Безопасность данных при обмене через Интернет

Последние изменения: 2024-03-26

Когда у продуктов «Клеверенс» появилась возможность обмениваться данными с удаленными устройствами через Интернет, многие пользователи этих продуктов забеспокоились: а как же безопасность данных? Ведь то, что отправляется в открытый доступ, всегда может попасть в руки злоумышленникам и причинить ущерб пользователю.

Но в отличие от ситуации, когда пользователь самостоятельно вывешивает базу в открытую сеть (для обмена с удаленными устройствами), функционал обмена через Интернет от «Клеверенс» уже предполагает многостороннюю защиту данных. И чем обеспечивается эта защита данных, мы расскажем в данной статье.

Защита данных при обмене через Интернет v1

С помощью обмена через Интернет v1 реализован офлайн-обмен данными между базой Mobile SMARTS и ТСД, и все данные проходят через промежуточный сервер, который фактически является облачным сервисом. Поэтому для защиты данных от несанкционированного доступа используются:

- **Сквозное шифрование передаваемых данных.**

  При таком шифровании данные кодируются при помощи пары ключей на сервере Mobile SMARTS (на ПК пользователя) и расшифровываются только на мобильном устройстве, а промежуточные узлы и третьи лица не имеют к ним доступа. Вся информация проходит через промежуточный сервер в зашифрованному виде и доступа к ней не имеет даже сотрудник «Клеверенс».

  Такой же вид шифрования используется в мессенджерах WhatsApp, Telegram и др.

- **HTTPS протокол.**

  Так же как и локальный, промежуточный сервер использует специальный протокол https — безопасное соединение, гарантирующее защищенность передаваемой на сервер информации.

Дополнительно к перечисленным механизмам защиты данных пользователь может включить защиту локального сервера Mobile SMARTS и авторизацию по пользователю.

Защита данных при обмене через Интернет v2

Сравнение обмена через Интернет v1 и v2

В обмене через Интернет v2 доступны оба способа обмена данными: офлайн и онлайн. Офлайн-режим работы реализован точно так же, как и в v1, а онлайн-обмен подразумевает доступ к данным в учетной системе в режиме реального времени (благодаря шлюзу).

Поэтому средства обеспечения безопасности при обмене через Интернет v2 зависят от того, в каком режиме работает пользователь:

- **При работе в офлайн-режиме** — используются те же способы защиты

данных, что и в v1.

- **При работе в онлайн-режиме** — для защиты клиентских запросов используются встроенные средства шлюза. Если в базе Mobile SMARTS не включена авторизация по пользователю, данные все равно будут защищены встроенными средствами защиты шлюза, который перенаправляет онлайн-запросы от мобильного клиента (или учетной системы) на сервер Mobile SMARTS. Если же вы самостоятельно включите авторизацию по пользователю и доступ по https, то встроенная защита не понадобится.

Не нашли что искали?

Задать вопрос в техническую поддержку