



КАК ОБЕСПЕЧИВАЕТСЯ БЕЗОПАСНОСТЬ ДАННЫХ В ОБЛАЧНОМ СЕРВИСЕ МУОБЪЕКТ

При внедрении системы через публичное облако или с развёртыванием частного корпоративного облака под управлением поставщика безопасность данных будет обеспечена на уровне, недостижимом на большинстве предприятий.

Основной источник рисков утечки данных – заинтересованный персонал организации – при удалённой обработке данных в дата-центре физически изолирован от возможности прямого доступа к оборудованию.



ТЕЛЕФОН

(843) 2-250-240
8-800-500-3567



ИНТЕРНЕТ

info@myobject.ru
www.myobject.ru

ПОЛИТИКА БЕЗОПАСНОСТИ

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

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

БЕЗОПАСНОСТЬ В КЛИЕНТСКОМ ПРИЛОЖЕНИИ

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

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

БЕЗОПАСНОСТЬ ПРИ ПЕРЕДАЧЕ

При передаче данных между пользователем и серверами создаётся зашифрованный канал связи по протоколу SSL.

БЕЗОПАСНОСТЬ ПРИ ОБРАБОТКЕ

Виртуальная и физическая архитектура серверной инфраструктуры сервиса «облаков» myObject построена с прямым обменом данными между компонентами.

Серверы физически размещены в российском дата-центре высокого уровня безопасности.

Здание дата-центра находится под круглосуточным видеонаблюдением. Все помещения оборудованы системами контроля 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 расположены круглосуточные посты вооружённой охраны.

Обеспечение защиты информации является критически важным для самого бизнеса дата-центра и постоянно находится в центре его внимания.

РЕЗЕРВИРОВАНИЕ

Серверная инфраструктура myObject включает модуль резервирования данных пользователей с циклом в 28 дней. Пользователям в любой момент времени доступны:

- 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.

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

Пользователи идентифицируются по имени и паролю. myObject пароли пользователей в открытом виде не хранит. Пользователи должны соблюдать меры по сокрытию паролей.

Администратору организации предоставляется инструментарий для управления доступом пользователей, включая ограничение доступа к отдельным данным.