ГДЕ НАХОДЯТСЯ СЕРВЕРА AMOCRM?

Для того, чтобы система являлась надежной, применяется метод общегеографического распределения серверов по всей Российской Федерации. Синхронизация данных между ними происходит постоянно, круглые сутки в режиме реального времени. Это гарантирует надежную защиту от потери важных данных в случае непредвиденной, экстренной ситуации.

БЕЗОПАСНОСТЬ ДАННЫХ

Работа происходит исключительно по лицензионному соглашению. Ваши данные всегда находятся под серьезной и многоуровневой защитой. Ни при каких обстоятельствах amoCRM не имеем права передавать Ваши данные посторонним, третьим лицам или пользоваться ими в собственных интересах. AmoCRM принципиально важен момент конфиденциальности.

КТО ИМЕЕТ ДОСТУП К ДАННЫМ

К вопросу о безопасности amoCRM относится крайне внимательно. Доступ к данным, которыми обладаете - открыт исключительно Вам. Так же, никто из сотрудников компании, за небольшим исключением в виде всего 2-х человек, не имеет возможности доступа к серверам проекта и уж тем более к административной панели. Использование ваших данных в собственных интересах или раскрытие их третьим лицам строго запрещено. Деятельность amoCRM связанна с реализацией сервиса, удобством его эксплуатации и ни каким образом не будет пересекаться с вашей деятельностью или деятельностью вашей компании.

СОХРАННОСТЬ ДАННЫХ, РЕЗЕРВНОЕ КОПИРОВАНИЕ

AmoCRM крайне бережно относится ко всем вашим данным и ведет неустанную деятельность для того, чтобы они оставались в сохранности. Один раз в двадцать четыре часа оборудование автоматически копирует абсолютно всю информацию и данные, при этом сохраняя их на внешнем, защищенном носителе. В связи с этим, у amoCRM всегда будет возможность восстановить полную работоспособность системы даже после тотального сбоя серверов проекта.

ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ СЕРВЕРОВ ПРОЕКТА

Специализированный дата-центр обеспечивает наивысший уровень защиты серверов проекта, которые все время находятся под защитой. Дата-центр оснащен самой современной противопожарной системой, а также в случае необходимости питанием из резервного источника. Система надежной охраны гарантирует, что любая попытка физического проникновения, осуществляемого без разрешения или ведома высшей инстанции будет молниеносно пресечена. Все сказанное ранее дает возможность быть уверенным в работоспособном функционировании системы проекта круглые сутки.

ШИФРОВАНИЕ КАНАЛА ПЕРЕДАЧИ ДАННЫХ

Все данные, которые передаются непосредственно между вашим браузером, например, такими как «Google», «Яндекс» или любыми другими, находятся под надежной защитой при помощи сертификата безопасности SSL. Механизм основанный на 128-битной структуре, предотвращает нежелательный доступ к пакетам, передаваемым между вашим устройством и проектом amoCRM посредством шифрования.

ЗАЩИТА АВТОРИЗАЦИИ

Вы можете быть абсолютно уверены, что вовремя авторизации в системе amoCRM, ваша сессия не окажется похищенной, так же, как и использована в целях хищения персональных данных. Период, во время которого пользователь работал с программой сохраняется в специализированных таблицах БД, у них ограниченный срок существования, идентификатор сессии изменяется несколько раз за короткий промежуток времени, что делает хищение сессии бесполезной в полном объеме для преступников.

ИЗМЕНЕНИЕ КЛЮЧА API

API–ключ (Application Programming Interface – Интерфейс программирования приложения) который используется для авторизации в API, настоятельно рекомендуется осуществлять обновления при использовании формы смены вашего пароля.

Если по истечению срока в полгода ключ не проходил обновления, то это произойдет автоматически, так как система оставляет за собой подобное право. Плюс стоит обратить внимание что API–ключ изменяется при смене логина и пароля пользователя без каких-либо предупреждений.