МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
Минтранс России

Транспортный университет

Способ повышения защиты информации от несанкционированного доступа с использованием дополнительных признаков при вводе пароля с клавиатуры

Ожидаемые сроки исполнения: Один семестр (Сентябрь 2023 - Декабрь 2023)

Контекст

В какой области решаем проблему?

Данный проект относится к информационным технологиям и защите информации.

Проблема

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

У кого возникает ограничение в его деятельности? Различные мошеннические схемы применяются для получения паролей пользователей социальных сетей, государственных порталов и банковских приложений. Получение пароля или иной информации неизбежно ведет к денежным и репутационным потерям. Проблема. Цель Чего хочет добиться Носитель проблемы, но не может? Какое целевое состояние? Надежная защита паролей и личной информации от несанкционированного доступа Проблема. Барьер Что мешает Носителю проблемы достичь цели? Ограниченный набор современных инструментов создания паролей при вводе с клавиатуры, позволяющих контролировать и бороться с мошенничествами для защиты конфиденциальной информации

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
Минтранс России

Транспортный университет

Пользователи

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

Заказчик и другие стейкхолдеры

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

Заказчиком выступит ООО ЖелдорЦТИ. Заинтересованными сторонами являются все пользователи социальных сетей, государственных и банковских порталов

Данные

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

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
Минтранс России

Транспортный университет

Рекомендуемые инструменты

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

Анализ аналогов

Какой вам известен мировой опыт в решении такого рода проблем?

Существующие способы сводятся к следующим: 1. Простые пароли, которые основаны на знакомых словах и словосочетаниях 2. Короткие пароли с малым количеством дополнительных символов 3. Пароли и парольные фразы, которые генерируются автоматически 4. Набор символов в виде пароля, предлагаемый системой регистрации Вышеперечисленные способы не могут гарантировать защиту от несанкционированного доступа к конфиденциальной или личной информации пользователя в полном объеме, т.к. либо слишком просты, либо основаны на информации связанной с пользователем. Пароли предлагаемые системой регистрации часто забываются или записываются людьми в ненадежных местах хранения, т.к. являются не ассоциируемым набором символов.

Предполагаемый тип решения

В каком направлении предлагаем участникам искать решения?

Информационный продукт, который позволит на новом уровне защитить от несанкционированного доступа конфиденциальную и личную информацию пользователя

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
Минтранс России

Транспортный университет

Предполагаемая ролевая структура команды

Состав ролей участников команды. Возможные направления подготовки участников

1 ЛИД+ 4 участника команды

Доступная экспертиза

Какими экспертами мы обеспечим решение этой задачи

Сотрудники ООО ЖелдорЦТИ

Дополнительные материалы

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

https://www.drivereasy.com/knowledge/random-password-generator-what-is-it-and-how-to-use-it/ https://www.keepersecurity.com/ru_RU/resources/glossary/what-is-a-passphrase/a>

Возможный реализатор проекта

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

АВИШ