БЕЗОПАСНОСТЬ ТРЕКЕРА

ВВЕДЕНИЕ

GPS-трекеры предназначены для повышения эффективности бизнеса и защиты транспортных средств от краж. В то же время они могут быть украдены с целью их продажи, могут быть выключены путем перенастройки с неверными параметрами или взломаны для кражи конфиденциальных данных. Чтобы предотвратить несанкционированный доступ к трекерам, необходимо принять дополнительные меры безопасности для входа в систему через все возможные устройства. В случае сбоя входа в систему пользователю отказывают в доступе, и трекеры остаются в безопасности.

ВЫЗОВЫ

Автомобильные трекеры хранят **конфиденциальные данные** для бизнеса и, благодаря различным функциям, помогают организовать оптимальные маршруты, чтобы избежать задержек, снизить расход топлива, обеспечить своевременное обслуживание и обезопасить груз с помощью рационального использования транспортного средства. При потере трекера или контроля над ним клиент теряет возможность следить за транспортным средством, что может привести к серьезным последствиям.

Кража трекера или перехват контроля над ним может вызвать серьезные проблемы как для крупного бизнеса, так и для небольших компаний. Но Вы можете предпринять действенные меры для **повышения безопасности** Ваших трекеров. Хотя и нет абсолютных гарантий, Вы должны сделать так, чтобы злоумышленникам было как можно сложнее саботировать работу трекеров, на установку и настройку которых Вы потратили время для эффективного сбора и мониторинга данных. В противном случае потеря трекера также будет означать потерю вашего дохода.

Наши решения для отслеживания предлагают гораздо больше, чем просто отслеживание. Доступен широкий спектр функций и, что наиболее важно, мы обеспечиваем **безопасное соединение** для всех наших устройств.

РЕШЕНИЕ

Перед использованием трекера необходимо настроить пароль, PIN-код или ключевое слово. Установка трекера из коробки без перенастройки в целях безопасности - одна из самых распространенных ошибок, которые допускают интеграторы. Однако это легко исправить, создав **надежные пароли** (не менее 8 символов: сочетание прописных и строчных букв, цифр и минимум одного специального символа). Если эти изменения не будут внесены, злоумышленникам будет проще получить доступ к трекерам, поскольку они могут знать или узнать исходные настройки.

С опциями Teltonika для безопасного конфигурирования становится трудно украсть или перенастроить трекеры. Все устройства слежения Teltonika поддерживают перечисленные ниже меры безопасности, включая FMB130, который является идеальным выбором для различных сценариев использования.

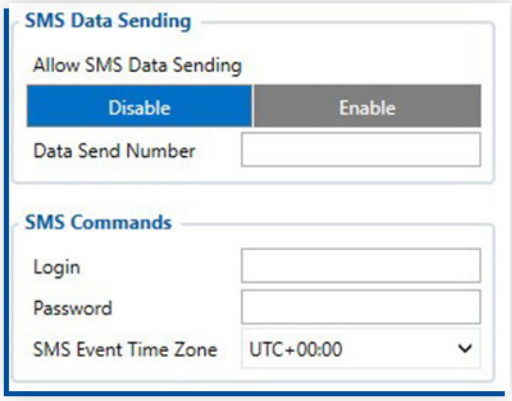
ПАРОЛЬ КОНФИГУРАТОРА

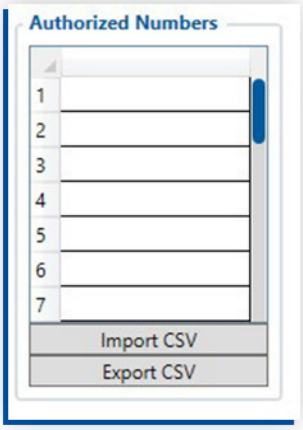
Доступ к конфигуратору должен быть предоставлен только тем, кому нужно им пользоваться. Чтобы сотрудники компании могли настроить трекеры через компьютер, необходимо ввести ключевое слово при подключении через USB. В случае доступа к конфигурации трекера через соединение Bluetooth, помимо ключевого слова, для сопряжения с устройством используется пин-код.

ЗАЩИТА КОНФИГУРИРОВАНИЯ ЧЕРЕЗ СМС КОМАНДЫ

Вы можете использовать SMS-логин и SMS-пароль для доступа к трекерам Teltonika. Кроме того, можно настроить устройства с помощью SMS-команд.

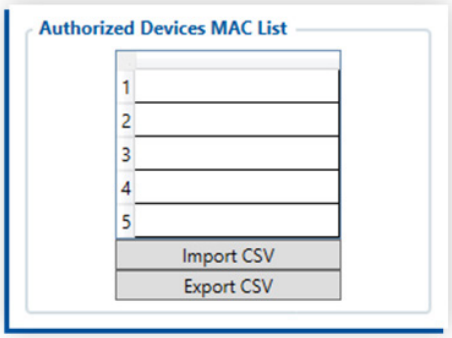
Для дополнительной безопасности с помощью SMS вы можете добавить телефонные номера в список авторизованных номеров в конфигураторе Teltonika. Трекеры будут игнорировать все команды, поступающие с номеров, не указанных в конфигураторе, таким образом, никто другой не сможет настроить устройства или саботировать их.

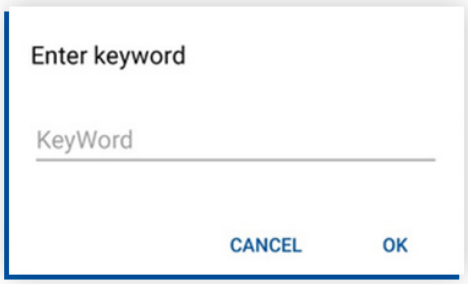




ПРИЛОЖЕНИЕ FMBT

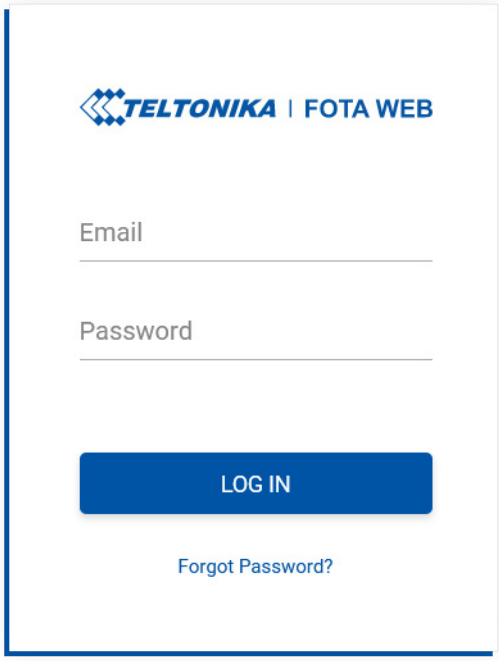
Используя приложение Teltonika FMBT на смартфонах и введя пин-код для сопряжения с трекером или добавив свое устройство в список MAC-адресов разрешенных конфигуратором устройств, Вы можете увидеть все детали о своем устройстве, включая основную информацию, GNSS, GSM, состояние элементов ввода / вывода, OBD и LV-CAN200 / ALL-CAN300 данные в реальном времени. Чтобы настроить трекер через соединение Bluetooth, Вам необходимо вставить ключевое слово, и приложение позволит вам изменить IP-адрес Вашего сервера, порт и данные APN на устройстве.





FOTA WEB

С FOTA WEB у Вас будет легкий доступ к своему автопарку в любой точке мира. Чтобы обновить прошивку или внести изменения в конфигурацию, Вам просто нужно ввести логин и пароль в Вашем браузере, который использует протокол HTTPS - это означает, что вся связь между Вашим браузером и веб-сайтом зашифрована! В целях безопасности не разглашайте свои данные для входа третьим лицам.



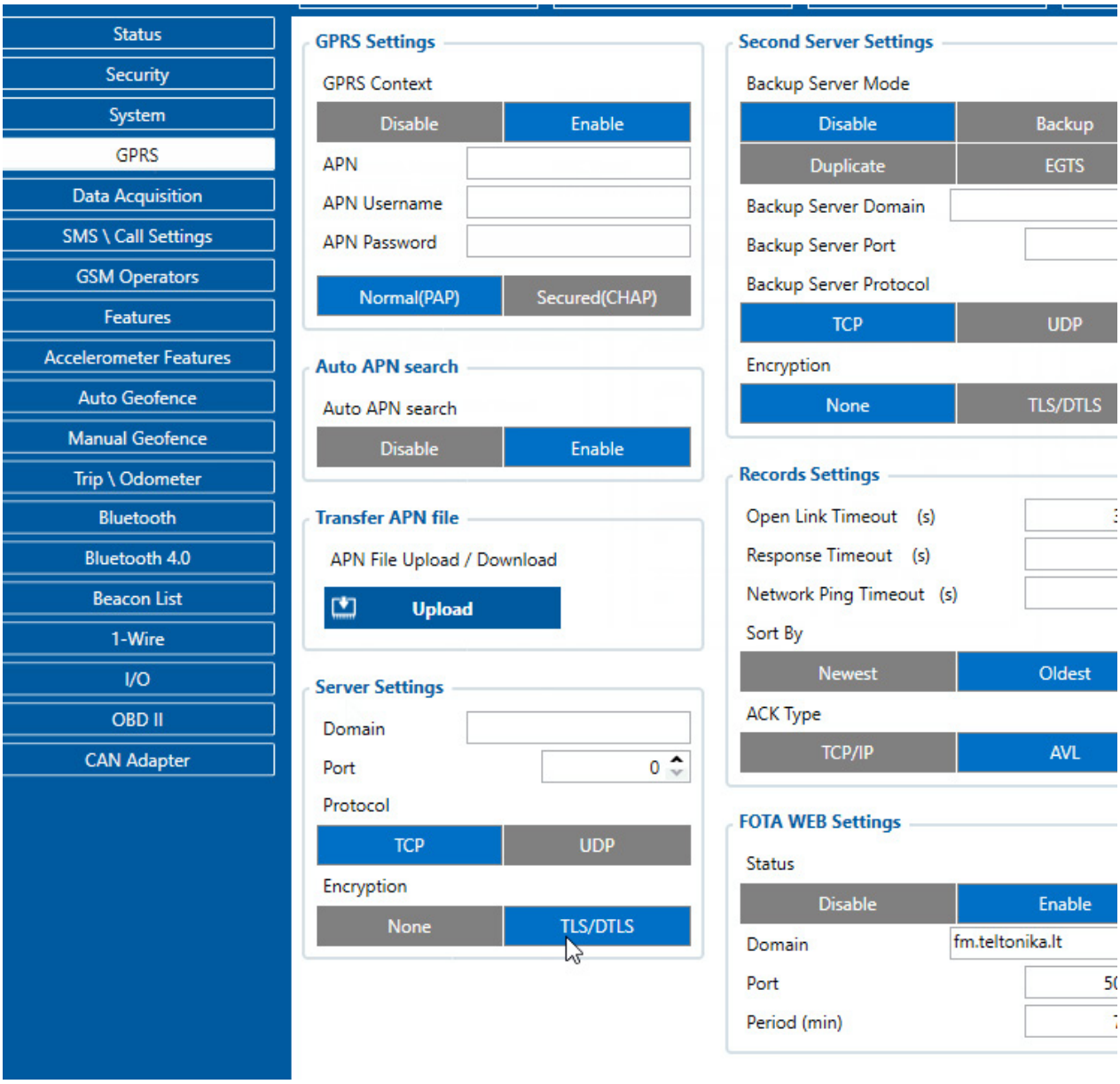
СТАНДАРТ BLE AES-128

Начиная с базовой версии прошивки **03.27.07**, мы успешно внедрили Advanced Encryption Standard AES-128 для обеспечения максимально безопасной передачи данных Bluetooth Low Energy (BLE) между Teltonika GPS трекерами и специальными мобильными приложениями. При наличии AES Key в HEX формате, исходящие данные будут шифроваться с помощью настроенного ключа, а входящие - расшифровываться.

Обратите внимание, что это одна из самых надежных и сложных схем последовательного шифрования на сегодняшний день. Вы можете узнать больше о технических аспектах этой функции здесь.

БЕЗОПАСНОЕ СОЕДИНЕНИЕ С СЕРВЕРОМ (TLS)

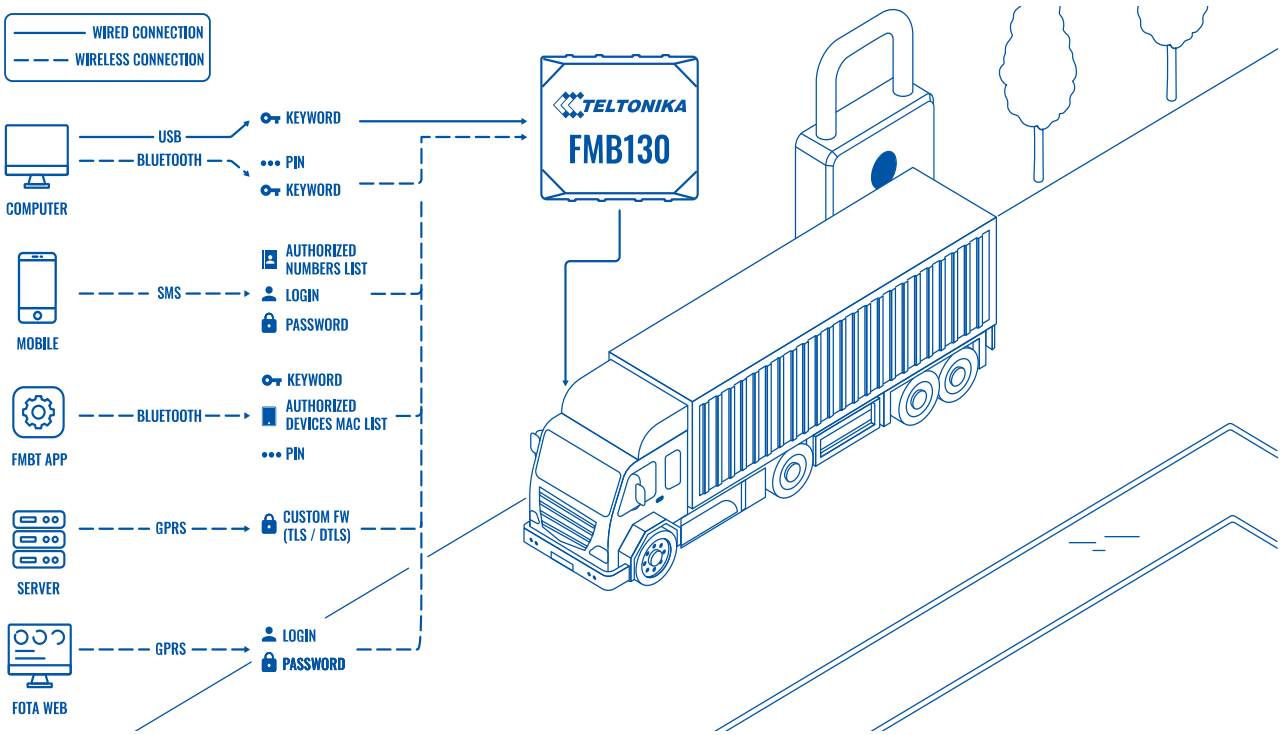
Далее, начиная с базовой версии прошивки **03.27.07**, функция Transport Layer Security TLS была обновлена и реализована для GPS-устройств Teltonika серий FMB0YX, FMB9X0, FMB1YX, FMU1YX, FMM1YX, FMC1YX, FMB2YX и модели FMT100. Этот уровень представляет собой криптографический протокол, который обеспечивает сквозную безопасность данных, передаваемых между сервером и автомобильным GPS-трекером. Подробнее о технических аспектах обновления TLS можно узнать здесь.



VPN

При подключении личных смартфонов и мобильных устройств к трекерам существует проблема безопасности. Частные телефоны более уязвимы для хакерских атак, чем серверы, подключенные к корпоративной сети. Многие компании предлагают недорогое мобильное программное обеспечение, которое шифрует трафик данных или отслеживает подозрительную активность телефонов. Хотя угрозы были минимальными и до сих пор не доставляли больших неудобств, за ними нужно следить. Для безопасного соединения Вы можете использовать SIM-карту с поддержкой VPN-соединения. VPN позволяет создать безопасное соединение с другой сетью через Интернет и защитить Вашу активность в Интернете.

ТОПОЛОГИЯ



ПРЕИМУЩЕСТВА

• **Параметры безопасности для различных устройств** – убедитесь, что трекеры Teltonika безопасны для использования в Вашем бизнесе и в них настроены различные параметры безопасности (ключевые слова, логины, пароли, контакты и списки авторизованных номеров) для всех видов. устройств (телефоны, смартфоны, компьютеры, серверы и приложение FMBT), обеспечивающие безопасность Ваших данных.

• **Быстрый способ настройки безопасного входа** – в конфигураторе Teltonika легко настроить или изменить ключевые слова, логины и пароли, добавить авторизованные телефонные номера или заполнить список MAC-адресов авторизованных устройств.

• **Безопасная отправка данных** – шифрование данных VPN.

ПОЧЕМУ TELTONIKA?

Приватное подключение к трекерам Teltonika позволяет Вам чувствовать себя в безопасности по отношению к конфиденциальным бизнес-данным и быть уверенным, что никто другой не сможет подключиться к устройствам. Основываясь на нашем девизе «Простые решения для IoT», мы предлагаем быстрый способ настройки логинов, паролей или ключевых слов, а также беспроблемное обновление прошивки и настройку трекеров Teltonika.

ПРЕДЛАГАЕМОЕ УСТРОЙСТВО

FMB130

РЕКОМЕНДУЕМОЕ РЕШЕНИЕ

Все устройства слежения Teltonika