– предоставление упорядоченного набора структурированной информации об автопарке, с возможностью ее изменения, поиск транспортного средства по заданным параметрам;

– составление маршрута, с возможностью его последующей корректировкой;

– реализована ролевая модель приложения, которая содержит в себе две сущности: клиент – оформление заказов после получения полной информации о предоставляемых услугах через информационную систему; администратор – проведение принятых заказов при помощи инструментов разработанного приложения;

– контроль за исполнением и информированием клиента о статусе перевозки груза;

– формирование отчетности и прочих финансовых, сопроводительных документов.

Программное средство написано с использованием возможностей клиент-серверной архитектуры. Таким образом, клиент-серверная структура позволяет осуществлять полный, удаленный контроль над работой транспортного предприятия. Ролевая модель позволяет осуществлять быстрое, информативное принятие и проведение заказов. А также возможность работы в режиме реально времени множеству пользователей системы, как с мобильного, так и с персонального устройства.

Литература

1 Клиент-серверная архитектура [Электронный ресурс]. – Режим доступа: https://qastart.by/. – Дата доступа: 10.02.2022.

А. О. Шульжицкий
(*ГрГУ им. Я. Купалы, Гродно*)

СИСТЕМА БЕЗОПАСНОЙ АУТЕНТИФИКАЦИИ СОТРУДНИКОВ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНОЙ МОДЕЛИ БЕЗОПАСНОСТИ RBA

Пароли были и остаются преобладающим механизмом аутентификации онлайн-сервисов. Однако угрозы аутентификации на основе паролей возрастают, например, из-за крупномасштабных утечек базы

данных паролей и подбора учетных данных. Поэтому операторы вебсайтов должны предоставлять дополнительные или альтернативные механизмы аутентификации для адекватной защиты своих пользователей [1].

Двухфакторная аутентификация (2FA) – это одна из таких мер, которая широко используется, но оказывается непопулярной среди пользователей. Биометрическая аутентификация считается нецелесообразной для крупных онлайн-сервисов, поскольку требует специального оборудования и активного участия пользователя. По этим причинам несколько крупных онлайн-сервисов используют аутентификацию на основе рисков (RBA) для защиты своих пользователей.

RBA – risk-based authentication, это адаптивная мера аутентификации, которая обеспечивает высокий уровень безопасности с минимальным влиянием на взаимодействие с пользователем и, таким образом, может быть более приемлемой для пользователей, чем двухфакторная аутентификация. Во время ввода пароля RBA отслеживает дополнительные источники, например, IP-адрес или пользовательский агент, а также использует запросы на повторную аутентификацию при обнаружении определенного риска. Кроме того, RBA рекомендуется в рекомендациях NIST по цифровой идентификации для предотвращения захвата учетной записи.

Проведенные исследования можно использовать для разработки систем аутентификации на основе RBA, а также для улучшения защиты существующих систем, используя RBA в качестве дополнительного фактора аутентификации.

Литература

1 Корт, С. С., Теоретические основы защиты информации: учебное пособие / С. С. Корт. – М. : Гелиос АРВ, 2004. – 240 с.