О безопасности данных в облачном сервисе myObject.ru

Политика сервиса myObject.ru

Мы понимаем, что безопасность данных, которые наши пользователи хранят в сервисе myObject.ru, является для них критически важной. И если мы не оправдаем ожиданий наших пользователей относительно этой безопасности, то утратим доверие клиентов, которые оплачивают само существование сервиса.

Поэтому мы уделяем особое внимание всем аспектам информационной безопасности при разработке и эксплуатации системы.

Безопасность данных при работе пользователя в клиентском приложении в браузере

Безопасность при работе конечного пользователя на персональном устройстве обеспечивается политикой безопасности браузера, а частично также политикой доступа к глобальным сетям, установленным администратором корпоративной сети.

Подразумевается, что меры безопасности на персональном устройстве должны обеспечивать защиту данных от хищения, искажения и несанкционированного доступа

Безопасность данных при передаче через сеть Интернет

При передаче данных через сеть Интернет создаётся зашифрованный канал связи по протоколу SSL от персонального устройства конечного пользователя до сервера приложения системы myObject.ru.

Безопасность данных при обработке сервером дата-центра

Виртуальная и физическая архитектура серверной инфраструктуры сервиса myObject.ru построена с прямым обменом данными между компонентами системы.

Серверы физически размещены в дата-центре уровня Tier-3 («Дубровка-3» компании «Селектел» в г. Санкт-Петербурге), гарантирующего высочайший уровень безопасности и надёжности инфраструктуры и данных.

Здание дата-центра находится под круглосуточным видеонаблюдением. Все помещения оборудованы системами контроля и учёта доступа по магнитным картам, видеокамерами и датчиками пожарной сигнализации. В серверных помещениях установлены автоматические системы газового пожаротушения. При въезде на территорию и на входе в каждое здание комплекса дата-центра расположены круглосуточные посты вооруженной охраны.

Следует подчеркнуть, что основной источник рисков кражи данных – заинтересованный персонал организации – при удалённой обработке данных в дата-центре физически изолирован от возможности прямого доступа к ним. Что касается самого дата-центра, то обеспечение защиты информации является критически важным для его бизнеса и постоянно находится в центре внимания, в отличие от персонала it-служб организации.

Резервирование

Данные организаций в системе myObject.ru регулярно резервируются как с целью безопасности при сбоях в системе, так и на случай непреднамеренного нарушения данных от действий конечных пользователей.

Серверная инфраструктура сервиса myObject.ru включает систему резервирования настроек приложения и данных пользователей. Для процедуры резервного копирования используется алгоритм с циклом в 28 дней, обеспечивающий доступность пользователям в любой момент времени следующих резервных копий:

- 7 резервных копий за дни последней недели;
- 4 резервные копии за 1, 8, 15 и 22 дни цикла;
- 12 резервных копий за каждый первый день цикла за последний год.

Сервер резервного хранилища физически обособлен от рабочих серверов системы.

Безопасность данных в сервисе myObject.ru

Пользователи сервиса при доступе идентифицируются по имени (адрес e-mail) и персональному паролю. Администратору организации предоставляется инструментарий для управления доступом отдельных пользователей, включая ограничение доступа к отдельным данным.

Безопасность паролей должна быть обеспечена организационными мероприятиями организации-заказчика.

Сервис myObject.ru пароли пользователей в открытом виде не хранит.