Организация Объединенных Наций ECE/TRANS/WP.29/2022/27

Экономический и Социальный Совет

Distr.: General
23 December 2021
Russian
Original: English

Европейская экономическая комиссия

Комитет по внутреннему транспорту

Всемирный форум для согласования правил в области транспортных средств

Сто восемьдесят шестая сессия
Женева, 8–11 марта 2022 года
Пункт 4.8.7 предварительной повестки дня
Соглашение 1958 года: рассмотрение проектов поправок к существующим правилам ООН, представленных GRSG

Предложение по дополнению 1 к первоначальному варианту Правил № 161 ООН (Устройства для предотвращения несанкционированного использования)

Представлено Рабочей группой по общим предписаниям, касающимся безопасности*

Воспроизведенный ниже текст был принят Рабочей группой по общим предписаниям, касающимся безопасности (GRSG), на ее сто двадцать второй сессии (ECE/TRANS/WP.29/GRSG/101, пункт 76). В его основу положен документ ECE/TRANS/WP.29/GRSG/2021/24. Этот текст представляется Всемирному форуму для согласования правил в области транспортных средств (WP.29) и Административному комитету (AC.1) для рассмотрения на их сессиях в марте 2022 года.

* В соответствии с программой работы Комитета по внутреннему транспорту на 2022 год, изложенной в предлагаемом бюджете по программам на 2022 год (A/76/6 (часть V, разд. 20), п. 20.76), Всемирный форум будет разрабатывать, согласовывать и обновлять правила Организации Объединенных Наций в целях улучшения характеристик транспортных средств. Настоящий документ представлен в соответствии с этим мандатом.

Пункт 2.8 изменить следующим образом:

«2.8 “Ключ” означает любое механическое и/или электронное решение, спроектированное и разработанное для того, чтобы служить в качестве средства управления блокирующей системой, спроектированной и сконструированной таким образом, чтобы ею можно было управлять при помощи этого механического и/или электронного решения».

Включить новые пункты 2.10–2.12 следующего содержания:

«2.10 “Основной пользователь” — это пользователь, который может осуществлять авторизацию цифровых ключей. Основных пользователей может быть несколько.

2.11 “Цифровой ключ” означает ключ, разработанный таким образом, чтобы с помощью специальных процессов основной(ые) пользователь(ли) мог(ли) передать его на несколько устройств.

2.12 “В непосредственной близости” означает на расстоянии менее 6 м».

Пункт 5.1.16 изменить следующим образом:

«5.1.16 Кроме того, цифровые ключи должны соответствовать положениям приложения 9».

Приложение:

Включить новое приложение 8 следующего содержания:

«Приложение 8 (зарезервировано)»

Включить новое приложение 9 следующего содержания:

«Приложение 9

Предписания, касающиеся безопасности цифровых ключей

1. Общие положения

Цель настоящего приложения состоит в уточнении требований в отношении документации и проверки цифровых ключей, применяемых с целью эксплуатации устройства для предотвращения несанкционированного использования транспортного средства.

2. Определения

2.1 “*Процесс авторизации*” означает любой метод передачи цифрового ключа, который позволяет эксплуатировать “устройство для предотвращения несанкционированного использования” транспортного средства.

2.2 “*Процесс отмены авторизации*” означает любой метод недопущения применения цифрового ключа с целью эксплуатации “устройства для предотвращения несанкционированного использования” транспортного средства.

2.3 “*Пределами функциональных возможностей*” определяются внешние физические границы (например, расстояние), в которых при помощи цифрового ключа можно эксплуатировать “устройство для предотвращения несанкционированного использования” транспортного средства.

3. Документация

Для официального утверждения по типу конструкции изготовитель транспортного средства представляет следующую документацию:

3.1 описание процесса авторизации;

3.2 описание процесса отмены авторизации;

3.3 описание пределов функциональных возможностей;

3.4 описание мер безопасности, предназначенных для обеспечения безопасной эксплуатации транспортного средства в рамках процесса отмены авторизации цифрового ключа.

4. Требования, касающиеся безопасности эксплуатации

4.1 Цифровой ключ может передаваться на то или иное устройство только с помощью процесса авторизации.

4.2 Должна быть предусмотрена процедура отмены авторизации.

4.2.1 Отмена авторизации цифрового ключа не должна приводить к возникновению небезопасных условий.

С использованием такого стандарта функциональной безопасности, как ISO 26262, и такого стандарта безопасности предполагаемой функциональности, как ISO/PAS 21448, проводится анализ снижения риска, позволяющий документально обосновать степень риска, которому подвергаются водитель и пассажиры транспортного средства в результате отмены авторизации цифрового ключа, а также документально подтвердить возможность снижения риска в результате реализации установленных функций или характеристик по снижению риска.

4.2.2 У основного(ых) пользователя(ей) должна быть возможность устанавливать число зарегистрированных цифровых ключей с действующей авторизацией.

4.3 Пределы функциональных возможностей устройства для предотвращения несанкционированного использования:

4.3.1 Для разблокировки устройства для предотвращения несанкционированного использования необходимо, чтобы зарегистрированный цифровой ключ с действующей авторизацией был обнаружен в салоне транспортного средства или в непосредственной близости от транспортного средства.

4.3.2 Требования, изложенные в пункте 4.3.1, не применяются во время дистанционно управляемого маневрирования и дистанционно управляемой парковки согласно определению, содержащемуся в Правилах № 79 ООН.

4.4 Подробная информация должна содержаться в руководстве по эксплуатации транспортного средства или передаваться с помощью любых других средств предоставления информации, имеющихся на транспортном средстве. Эта информация должна включать по крайней мере следующие описания:

a) описание метода(ов) авторизации цифрового ключа;

b) описание метода(ов) отмены авторизации цифрового ключа.

5. Эффективность системы не должна зависеть от кибератак, киберугроз и наличия уязвимостей. Эффективность мер безопасности доказывается соблюдением положений Правил № 155 ООН.

6. Проверка

Проверку функциональности цифрового ключа проводят с использованием представленной изготовителем документации, указанной в пункте 3.

7. Компетентность контролеров/экспертов по оценке

Оценки на основании настоящего приложения производятся только теми контролерами/экспертами по оценке, которые располагают техническими и административными знаниями, необходимыми для таких целей. В частности, они должны обладать компетенцией контролера/эксперта по оценке согласно стандартам ISO 26262-2018 (Функциональная безопасность — дорожные транспортные средства) и ISO/PAS 21448 (Безопасность в контексте предполагаемых функциональных возможностей дорожных транспортных средств), а также должны быть в состоянии установить необходимую связь с аспектами кибербезопасности в соответствии с Правилами № 155 ООН и стандартом ISO/SAE 21434. Их компетентность должна быть подтверждена наличием у них соответствующей квалификации или другими эквивалентными свидетельствами о профессиональной подготовке».