МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
Минтранс России

Транспортный университет

Лаборатория безопасности ПО

Ожидаемые сроки исполнения: Два семестра (Февраль 2023 - Декабрь 2023)

Контекст

В какой области решаем проблему?

Кибербезопасность ПО, безопасность АСУТП, Безопасность информации (включая персональных данных), информационная безопасность, защита информации

Проблема

Что за проблема: кто пытается достичь какую цель и что мешает?

Начальник отдела информационной безопасности департамента критической инфраструктуры хочет получить отказоустойчивое и киберзащищенное программное обеспечение для реализации надежного управления объектами критической инфраструктуры, но не может, потому что используемый ранее софт уязвим для атак/закладок, альтернативные решения проприетарные и поставляются из недружественных стран.

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
Минтранс России

Транспортный университет

Пользователи

Чья это проблема? Кто хочет что-то получить, но не может?

Начальник отдела информационной безопасности департамента критической инфраструктуры

Заказчик и другие стейкхолдеры

Кто вовлечен (какие стейкхолдеры/целевые аудитории и их сегменты)?

Минтранс России, регуляторы в сфере обеспечения безопасности информации и ее защиты (ФСТЭК России, ФСБ России, Минцифры России и др.), организации, осуществляющие деятельность в сфере разработки программных средств защиты информации для транспортной отрасли

Данные

Какие есть (если есть) исходные данные для решения такой проблемы? Где их искать/собирать/парсить?

Нормативно-правовые акты по обеспечению безопасности информации (законы, ГОСТы, руководящие документы регуляторов и т.п.), средства анализа исходных текстов программ.

Рекомендуемые инструменты

Есть ли у заказчика предпочтения/рекомендации по инструментам/методам, которыми такие проблемы решают?

Целесообразно использовать методы безопасной разработки, развёртывания и технической поддержки ПО, ориентированные на контроль информационной безопасности на всех этапах жизненного цикла ПО, реагирования на новые угрозы и уязвимости ПО, использоваться высокопроизводительные ЭВМ.

Анализ аналогов

Какой вам известен мировой опыт в решении такого рода проблем?

SICA, ENISA

Предполагаемый тип решения

В каком направлении предлагаем участникам искать решения?

разработка стендового оборудования для исследования ПО, разработки По для АСУТП, реализация безопасного беспилотного транспорта

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
Минтранс России

Транспортный университет

Предполагаемая ролевая структура команды

Состав ролей участников команды. Возможные направления подготовки участников

архитектор, програмист, тестировщик, администратор

Доступная экспертиза

Какими экспертами мы обеспечим решение этой задачи

генеральный директор "Эшелон" Дорофеев А., менеджер по продажам "Лаборатория Касперского" Малыгин В., нач. учебного центра АО Астра LINUX Елена Гарбар

Дополнительные материалы

Ссылки на дополнительные материалы или дополнительная информация, которая позволит более полно раскрыть суть проекта

планируется на 2 года.

Возможный реализатор проекта

Какому институту/академии потенциально может быть интересен данный проект для реализации

ИТТСУ, ИУЦТ, ИЭФ, ЮИ