Работа трекеров серий СИГНАЛ и СМАРТ с телематическим сервером в режиме шифрования данных по стандарту AES128

Для защиты от перехвата данных, передаваемых от телематического устройства к серверу по открытым каналам связи, в протоколе TCP/IP предусмотрена возможность шифровать данные в устройстве перед их отправкой и расшифровывать на сервере при их получении. При этом используется один и тот же алгоритм и ключ шифрования, известный только лицу, отвечающему за заведение устройства на сервере.

При передаче данных в режиме шифрования используется стандарт AES128 (Advanced Encryption Standard), также известный как Rijndael — симметричный алгоритм блочного шифрования (размер блока: 128 бит, ключ: 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES. Этот алгоритм хорошо проанализирован, имеет высокую криптостойкость и в настоящий момент широко используется, в том числе и для передачи данных, составляющих государственную тайну.

Настройка режима шифрования в устройстве

Настройка устройств СИГНАЛ S-255X и СМАРТ S-233X для передачи данных в зашифрованном виде производится при помощи программы NTC Configurator версии 2.4.1 и выше.

Версии прошивок устройств с поддержкой режима шифрования

*Для **СИГНАЛ S-2550**: от **05.02.08** и выше.*
*Для **СИГНАЛ S-2551**: от **06.02.08** и выше.*
*Для **СМАРТ S-2330**: от **04.02.08** и выше.*
*Для **СМАРТ S-2332**: от **04.02.08** и выше.*
*Для **СМАРТ S-2333**: от **04.02.08** и выше.*

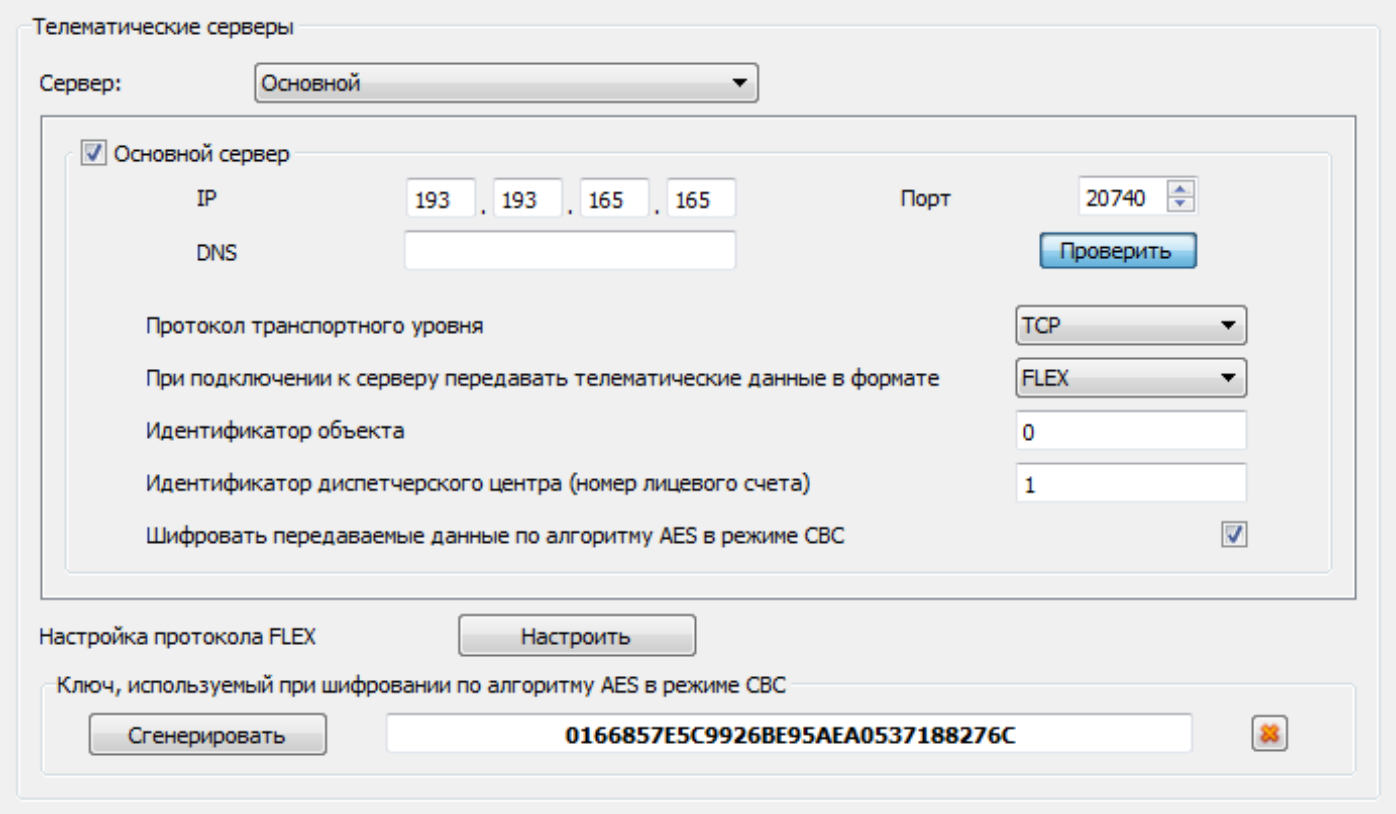
Для включения функции шифрования необходимо во вкладке «2. Передача данных» поставить галочку напротив настройки «Шифровать передаваемые данные по алгоритму AES в режиме CBC». Алгоритм шифрования по стандарту AES128 должен поддерживаться выбранным телематическим сервером.

После включения функции шифрования ниже становится доступной кнопка «Сгенерировать», при нажатии на которую появляется ключ шифрования, сгенерированный для этого устройства случайным образом.

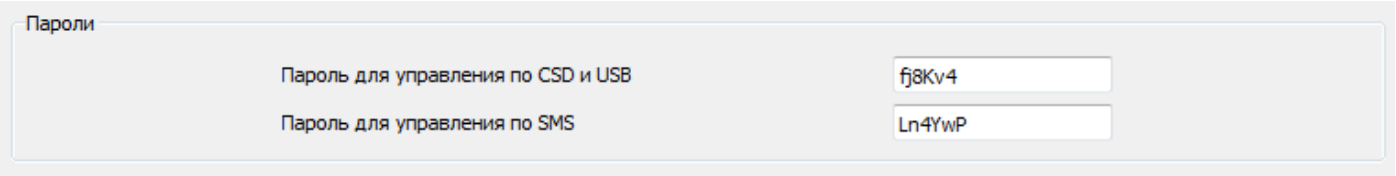
Примечание

В устройствах серий СИГНАЛ и СМАРТ имеется возможность передавать данные на несколько серверов одновременно. Данные будут шифроваться только для тех серверов, для которых установлена соответствующая галочка, разрешающая шифрование.

Перед тем как загрузить настройки в устройство ключ шифрования необходимо скопировать из окна программы NTC Configurator и внести его в настройки объекта на телематическом сервере при заведении устройства.



Для того чтобы посторонние лица не могли соединиться с устройством и считать из него настройки с ключом шифрования, рекомендуется устанавливать сложные пароли на управление по USB и SMS во вкладке «4. Системные настройки».

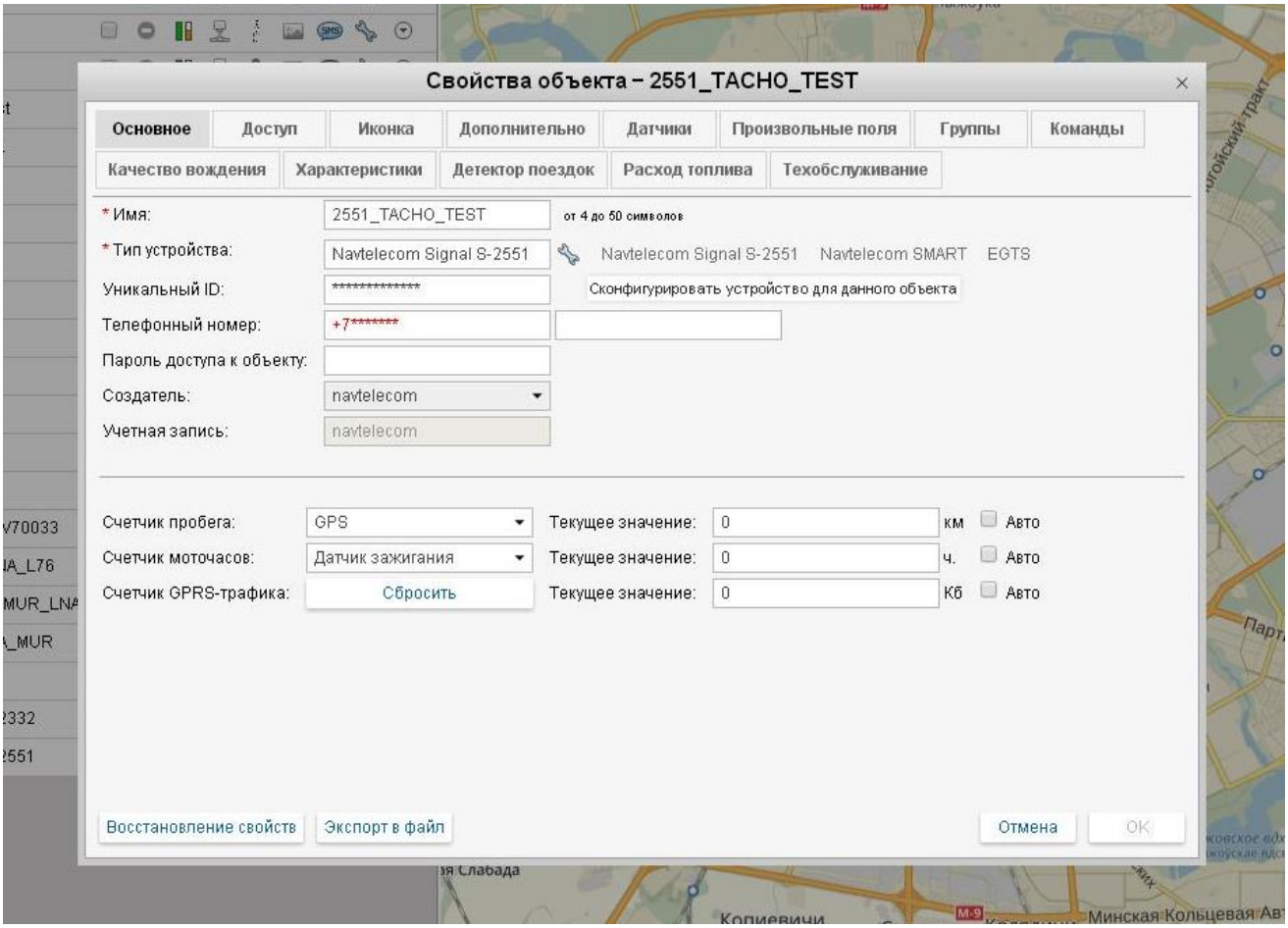


После того, как настройки будут загружены в устройство, оно начнёт передачу данных на заданный телематический сервер в зашифрованном виде.

Настройка режима шифрования при заведении устройства на телематический сервер

На данный момент работа в режиме шифрования данных с устройствами серий СИГНАЛ и СМАРТ реализована в системе мониторинга Wialon Hosting. Пользователи Wialon PRO также могут настроить этот режим, запросив обновлённые скрипты для необходимых устройств (Navtelecom Signal S-2550, Navtelecom Signal S-2551 и Navtelecom SMART) в службе технической поддержки Gurtam.

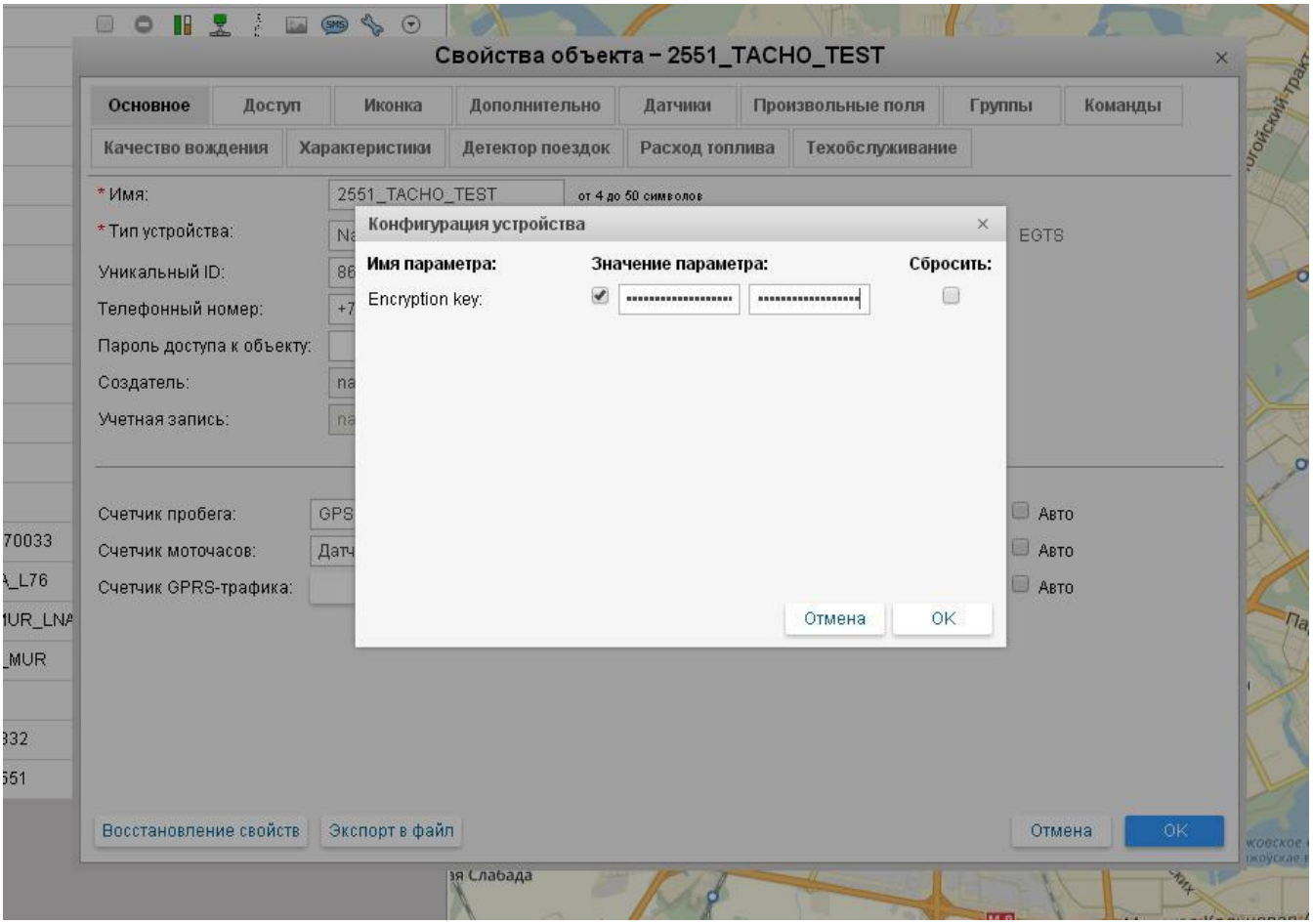
В окне «Свойства объекта» системы мониторинга Wialon Hosting при выборе типа устройства, например Navtelecom Signal S-2551, необходимо нажать на значок «гаечный ключ» рядом с этим полем (Сконфигурировать устройство для данного объекта).



В появившемся окне «Конфигурация устройства» необходимо установить галочку с подсказкой «Изменить пароль». В оба поля для ввода вставьте один и тот же ключ шифрования, скопированный при настройке устройства. Сохранить настройки, нажав «ОК».

При последующем открытии окна «Конфигурация устройства» галочка и звездочки в полях ввода ключа отображаться не будут, тем не менее, для этого устройства режим шифрования с сохранённым ранее ключом будет активен.

Для того чтобы отключить режим шифрования на сервере для данного объекта, необходимо в окне «Конфигурация устройства» установить галочку «Сбросить» и нажать «ОК».



Если устройство по характеру светодиодной индикации находится на связи с сервером (постоянное горение светодиода «GSM»), однако от него не поступают сообщения, то необходимые изменения не успели вступить в силу на сервере. В этом случае необходимо сделать перезагрузку устройства, чтобы оно заново прошло процедуру соединения с сервером.

Работа в режиме шифрования данных, никаким образом не влияет на параметры в передаваемых сообщениях, но увеличивает размер пакета телематической записи примерно на 10-15%.