FOQUZ

Меры безопасности и соответствие стандартам

Реестр российского ПО Минцифры

Платформа FOQUZ входит в реестр российского программного обеспечения Минцифры — публичной электронной системе учёта ПО, которое официально признано происходящим из России и рекомендовано для использования как государственными, так и коммерческими компаниями в РФ. Реестровая запись №17175 от 03.04.2023.

Отсутствие уязвимостей

При включении ПО в реестр программы тщательно проверяются на предмет использования безопасных компонентов и отсутствию уязвимостей. По информации банка данных угроз безопасности ФСТЭК России, уязвимости в платформе FOQUZ отсутствуют.

Импортозамещение

Маркетплейс российского ПО Минцифры РФ рекомендует платформу FOQUZ на замену иностранных программных продуктов, таких как: SurveyMonkey, Qualtrics, GetFeedback, Survio, Alchemer и других крупнейших мировых сервисов опросов и сбора обратной связи.

Сертификат информационной безопасности

Производитель и оператор платформы FOQUZ, ООО «Технологии управления обратной связью», в конце 2023 года прошел сертификацию по международному стандарту информационной безопасности ГОСТ Р ИСО/МЭК 27001-2021 (ISO/IEC 27001:2013)

Лицензия

Наша платформа имеет государственную регистрацию программы для ЭВМ и внесена в Реестр программ для ЭВМ Федеральной службы по интеллектуальной собственности Роспатента РФ.

Соответствие ФЗ-152

Обработка персональных данных на территории РФ должна осуществляться в строгом соответствии с Федеральным законом «О персональных данных» (ФЗ-152). Производитель и оператор платформы FOQUZ является официально зарегистрированным Роскомнадзором оператором персональных данных (регистрационный номер 77-22-133156).

Меры безопасности

Платформа FOQUZ работает на серверах Yandex Cloud и Beget, на которых внедрена система управления информационной безопасностью (СУИБ). Она описывает политику и процедуры, которые позволяют обеспечивать информационную безопасность (ИБ) и минимизировать риски. СУИБ определяет процессы безопасной разработки, правила установки обновлений ПО, действия при возникновении инцидентов. Подробнее о мерах безопасности Yandex Cloud.

Защита от DDoS-атак

Для защиты от кибератак наши облачные сервисы используют технологию Yandex DDoS Protection, которая позволяет минимизировать негативное влияние от DDoS атаки на работу сервиса, а также предотвращать такие угрозы.

Защита ЛК

Мы стремимся минимизировать риски взломов или несанкционированных проникновений в личные кабинеты пользователей и компаний. Для этого постоянно анализируем возможные угрозы и совершенствуем методы защиты и безопасности. На сервисе реализована проактивная система анализа авторизаций и активности пользователей с автоматической блокировкой подозрительного аккаунта.

Резервное хранение

Мы осуществляем резервное копирование всех данных не реже одного раза в сутки. Данные дублируются в двух дата-центрах с настройкой переключения в случае аварии на одном из них. При необходимости для ключевых партнеров с отдельным выделенным сервером возможна индивидуальная настройка резервного копирования всех или наиболее значимых данных.

Методология обновлений CI/CD

Мы развиваем наш продукт в соответствии с растущими требованиями рынка и пожеланиями наших ключевых партнеров. Не реже одного раза за квартал мы обновляем сервис, добавляя в него новые возможности и улучшения. При этом мы используем принцип непрерывной интеграции CI/CD, который позволяет обеспечивать для потребителей прежде всего стабильную работу сервиса и регулярные публикации нового функционала.