## Экспертное заключение

**Автор:** Шарунцова Анна Александровна, КБ-51СО

**Программа:** Online-store authorization.

Выполнена в рамках курсовой работы: Некоторые вопросы обеспечения информационной безопасности при проектировании веб-сайта.

**Научный руководитель:** Мурин Дмитрий Михайлович.

**Аннотация:**   Программа предназначена для авторизации пользователей в личном кабинете интернет-магазина. Программа обеспечивает ряд следующих функций:

1. Возможность регистрации по номеру телефона.
2. Возможность входа в личный кабинет по номеру телефона и многоразовому паролю.
3. Возможность восстановить пароль по номеру телефона и одноразовому паролю.
4. Возможность двухфакторной аутентификации для совершения важных в плане безопасности действий.

**Условия эксплуатации:** Для корректной работы программы необходимо иметь следующее программное обеспечение:

* Платформа Node.js версии 2.10.3.
* Сервер базы данных Redis версии не ниже 2.6.14.
* Сервер базы данных MySQL версии не ниже 5.6.43.
* Сервер базы данных MongoDB версии не ниже 4.0.

**Данные:**

1. Входные данные

Введенные пользователем данные в интерфейсе клиентской части программы.

1. Выходные данные

Обработанные сервером клиентские запросы.

1. Хранение данных

Учетные данные пользователей хранятся в БД MySQL. Данные о текущих сессиях хранятся в БД Redis. Данные об одноразовых сгенерированных смс-кодах хранятся в БД MongoDB.

**Среда разработки:** JetBrains WebStorm 2018.3.

**Языки программирования:** JavaScript, HTML, CSS.

Программа написана на основе фреймворка Express.js.

Использованы следующие модули:

* "connect-redis": "3.1.0",
* "cookie-parser": "1.4.4",
* "express": "~4.16.1",
* "express-handlebars": "^3.1.0",
* "express-session": "1.14.1",
* "hbs": "^4.0.4",
* "http-errors": "~1.6.3",
* "mongodb": "^3.2.4",
* "mongoose": "^5.5.7",
* "morgan": "~1.9.1",
* "mysql-promise": "^5.0.0",
* "passport": "0.3.2",
* "passport-local": "1.0.0",
* "password-validator": "^4.1.1",
* "promise-mysql": "^3.3.1",
* "promise-redis": "0.0.5",
* "random-number": "0.0.9",
* "request": "^2.88.0",
* "request-promise-native": "^1.0.7",
* "uglify-js": "^3.5.11"

Использована библиотека jQuery 1.8.3 и плагин jQuery.mask.js.

### **Объём программы:** Общий объем программы составляет - 31,7 МБ. Из него 31,1 МБ составляют встроенные модули.

**Используемые принципы и алгоритмы решения задач:**

1. Алгоритм MD5 для хеширования паролей.
2. Алгоритм аутентификации по многоразовым паролям.
3. Алгоритм аутентификации по одноразовым паролям.

**Структура программного средства:**

1. Пользователь получает страницу с возможностью зарегистрироваться или зайти в личный кабинет.
2. При выборе варианта «зарегистрироваться» пользователь
   1. Вводит свой номер телефона
   2. Подтверждает, что телефон принадлежит ему, путем ввода смс-кода, отправленного ему на телефон.
   3. Вводит имя и пароль для окончания регистрации.
   4. Затем перенаправляется на страницу входа в личный кабинет.
3. При выборе варианта «зайти» пользователь
   1. Вводит номер телефона в качестве логина и пароль.
   2. Если он не помнит пароль, то может пройти процедуру сброса пароля, получив код по смс для подтверждения, что телефон принадлежит ему, и создав новый пароль.
      1. После чего отправляется на страницу входа в личный кабинет.

3.3 После входа пользователь оказывается в личном кабинете, функционал которого представляет собой возможность выйти из личного кабинета.

**Тестирование:**

Тестирование серверной части проводилось с использованием программы Postman путем отправки на сервер различных запросов. Тестирование клиентской части проводилось вручную методом чёрного ящика.

Дата Подпись автора:

Заключение комиссии:

Дата:

Члены комиссии: