù hợp để thực hiện dịch vụ hỗ trợ kỹ thuật, bảo trì và vận hành hệ thống. Chi phí duy trì hệ thống sẽ được Trung tâm tổng hợp và đề xuất trong kế hoạch bảo trì, nâng cấp phần mềm của các giai đoạn đầu tư tiếp theo.

# XIII. TỔ CHỨC QUẢN LÝ DỰ ÁN, BAO GỒM XÁC ĐỊNH CHỦ ĐẦU TƯ, PHÂN TÍCH LỰA CHỌN HÌNH THỨC TỔ CHỨC QUẢN LÝ THỰC HIỆN DỰ ÁN, MỐI QUAN HỆ VÀ TRÁCH NHIỆM CỦA CÁC CHỦ THỂ LIÊN QUAN ĐẾN QUÁ TRÌNH THỰC HIỆN DỰ ÁN, TỔ CHỨC BỘ MÁY QUẢN LÝ KHAI THÁC DỰ ÁN

## 1. Chủ đầu tư

- Trung tâm 386 – Bộ Tư lệnh 86.

- Trụ sở: 39 Phan Tư, Mỹ An, Ngũ Hành Sơn, Đà Nẵng

## 2. Phân tích lựa chọn hình thức tổ chức quản lý thực hiện dự án

Căn cứ vào quy mô, tính chất chuyên môn đặc thù của nhiệm vụ cũng như năng lực tổ chức, triển khai của đơn vị, Bộ Tư lệnh 86 giao cho Trung tâm 386 là đơn vị trực tiếp tổ chức quản lý và thực hiện nhiệm vụ xây dựng Hệ thống hỗ trợ săn tìm mối nguy cơ trên mạng máy tính quân sự tại địa bàn miền Trung – Tây Nguyên.

**\* Tổ chức nhân sự tham gia dự án**

- Chỉ đạo chung

Đồng chí Thiếu tá Nguyễn Viết Học, Cụm trưởng Cụm 31.

- Nhóm thực hiện nhiệm vụ

+ Đại úy Nguyễn Đức Anh - Đội trưởng Đội 1, Cụm 31: Chủ nhiệm nhiệm vụ.

+ Trung úy Lê Thế Nhật - SQTCM Đội 1/Cụm 31: Thành viên.

+ Trung úy Mạnh Tuấn Đạt - SQTCM Đội 1/Cụm 31: Thành viên.

+ Thượng úy Ngô Thị Hòa - Trợ lý KHTH/Cụm 31: Thành viên.

# XIV. CÁC ĐỀ XUẤT, KIẾN NGHỊ

Trong quá trình thực hiện nhiệm vụ, kính đề nghị chỉ huy, lãnh đạo các cơ quan thường xuyên quan tâm, chỉ đạo cũng như tạo điều kiện thuận lợi về thời gian, thủ tục để bảo đảm triển khai tốt nhiệm vụ, đúng tiến độ và mục tiêu đã đề ra.

# XV. PHỤ LỤC: THUYẾT MINH DỰ TOÁN

## 1. Cơ sở lập dự toán chi tiết

- Thông tư số 03/2020/TT-BTTTT ngày 24/02/2020 của Bộ Thông tin và Truyền thông Quy định về lập đề cương và dự toán chi tiết đối với hoạt động ứng dụng công nghệ thông tin sử dụng kinh phí chi thường xuyên thuộc nguồn vốn ngân sách nhà nước;

- Hướng dẫn được ban hành kèm theo Quyết định số 671/BTTTT ngày 26/4/2024 của Bộ Thông tin và Truyền thông hướng dẫn xác định chi phí phát triển, nâng cấp phần mềm nội bộ;

- Hướng dẫn kèm Quyết định số 129/QĐ-BTTTT ngày 03/02/2021 của Bộ Thông tin và Truyền thông về xác định đơn giá nhân công trong quản lý chi phí đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.

- Kế hoạch số 2012/KH-BTL ngày 31/12/2023 của Bộ Tư lệnh 86 về triển khai xây dựng, thẩm định, xét duyệt các nhiệm vụ đề xuất triển khai theo Nghị quyết số 29/NQ-TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược Bảo vệ Tổ quốc trên không gian mạng năm 2024.

## 2. Dự toán chi tiết

### 2.1. Tổng hợp dự toán

*Đơn vị tính: đồng*

| **STT** | **Nội dung** | **Tổng dự toán** | **Ghi chú** |
| --- | --- | --- | --- |
| 1 | Chi phí xây dựng phần mềm nội bộ | 800.000.000 |  |
| **Tổng cộng:** | | **800.000.000** |  |

### 2.2. Dự toán chi tiết

*Đơn vị tính: đồng*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TT** | **Hạng mục** | **Diễn giải** | **Giá trị** | **Ghi chú** |
| **I** | **Tính điểm trường hợp sử dụng (Use-Case)** |  |  |  |
| 1 | Điểm Actor (TAW) |  | 3 |  |
| 2 | Điểm Use case (TBF) |  | 108 |  |
| 3 | Tính điểm UUCP | UUCP = TAW +TBF | 112 |  |
| 4 | Điểm hệ số KT-CN (TCF) | TCF = 0,6 + (0,01 x TFW) | 0.96 |  |
| 5 | Điểm hệ số môi trường (EF) | EF = 1,4 + (-0,03 x EFW) | 0.965 |  |
| 6 | Tính điểm AUCP | AUCP = UUCP x TCF x EF | 103.7568 |  |
| **II** | **Nội suy thời gian lao động (P)** | P: người/giờ/AUCP | 29.5 |  |
| **III** | **Giá trị nỗ lực thực tế I** | E = 10/6 x AUCP | 172.9280 |  |
| **IV** | **Mức lương lao động bình quân (H)** | H: người/giờ | 64,101 |  |
| **V** | **Giá trị phần mềm nội bộ (G)** | G = 1,4 x E x P x H | **457,807,302.389** |  |
| **VI** | **Chi phí chung I** | C = G x 65% | 297,574,746.553 |  |
| **VII** | **Thu nhập chịu thuế tính trước (TL)** | TL = (G+C) x 6% | 45,322,922.936 |  |
| **VIII** | **Chi phí phần mềm (GPM)** | GPM = G + C + TL | 800,704,971.878 |  |
|  | **TỔNG CỘNG (làm tròn)** | **GPM** | 800,000,000 |  |

## 3. Thuyết minh diễn giải chi tiết dự toán

### 3.1. Bảng danh sách tác nhân (Actors)

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên tác nhân** | **Mô tả tác nhân** | **Phân loại tác nhân** |
| 1 | Quản trị hệ thống | Quản lý và duy trì toàn bộ hệ thống, bao gồm việc cài đặt, cấu hình, và bảo trì phần cứng và phần mềm. | Phức tạp |
| 5 | Người dùng cuối | Người sử dụng các dịch vụ và tính năng trên hệ thống | Phức tạp |

### 3.2. Bảng danh sách các yêu cầu chức năng của phần mềm

| **TT** | **Mô tả yêu cầu** | **Phân loại** | **Ghi chú** |
| --- | --- | --- | --- |
| **1** | **Đối chiếu và phân loại cảnh báo** | **Trung bình** |  |
|  | Từ dữ liệu thu thập được, hệ thống tiến hành trích xuất các thông tin quan trọng. |  |  |
|  | Tiến hành so khớp dữ liệu thu thập được với cơ sở dữ liệu địa chỉ máy chủ. |  |  |
|  | Gán nhãn cho dữ liệu là độc hại hay lành tính dựa trên kết quả so sánh. |  |  |
|  | Hiển thị cảnh báo biểu thị kết quả đối chiếu và phân loại |  |  |
| **2** | **Sao lưu dữ liệu** | **Trung bình** |  |
|  | Theo định kỳ, dữ liệu sẽ được tiến hành sao lưu, và lưu trữ dưới định dạng khác để giải phóng dung lượng cho cơ sở dữ liệu. |  |  |
|  | Các dữ liệu, bản ghi được export thành file json và lưu trữ ngoại tuyến |  |  |
|  | Hệ thống cho phép người dùng import dữ liệu từ file json do hệ thống export ra. |  |  |
|  | Dữ liệu sau khi import sẽ được đồng bộ với dữ liệu hiện có trên hệ thống để tiện lợi hơn cho người dùng trong tìm kiếm, truy xuất thông tin. |  |  |
| **3** | **Quản lý đăng nhập** | **Trung bình** |  |
|  | Người dùng trên hệ thống sẽ được phân quyền để hạn chế truy cập các tính năng quan trọng của hệ thống. |  |  |
|  | Người quản trị có quyền quản lý người dùng. Có quyền thêm mới, xóa bỏ người dùng trên hệ thống. |  |  |
|  | Các thông tin quan trọng như mật khẩu, sẽ được mã hóa trước khi lưu trữ vào trong cơ sở dữ liệu. Đảm bảo an toàn, hạn chế tối đa nguy cơ lộ lọt thông tin, mật khẩu. |  |  |
|  | Mỗi phiên đăng nhập sẽ được duy trì trong một khoảng thời gian nhất định, nếu tần suất hoạt động của người dùng ít, hệ thống sẽ tự động đăng xuất để giảm thiểu nguy cơ mất ATTT. |  |  |
| **4** | **Thu thập dữ liệu** | **Trung bình** |  |
|  | Hệ thống thiết lập kết nối tới máy chủ lưu trữ cơ sở dữ liệu FMS để truy vấn dữ liệu. Với việc khởi tạo kết nối trực tiếp đến CSDL của FMS sẽ tốc độ xử lý tối ưu và độ trễ tối thiểu nhất. |  |  |
|  | Hệ thống tự động truy vấn và thu thập các cảnh báo trên FMS dựa trên các đầu mối đơn vị, các loại cảnh bảo. |  |  |
|  | Khởi tạo bộ nhớ tạm để lưu trữ dữ liệu, đảm bảo không lưu trữ quá nhiều dữ liệu vào cơ sở dữ liệu, tránh tình trạng quá tải, gây chậm trễ cho hệ thống trong |  |  |
|  | Dữ liệu sau khi thu thập và xử lý sơ bộ, sẽ được bổ sung các trường dữ liệu và lưu trữ vào cơ sở dữ liệu, phục vụ cho quá trình phân loại |  |  |
| **5** | **Quản lý địa chỉ máy chủ** | **Đơn giản** |  |
|  | Hệ thống cho phép người sử dụng có thể thêm địa chỉ máy chủ độc hại kèm các thông tin liên quan, linh hoạt trong mở rộng cơ sở dữ liệu để cập nhật mới nhất với tình hình ATTT trên thế giới. |  |  |
|  | Sửa thông tin địa chỉ máy chủ |  |  |
|  | Xóa địa chỉ máy chủ |  |  |
| **6** | **Trực quan hóa dữ liệu** | **Đơn giản** |  |
|  | Hệ thống cho phép biểu diễn dữ liệu dưới dạng biểu đồ, thân thiện cho người dùng trong quan sát. |  |  |
|  | Hệ thống cho phép biểu diễn dữ liệu dưới dạng bảng, thân thiện cho người dùng trong quan sát. |  |  |
|  | Biểu diễn tình trạng an toàn thông tin theo thời gian, cung cấp cái nhìn tổng quan nhất về tình hình ATTT trong đơn vị |  |  |
| **7** | **Thống kê báo cáo** | **Trung bình** |  |
|  | Hệ thống cho phép thống kê cảnh báo theo nhóm hành vi độc hại. |  |  |
|  | Hệ thống cho phép thống kê cảnh báo theo khoảng thời gian diễn ra các truy vấn, hành vi độc hại. |  |  |
|  | Hệ thống cho phép thống kê truy vấn, hành vi độc hại theo từng máy tính, hộ trợ tốt cho công tác điều tra, truy vết. |  |  |
|  | Hệ thống cho phép thống kê truy vấn, hành vi độc hại theo từng đơn vị, giúp người dùng dễ dàng đánh giá tình hình ATTT của từng đầu mối. |  |  |
|  | Hệ thống cho phép export báo cáo theo định dạng PDF/Excel. |  |  |

### 3.3. Bảng chuyển đổi yêu cầu chức năng sang trường hợp sử dụng (usecase)

| **TT** | **Tên Use-case** | **Tên tác nhân** | **Giao dịch**  **(Transaction)** | **Phân loại theo BMT** | **Phân loại theo độ phức tạp** |
| --- | --- | --- | --- | --- | --- |
| **1** | **Đối chiếu và phân loại cảnh báo** | **Hệ thống** | **Đối chiếu và phân loại cảnh báo** | **M** | **Trung bình** |
|  |  |  | Trích xuất thông tin quan trọng từ dữ liệu thu thập được. |  |  |
|  |  |  | So khớp dữ liệu thu thập được với cơ sở dữ liệu địa chỉ máy chủ. |  |  |
|  |  |  | Gán nhãn cho dữ liệu dựa trên kết quả so sánh. |  |  |
|  |  |  | Hiển thị cảnh báo. |  |  |
| **2** | **Sao lưu dữ liệu** | **Hệ thống** | **Sao lưu dữ liệu** | **M** | **Trung bình** |
|  |  |  | Sao lưu dữ liệu định kỳ |  |  |
|  |  |  | Xuất file sao lưu |  |  |
|  |  |  | Nhập dữ liệu từ file sao lưu |  |  |
|  |  |  | Tìm kiếm, trích xuất dữ liệu |  |  |
| **3** | **Quản lý đăng nhập** | **Hệ thống** | **Quản lý đăng nhập** | **M** | **Trung bình** |
|  |  |  | Phân quyền người dùng |  |  |
|  |  |  | Quản lý cơ sở dữ liệu người dùng. |  |  |
|  |  |  | Mã hóa dữ liệu đăng nhập. |  |  |
|  |  |  | Quản lý phiên đăng nhập. |  |  |
| 4 | Thu thập dữ liệu | Hệ thống | Thu thập dữ liệu | **M** | **Trung bình** |
|  |  |  | Thiết lập kết nối tới máy chủ lưu trữ cơ sở dữ liệu FMS. |  |  |
|  |  |  | Trích xuất dữ liệu |  |  |
|  |  |  | Khởi tạo bộ nhớ tạm để lưu trữ dữ liệu. |  |  |
|  |  |  | Quản lý dữ liệu thu thập. |  |  |
| **5** | **Quản lý địa chỉ máy chủ** | **Hệ thống** | **Quản lý địa chỉ máy chủ** | **M** | **Đơn giản** |
|  |  |  | Thêm địa chỉ máy chủ. |  |  |
|  |  |  | Sửa thông tin địa chỉ máy chủ |  |  |
|  |  |  | Xóa địa chỉ máy chủ |  |  |
| **6** | **Trực quan hóa dữ liệu** | **Hệ thống** | **Trực quan hóa dữ liệu** | **M** | **Đơn giản** |
|  |  |  | Biểu diễn dữ liệu dưới dạng biểu đồ. |  |  |
|  |  |  | Biểu diễn dữ liệu dưới dạng bảng. |  |  |
|  |  |  | Biểu diễn tình trạng an toàn thông tin theo thời gian. |  |  |
| **7** | **Thống kê báo cáo** | **Hệ thống** | **Thống kê báo cáo** | **M** | **Trung bình** |
|  |  |  | Thống kê theo nhóm hành vi. |  |  |
|  |  |  | Thống kê theo khoảng thời gian. |  |  |
|  |  |  | Thống kê theo từng máy tính. |  |  |
|  |  |  | Thống kê theo từng đơn vị. |  |  |
|  |  |  | Xuất báo cáo theo định dạng PDF/Excel. |  |  |

### 3.4. Bảng tính toán điểm các tác nhân (actors) tương tác, trao đổi thông tin với phần mềm

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Loại actor** | **Mô tả** | **Trọng số** | **Số tác nhân** | **Điểm của từng loại tác nhân** |
| 1 | Đơn giản (Simple actor) | Giao diện lập trình ứng dụng (API) | 1 | 0 | 0 |
| 2 | Trung bình (Average actor) | Giao diện dòng lệnh (CLI) hoặc giao diện thông qua một giao thức nào đó nhưng không phải giao diện lập trình ứng dụng (API) | 2 | 0 | 0 |
| 3 | Phức tạp (Complex actor) | Giao diện đồ họa người dùng (GUI) | 3 | 1 | 3 |
|  | **TAW = Tổng các Actors theo trọng số** |  |  |  | **3** |

### 3.5. Bảng tính toán điểm các trường hợp sử dụng

| **TT** | **Loại** | **Trọng số** | **Hệ số BMT** | **Số trường hợp sử dụng** | **Điểm của từng loại trường hợp sử dụng** |
| --- | --- | --- | --- | --- | --- |
| 1 | **B** |  |  |  |  |
|  | Đơn giản | 5 | 1 | 0 | 0 |
| Trung bình | 10 | 1 | 0 | 0 |
| Phức tạp | 15 | 1 | 0 | 0 |
| 2 | **M** |  |  |  |  |
|  | Đơn giản | 5 | 1,2 | 4 | 24 |
| Trung bình | 10 | 1,2 | 4 | 48 |
| Phức tạp | 15 | 1,2 | 2 | 36 |
| 3 | **T** |  |  |  |  |
|  | Đơn giản | 5 | 1,5 | 0 | 0 |
| Trung bình | 10 | 1,5 | 0 | 0 |
| Phức tạp | 15 | 1,5 | 0 | 0 |
|  | **Cộng 1+2+3** |  |  | **TBF** | **80** |

### 3.6. Bảng tính toán hệ số phức tạp kỹ thuật – công nghệ

| **TT** | **Các hệ số** | **Trọng số** | **Giá trị xếp hạng** | **Kết quả** | **Ghi chú** |
| --- | --- | --- | --- | --- | --- |
| **I** | **Hệ số KT-CN (TFW)** |  |  | **36** |  |
| 1 | Xử lý phân tán | 1 | 1 | 1 | Hệ thống xử lý tập trung tại máy chủ cài đặt Cổng TTĐT của Viện |
| 2 | Mức độ quan trọng của hiệu năng | 1 | 3 | 3 | Yêu cầu cụ thể hiệu năng trong toàn bộ thời gian tác nghiệp |
| 3 | Hiệu quả sử dụng cho người dùng | 1 | 2 | 2 | Yêu cầu hệ thống đáp ứng các tiêu chí: 1. Trợ giúp điều hướng (ví dụ: các menu được tạo động và thêm bớt tùy nhu cầu người dùng, Hypermedia thích hợp,…).; 2. Các phím chức năng được cài đặt sẵn (các phím tắt được gán cho các phím hoặc tổ hợp phím cho phép thực hiện tác vụ nào đó, như tổ hợp phím Alt+phím, Ctrl+phím,…); 3. Các ràng buộc đơn giản (ví dụ: tính hợp lệ của trường dữ liệu nhập vào, như dữ liệu kiểu số, dữ liệu ngày tháng,…) được kiểm tra ngay trên màn hình chức năng mà người dùng tương tác; 4. Tối thiểu hóa số lượng giao diện để đạt được các mục tiêu nghiệp vụ (yêu cầu cụ thể số lượng giao diện tối thiểu); |
| 4 | Độ phức tạp của xử lý bên trong | 2 | 4 | 8 | Yêu cầu hệ thống đáp ứng các tiêu chí: 1. Yêu cầu kiểm soát dữ liệu và/hoặc xử lý bảo mật riêng; 2. Yêu cầu xử lý lô-gic mở rộng: là các yêu cầu bổ sung thêm làm các chức năng hoàn thiện hơn; 3. Yêu cầu xử lý ngoại lệ cho những giao dịch không hoàn chỉnh phải được xử lý lại  4. Yêu cầu xử lý nhiều loại thông tin đầu vào hoặc thông tin đầu ra (hình ảnh, tệp tin) |
| 5 | Khả năng tái sử dụng mã nguồn | 1 | 1 | 1 | Yêu cầu ứng dụng phải được đóng gói riêng và/hoặc tài liệu hóa nhằm tạo điều kiện cho việc tái sử dụng lại. Có yêu cầu có thể tùy chỉnh ứng dụng để tái sử dụng bằng cách điều chỉnh mã nguồn. |
| 6 | Dễ cài đặt | 0,5 | 3 | 1,5 | Yêu cầu cung cấp công cụ hỗ trợ cài đặt tự động trên một môi trường vận hành phần mềm (hệ điều hành máy chủ, máy tính, thiết bị di động,…), có yêu cầu thiết lập thông số khi cài đặt và có yêu cầu phải xây dựng tài liệu hướng dẫn cài đặt. |
| 7 | Dễ vận hành | 2 | 2 | 4 | Việc vận hành hệ thống thực hiện theo quy trình, có yêu cầu phải lập quy trình vận hành hệ thống. |
| 8 | Khả năng chuyển đổi | 1 | 3 | 3 | Có yêu cầu hệ thống vận hành được trên môi trường phần mềm hoặc phần cứng tương tự nhau. |
| 9 | Dễ dàng bảo trì | 1 | 5 | 5 | Có yêu cầu về việc chỉnh sửa hệ thống trong tương lai mà không cần lập trình lại từ đầu. |
| 10 | Xử lý đồng thời | 1 | 3 | 3 | Yêu cầu truy cập dữ liệu đồng thời tại mọi thời điểm. |
| 11 | Mức độ hỗ trợ bảo mật | 0.5 | 3 | 1.5 | Yêu cầu bảo mật mức 2 |
| 12 | Sự phụ thuộc vào mã lệnh của bên thứ ba | 1 | 3 | 3 | Sử dụng mã lệnh sẵn có (không cần hiệu chỉnh) để phát triển một phần của ứng dụng. |
| 13 | Mức độ hỗ trợ đào tạo người sử dụng | 0.5 | 3 | 1.5 | Không có yêu cầu hỗ trợ của hệ thống về đào tạo người sử dụng. |
| **II** | **Hệ số độ phức tạp về CN-KT (TCF)** |  |  | **0,96** |  |

### 3.7. Bảng tính toán hệ số tác động môi trường và nhóm làm việc, hệ số phức tạp về môi trường, xác định độ ổn định kinh nghiệm và nội suy thời gian lao động

| **TT** | **Các hệ số tác động môi trường** | **Trọng số** | **Giá trị xếp hạng** | **Kết quả** | **Độ ổn định kinh nghiệm** | **Ghi chú** |
| --- | --- | --- | --- | --- | --- | --- |
| **I** | **Hệ số tác động môi trường và nhóm làm việc (EFW)** |  |  | **29** |  |  |
| 1 | Có áp dụng quy trình phát triển phần mềm | 1.5 | 3 | 4.5 | 1 | Yêu cầu ít nhất 50% thành viên nhóm phát triển có kinh nghiệm tham gia dự án có áp dụng quy trình phát triển phần mềm. |
| 2 | Kinh nghiệm phát triển ứng dụng tương tự | 0.5 | 3 | 1.5 | 0.1 | Yêu cầu ít nhất 50% thành viên nhóm phát triển có kinh nghiệm phát triển ứng dụng tương tự. |
| 3 | Kinh nghiệm về hướng đối tượng | 1 | 3 | 3 | 0.6 | Yêu cầu ít nhất 50% thành viên nhóm phát triển có kinh nghiệm về hướng đối tượng. |
| 4 | Kinh nghiệm của trưởng nhóm lập trình | 0.5 | 3 | 1.5 | 0.1 | Yêu cầu trưởng nhóm lập trình đã có kinh nghiệm làm trưởng nhóm lập trình 4 dự án/nhiệm vụ. |
| 5 | Tính chủ động | 1 | 3 | 3 | 0.6 | Không yêu cầu nhóm phát triển thực hiện báo cáo theo các mốc công việc/sản phẩm trong kế hoạch thực hiện. |
| 6 | Độ ổn định của các yêu cầu | 2 | 1 | 2 | 0.1 | Các yêu cầu hệ thống ổn định, trong giai đoạn xây dựng, phát triển, mở rộng phần mềm chỉ cho phép điều chỉnh giao diện về mặt mỹ thuật |
| 7 | Sử dụng các nhân viên làm bán thời gian | -1 | 0 | 0 | 0 | Không sử dụng nhân viên làm bán thời gian. |
| 8 | Kinh nghiệm sử dụng ngôn ngữ lập trình | -1 | 0 | 0 | 0 | Yêu cầu ít nhất 20% thành viên nhóm lập trình có kinh nghiệm lập trình. |
| **II** | **Hệ số độ phức tạp về môi trường (EF)** |  |  | **0.935** |  |  |
| **III** | **Độ ổn định kinh nghiệm (ES)** |  |  |  | **2.5** |  |
| **IV** | **Nội suy thời gian lao động (P)** |  |  |  | **29,5** |  |

### 3.8. Bảng tính toán chi phí trực tiếp xây dựng, phát triển, mở rộng phần mềm nội bộ

| **TT** | **Hạng mục** | **Diễn giải** | **Giá trị** |
| --- | --- | --- | --- |
| **I** | **Tính điểm trường hợp sử dụng (Use-case)** |  |  |
| 1 | Điểm Actor (TAW) |  | 3 |
| 2 | Điểm Use case (TBF) |  | 108 |
| 3 | Tính điểm UUCP | UUCP = TAW +TBF | 112 |
| 4 | Hệ số phức tạp về KT-CN (TCF) | TCF = 0,6 + (0,01 x TFW) | 0.96 |
| 5 | Hệ số phức tạp về môi trường (EF) | EF = 1,4 + (-0,03 x EFW) | 0.965 |
| 6 | Tính điểm AUCP | AUCP = UUCP \* TCF \* EF | 103.7568 |
| **II** | **Nội suy thời gian lao động (P)** | P = người/giờ/AUCP | 29.5 |
| **III** | **Giá trị nỗ lực thực tế (E)** | E = AUCP x 10/6 | 172.9280 |
| **IV** | **Mức lương lao động bình quân (H)** | H = người/giờ | 64,101 |
| **V** | **Chi phí trực tiếp xây dựng, phát triển, nâng cấp, mở rộng phần mềm nội bộ (G)** | G = 1,4 \* E \* P \* H | 457,807,302.389 |

### 3.9. Chi phí đầu tư xây dựng, phát triển hình thành dịch vụ công nghệ thông tin

| **TT** | **Khoản mục chi phí** | **Cách tính** | **Ký hiệu** | **Giá trị** |
| --- | --- | --- | --- | --- |
| 1 | Chi phí trực tiếp xây dựng, phát triển, nâng cấp mở rộng phần mềm nội bộ | G | G | **457,807,302.389** |
| 2 | Chi phí chung | G x 65% | C | 297,574,746.553 |
| 3 | Thu nhập chịu thuế tính trước | (G + C) x 6 % | TL | 45,322,922.936 |
| 4 | Chi phí xây dựng, phát triển, nâng cấp, mở rộng phần mềm nội bộ | G + C + TL | GPM | 800,704,971.878 |

### 3.10. Bảng diễn giải cách tính giờ công H

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TT** | **Tiêu chí xác định** | **Tỷ lệ/ hệ số xác định** | **Cấp bậc, hệ số, mức lương** | | | | | **Ghi chú** |
| 1 | Cấp bậc kỹ sư |  | Bậc 1 | Bậc 2 | Bậc 3 | Bậc 4 | Bậc 5 |  |
| 2 | Hệ số lương theo cấp bậc | HCB | 2,34 | 2,65 | 2,96 | 3,27 | 3,58 | *Quyết định số 129/QĐ-BTTTT ngày 03/02/2021 của Bộ TT&TT* |
| 3 | Hệ số phụ cấp lương | HPC | 0 | 0 | 0 | 0 | 0 |  |
| 4 | Mức lương cơ sở | MLCS | 2.340.000 | 2.340.000 | 2.340.000 | 2.340.000 | 2.340.000 | *Nghị định số 38/2019/NĐ-CP ngày 09/05/2019 của Chính phủ* |
| 5 | Lương cơ bản | LCB = (HCB + HPC)\*MLCS | 5.475.600 | 6.201.000 | 6.926.400 | 7.651.800 | 8.377.200 |  |
| 6 | Hệ số điều chỉnh tăng tiền lương | HĐC | 1,2 | 1,2 | 1,2 | 1,2 | 1,2 | *Vùng I Quyết định số 129/QĐ-BTTTT ngày 03/02/2021 của Bộ TT&TT* |
| 7 | Các khoản nộp theo lương (3% BHYT, 17.5% BHXH, 1% BHTN, 2% KPCĐ) | BHLĐ = 0,235\*LCB | 1.286.766 | 1.457.235 | 1.627.704 | 1.798.173 | 1.968.642 | *Nghị định số 58/2020/NĐ-CP, Quyết định số 595/QĐ-BHXH* |
| 8 | Đơn giá ngày công trực tiếp | GNC = (LCB \* (1+HĐC) + BHLĐ)/26 | 512.811 | 580.748 | 648.684 | 716.621 | 784.557 | *Thời gian lao động để tính mức lương lao động bình quân tháng là 26 ngày.* |
| 9 | Mức lương lao động/giờ | H = GNC/8 | 64.101 | 72.593 | 81.086 | 89.578 | 98.070 | *Thời gian lao động 08 giờ/ngày* |

#### 