5 уровней защиты ваших данных

Защита от конкурентов

- Информация о ваших заказах, клиентах и сотрудниках не видна конкурентам. Более того, все ваши данные хранятся в зашифрованном виде так, что даже наши разработчики не могут получить к ним доступ.

Защита от мошенников

- Каждый зарегистрированный пользователь Upservice проходит верификацию данных (проверка Email).
- Каждая компания, добавляемая в Upservice, проверяется в реестрах на существование и соответствие законодательным процедурам.

Защита от поломок оборудования

- Наши серверы находятся в защищенном дата центре. Доступ к серверам имеют только сотрудники с высоким уровнем доступа.
- Дата центр оборудован новейшей системой пожаротушения и несанкционированного проникновения. За серверами ведется круглосуточное наблюдение системными инженерами.
- Вся информация с наших серверов регулярно копируется и сохраняется в бэкапы.

1

2

3

5 уровней защиты ваших данных

Защита от недобросовестных сотрудников

- Обиженный сотрудник не сможет удалить вашу базу клиентов или корпоративные файлы. Так же у него не получится уволить своих коллег или открыть доступ в кабинет компании посторонним людям.
- Корпоративный шпион не сможет получить доступ к задачам и заказам коллег, он будет ограничен только задачами, в которых сам выступает как автор или исполнитель.
- Сотрудники не смогут увести вашу базу клиентов и перепродать ее конкурентам: экспорт из системы невозможен, а доступ к каждому клиенту выдается только ответственному за конкретный заказ и его руководителю.

Защита от информационных атак

- Вся информация на нашем ресурсе передается по зашифрованному протоколу https, что исключает перехват информации третьими лицами.
- На серверах установлена мощная защита от DDoS атак.
- Два раза в сутки все системные файлы Upservice проверяются на наличие вирусов и троянов.
- Мы постоянно обновляем системы безопасности, включая программное обеспечение и аппаратные средства, чтобы закрыть уязвимости и предотвратить эксплуатацию новых методов атак.
- В Upservice реализована система мониторинга, которая отслеживает подозрительную активность пользователей, например, внезапные изменения в поведении или доступ к чувствительным данным из необычных мест.

4

5