Политики безопасности Bluetooth-канала

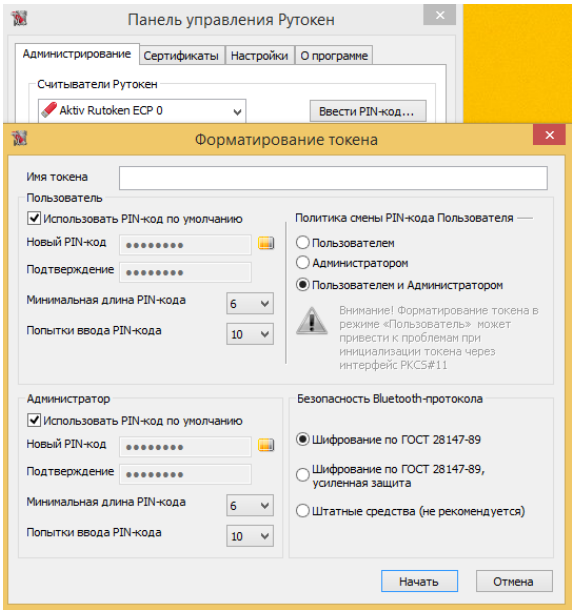
Электронный идентификатор Рутокен ЭЦП Bluetooth может быть отформатирован с 3-мя разными политиками безопасности Bluetooth-канала.

1. Штатные средства безопасности.
   В этом режиме канал между Рутокен ЭЦП Bluetooth защищён стандартным протоколом шифрования E0 (Safer+).
   Этот режим обеспечивает минимально-достаточную безопасность и не требует никаких дополнительных паролей.
   Вы просто "спариваете" Рутокен с компьютером, смартфоном или планшетом - и всё работает само собой.
2. Шифрование по ГОСТ 28147-89.
   В режиме шифрования по ГОСТ 28147-89 все критичные данные, проходящие через Bluetooth, дополнительно шифруются отечественным криптоалгоритмом.
   Симметричные ключи шифрования сменяются через каждые 1000 байт информации, а вырабатываются они из долговременных ключевых пар по алгоритму VKO ГОСТ Р 34.10-2001 (RFC4357).
   Для выработки долговременных ассиметричных ключевых пар и обмена публичными ключами на компьютере, смартфоне или планшете необходимо ввести пароль активации.
   Пароль генерируется токеном при его форматировании и выдаётся из токена наружу лишь один раз.
   Повторное извлечение пароля активации из токена невозможно.
   В этом режиме его длина составляет 16 символов.
3. Шифрование по ГОСТ 28147-89, усиленная защита.
   Этот режим отличается от предыдущего прежде всего длиной пароля активации, которая составляет 51 символ. Такая длина обусловлена требованиями безопасности регулирующего органа.
   Кроме того, в этом режиме выдаётся не 1, а 6 паролей, каждый из которых является одноразовым
   Это означает, что для для выработки долговременных ассиметричных ключевых пар на разных компьютерах, телефонах и планшетах необходимо использовать разные пароли активации.
   Рутокен ЭЦП Bluetooth жестко зафиксированный в режиме "шифрование по ГОСТ 28147-89, усиленная защита" сертифицирован ФСБ России по классу КС2.

Изменение политики безопасности Bluetooth-канала

Для того чтобы изменить политику безопасности Bluetooth-канала, необходимо подключить Рутокен ЭЦП Bluetooth в USB-режиме к компьютеру с установленными драйверами Рутокен версии 2.96.00.0531 или выше.

На вкладке "Администрирование" нажать кнопку "Login..." и ввести PIN-код администратора. После этого нажать кнопку "Форматировать", а в открывшемся окне выбрать одну из политик безопасности и нажать "Начать".



В случае выбора политик "Шифрование по ГОСТ 28147-89" или ""Шифрование по ГОСТ 28147-89", усиленная защита" после окончания форматирования будет высвечен один пароль активации - в первом случае, или несколько одноразовых паролей активации - во втором случае.

Постарайтесь записать или распечатать пароли, либо сохранить их на компьютере в безопасном месте. Повторно получить пароли из токена невозможно.