# RussianCraft Site Engine – RCSE

Целевой сайт – RussianCraft.su, FFCentral.org

Сайтовый движок, максимально гибкий и адаптируемый при помощи расширений (плагинов).

# Функционал

## Система пользователей

### Общее

Система отвечает за обработку данных пользователей – логины, пароли, ФИО, почту и прочую информацию. В обработку этих данных включаются понятия: регистрация, авторизация, редактирование, удаление(блокировка). Также система собирает и техническую информацию: название браузера, ОС и IP адрес(а), с которых пользователь производит авторизацию. Эта информация необходима для улучшения безопасности аккаунта, например:

Если пользователь пользуется исключительно связкой Chrome/Windows 10 и адресом 172.153.13.1, то при входе злоумышленника с параметрами Firefox/Linux; 167.125.53.52 пользователь будет оповещён о подозрительном входе в его аккаунт, после чего пользователь сможет либо изменить свой пароль, либо, в случае кражи аккаунта, без проблем получить помощь в службе поддержки.

### Авторизация

На странице (в модальном окне) входа пользователь указывает свои логин/почту и пароль и выбирает, сохранить ли вход в этом браузере (запись в куки входа на срок 1 года), после чего подтверждает вход нажатием кнопки «Войти». Обработка данных производится в несколько этапов:

1. Валидация введённых данных. Осуществляется в асинхронном JS скрипте. Помимо проверки корректности данных (использование только латиницы, символов @\_.-!() и цифр) проверять был ли введён логин или почта. В случае ошибки не отправлять запрос на сервер, вывести сообщение и указать поле с ошибкой. Если все ок – сформировать и отправить запрос в бекэнд. Вывести гифку колесо загрузки.
2. Запрос к базе данных. Из полученных от валидатора данных сформировать запрос к базе данных. В первую очередь проверить существование аккаунта с указанным логином/почтой. Если аккаунт есть, то сравнить хэши паролей, если совпадают – идём дальше, если нет – сообщить пользователю о не правильном пароле. Далее (пароль правильный) проверяем наличие блокировок аккаунта. Если блокировка входа имеется – сообщаем пользователю информацию о бане с предложением обратиться в поддержку. Если же все в порядке – записываем в лог (/userdata/%login%\_%email%/auth.json) данные о входе – Название браузера, ОС, IP-Адрес, дату-время входа, id входа, дату-время истечения входа, состояние. В куки записать данные входа – id входа, логин, стандартная длительность хранения – месяц, при сохранении входа – 1 год.