Организация Объединенных Наций ECE/TRANS/WP.29/2021/99

Экономический и Социальный Совет

Distr.: General
2 September 2021
Russian
Original: English

Европейская экономическая комиссия

Комитет по внутреннему транспорту

Всемирный форум для согласования правил в области транспортных средств

Сто восемьдесят пятая сессия
Женева, 23–25 ноября 2021 года
Пункт 4.7.3 предварительной повестки дня
Соглашение 1958 года: рассмотрение проектов поправок к существующим правилам ООН, представленных GRSG

Предложение по поправкам серии 01 к Правилам № 116 ООН (противоугонные системы и системы охранной сигнализации)

Представлено Рабочей группой по общим предписаниям, касающимся безопасности*

Воспроизведенный ниже текст был принят Рабочей группой по общим предписаниям, касающимся безопасности, на ее сто двадцать первой сессии, состоявшейся в апреле 2021 года (ECE/TRANS/WP.29/GRSG/100, п. 75). В его основу положен документ ECE/TRANS/WP.29/GRSG/2021/11 с поправками, содержащимися в документе GRSG-121-12. Этот текст представляется Всемирному форуму для согласования правил в области транспортных средств (WP.29) и Административному комитету Соглашения 1958 года (AC.1) для рассмотрения и проведения голосования на их сессиях в ноябре 2021 года.

* В соответствии с программой работы Комитета по внутреннему транспорту на 2021 год, изложенной в предлагаемом бюджете по программам на 2021 год (A/75/6 (часть V, разд. 20), п. 20.51), Всемирный форум будет разрабатывать, согласовывать и обновлять правила ООН в целях улучшения характеристик транспортных средств. Настоящий документ представлен в соответствии с этим мандатом.

Пункт 5.1.5 изменить следующим образом:

«5.1.5 "*Ключ*" означает любое механическое и/или электронное решение, спроектированное и сконструированное 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 5.1.7–5.1.9 следующего содержания:

«5.1.7 "*Основной пользователь*" — это пользователь, который может осуществлять авторизацию цифровых ключей. Может существовать более одного основного пользователя.

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

5.1.9 "*В непосредственной близости*" означает на расстоянии менее 6 м».

Включить новый пункт 5.2.16 следующего содержания:

«5.2.16 Кроме того, цифровые ключи должны соответствовать положениям приложения 11».

Пункт 6.1.8 изменить следующим образом:

«6.1.8 "*Ключ*" означает любое механическое и/или электронное решение, спроектированное и сконструированное 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 6.1.13 и 6.1.14 следующего содержания:

«6.1.13 "*Основной пользователь*" — это пользователь, который может осуществлять авторизацию цифровых ключей. Может существовать более одного основного пользователя.

6.1.14 "*Цифровой ключ*" означает ключ, разработанный таким образом, чтобы с помощью специальных процессов основной(ые) пользователь(ли) мог(ли) передать его на несколько устройств».

Включить новый пункт 6.2.10 следующего содержания:

«6.2.10 Кроме того, цифровые ключи должны соответствовать положениям приложения 11».

Включить новый пункт 7.2.7 следующего содержания:

«7.2.7 Кроме того, цифровые ключи должны соответствовать положениям приложения 11».

Пункт 8.1.6 изменить следующим образом:

«8.1.6 "*Ключ*" означает любое механическое и/или электронное решение, спроектированное и сконструированное 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 8.1.11–8.1.13 следующего содержания:

«8.1.11 "*Основной пользователь*" — это пользователь, который может осуществлять авторизацию цифровых ключей. Может существовать более одного основного пользователя.

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

8.1.13 "*В непосредственной близости*" означает на расстоянии менее 6 м».

Включить новый пункт 8.2.11 следующего содержания:

«8.2.11 Кроме того, цифровые ключи должны соответствовать положениям приложения 11».

Включить новые пункты 13.3 и 13.4 следующего содержания:

«13.3 Переходные положения, применимые к поправкам серии 01:

13.3.1 Начиная с официальной даты вступления в силу поправок серии 01 ни одна из Договаривающихся сторон, применяющих настоящие Правила, не должна отказывать в предоставлении или признании официальных утверждений типа ООН на основании настоящих Правил с внесенными в них поправками серии 01.

13.3.2 Начиная с 1 сентября 2022 года Договаривающиеся стороны, применяющие настоящие Правила, не обязаны признавать официальные утверждения типа ООН на основании поправок предыдущих серий (00), впервые выданные после 1 сентября 2022 года.

13.3.3 До 1 сентября 2024 года Договаривающиеся стороны, применяющие настоящие Правила, продолжают признавать официальные утверждения типа ООН на основании поправок предыдущих серий (00), впервые выданные до 1 сентября 2022 года.

13.3.4 Начиная с 1 сентября 2024 года Договаривающиеся стороны, применяющие настоящие Правила, не обязаны признавать официальные утверждения типа, выданные на основании поправок предыдущих серий к настоящим Правилам.

13.3.5 Независимо от положений пункта 13.3.4 Договаривающиеся стороны, применяющие настоящие Правила, продолжают признавать официальные утверждения типа ООН, выданные на основании поправок предыдущих серий к настоящим Правилам, в отношении транспортных средств, на которые не распространяются положения, введенные с поправками серии 01.

13.4 Общие переходные положения

13.4.1 Договаривающиеся стороны, применяющие настоящие Правила ООН, могут предоставлять официальные утверждения типа на основании любой предыдущей серии поправок к настоящим Правилам.

13.4.2 Договаривающиеся стороны, применяющие настоящие Правила ООН, продолжают предоставлять распространение существующих официальных утверждений, выданных на основании любой предыдущей серии поправок к настоящим Правилам».

Включить новое приложение 11 следующего содержания:

«Приложение 11

Предписания, касающиеся безопасности цифровых ключей

1. Общие положения

Целью настоящего приложения является уточнение требований в отношении документации и проверки цифровых ключей, которые используются для управления устройством для предотвращения несанкционированного использования, и/или системой сигнализации, и/или иммобилизатором транспортного средства.

2. Определения

2.1 "*Процесс авторизации*" означает любой метод передачи цифрового ключа, который позволяет осуществлять управление устройством для предотвращения несанкционированного использования, и/или системой сигнализации, и/или иммобилизатором транспортного средства.

2.2 "*Процесс отмены авторизации*" означает любой метод блокировки использования цифрового ключа для управления устройством для предотвращения несанкционированного использования, и/или системой сигнализации, и/или иммобилизатором транспортного средства.

2.3 "*Пределы функциональных возможностей*" определяют внешние физические границы (например, расстояние), в пределах которых с помощью цифрового ключа можно осуществлять управление устройством для предотвращения несанкционированного использования и/или иммобилизатором транспортного средства.

3. Документация

Для целей официального утверждения типа изготовитель транспортного средства представляет следующие документы:

3.1 описание процесса авторизации;

3.2 описание процесса отмены авторизации;

3.3 описание пределов функциональных возможностей;

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

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 стандарта функциональной безопасности, такого как ISO 26262, и стандарта безопасности заданных функций, такого как ISO/PAS 21448, проводится анализ снижения степени риска, позволяющий документально обосновать степень риска, которому подвергаются водитель и пассажиры транспортного средства в результате отмены авторизации цифрового ключа, а также документально подтвердить возможность уменьшения этого риска в

результате обеспечения конкретных функций или свойств, направленных на уменьшение риска.

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

4.3 Пределы функциональных возможностей устройства для предотвращения несанкционированного использования и иммобилизатора:

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 Для отключения иммобилизатора необходимо, чтобы зарегистрированный цифровой ключ с действующей авторизацией был обнаружен в салоне транспортного средства или чтобы отключение иммобилизатора было целенаправленно активировано пользователем, находящимся в непосредственной близости от транспортного средства.

Предельное значение расстояния, на котором возможно отключение иммобилизатора в результате обнаружения ключа в салоне транспортного средства, проверяют с помощью следующей процедуры с учетом допуска в 2000 мм по периметру транспортного средства:

a) Транспортное средство паркуют в безопасном месте, где отсутствуют какие-либо препятствия; при этом двигатель должен быть выключен, а все окна, двери и крыша – закрыты.

b) По согласованию с технической службой изготовитель транспортного средства предоставляет для проведения испытаний типичное устройство пользователя. Уровень заряженности элемента питания устройства с цифровым ключом должен быть максимальным.

c) Техническая служба устанавливает четыре испытательные точки, расположенные по периметру транспортного средства на расстоянии не менее 2000 мм от него. Под расстоянием понимают расстояние между ближайшей точкой транспортного средства и устройством пользователя.

d) Устройство пользователя размещается в каждой из испытательных точек. При попытке управления транспортным средством с использованием его собственной тяги двери транспортного средства должны быть закрыты. Если в одной из испытательных точек удается осуществить управление транспортным средством с использованием его собственной тяги, то требование испытания считается невыполненным.

4.3.3 Требования, изложенные в пункте 4.3.1 и пункте 4.3.2, 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 обеспечиваться с помощью любых других средств предоставления информации, имеющихся в транспортном средстве. Эта информация должна включать, по крайней мере, следующее:

a) описание метода(ов) авторизации цифрового ключа;

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

5. Кибератаки, киберугрозы и факторы уязвимости не должны оказывать негативного влияния на эффективность системы. Эффективность мер безопасности должна быть продемонстрирована соблюдением Правил № 155 ООН.

6. Проверка

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

7. Компетенция контролеров/оценщиков

Оценки согласно настоящему приложению производятся только теми контролерами/оценщиками, которые обладают техническими и административными знаниями, необходимыми для таких целей. Они должны, в частности, обладать компетенцией контролера/оценщика согласно стандартам ISO 26262-2018 (Функциональная безопасность — дорожные транспортные средства) и ISO/PAS 21448 (Безопасность заданных функций дорожных транспортных средств), а также быть в состоянии установить необходимую связь с аспектами кибербезопасности в соответствии с Правилами № 155 ООН и стандартом ISO/SAE 21434. Компетенция контролеров/оценщиков должна подтверждаться наличием у них соответствующей квалификации или другими эквивалентными свидетельствами о профессиональной подготовке».