|  |  |  |
| --- | --- | --- |
|  | Организация Объединенных Наций | ECE/TRANS/WP.29/GRSG/2021/26 |
| _unlogo | **Экономический и Социальный Совет** | Distr.: General30 July 2021RussianOriginal: English |

**Европейская экономическая комиссия**

Комитет по внутреннему транспорту

**Всемирный форум для согласования правил
в области транспортных средств**

**Рабочая группа по общим предписаниям,
касающимся безопасности**

**Сто двадцать вторая сессия**Женева, 12–15 октября 2021 года
Пункт 11 d) предварительной повестки дня
**Поправки к правилам, касающимся устройств
для предотвращения несанкционированного
использования, иммобилизаторов и систем охранной
сигнализации транспортных средств:
Правила № [163] ООН (системы охранной
сигнализации транспортных средств)**

 Предложение по дополнению 1 к первоначальному варианту Правил № [163] ООН о единообразных предписаниях, касающихся официального утверждения системы охранной сигнализации и официального утверждения транспортного средства в отношении
его системы охранной сигнализации

 Представлено экспертом от Международной организации предприятий автомобильной промышленности[[1]](#footnote-1)\*

 Воспроизведенный ниже текст был подготовлен экспертом от Международной организации предприятий автомобильной промышленности (МОПАП) в целях внесения поправок в Правила № [163] ООН для введения технических требований одинакового уровня в отношении цифровых ключей. В его основу положен неофициальный документ GRSG-121-39. Изменения к существующему тексту Правил ООН выделены жирным шрифтом в случае новых положений или зачеркиванием
в случае исключенных элементов.

 I. Предложение

*Пункт 2.10* изменить следующим образом:

«2.10 “*Ключ*” означает любое ~~устройство~~ **механическое и/или электронное решение**, спроектированное и разработанное для того, чтобы обеспечить метод эксплуатации блокирующей системы, спроектированной и сконструированной таким образом, чтобы ее можно было эксплуатировать ~~только~~ при помощи этого ~~устройства~~ **механического и/или электронного решения**».

*Включить новые пункты 2.14 и 2.15* следующего содержания:

«**2.14** **“*Основной пользователь*” — это пользователь, который способен осуществлять авторизацию цифровых ключей.** **Может существовать** **более одного основного пользователя.**

**2.15 “*Цифровой ключ*” означает ключ, предназначенный для передачи
на разные устройства основным(и) пользователем(ями) при помощи специальных процессов**».

*Включить новый пункт 5.10* следующего содержания:

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

*Включить новый пункт 10.7* следующего содержания:

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

*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 “системы охранной сигнализации” транспортного средства.**

**2. Определения**

**2.1 “*Процесс авторизации*” означает любой метод передачи цифрового ключа, который позволяет эксплуатировать “систему охранной сигнализации” транспортного средства.**

**2.2 “*Процесс отмены авторизации*” означает любой метод недопущения применения цифрового ключа с целью эксплуатации “системы охранной сигнализации” 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 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 передается на то или иное устройство только посредством процесса авторизации.**

**4.2 Предусматривается процесс 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** **Подробная информация должна содержаться в руководстве по эксплуатации транспортного средства или передаваться с помощью любых других средств предоставления информации, имеющихся
на транспортном средстве; как минимум эта информация должна включать описание следующего:**

**a) метода(ов) авторизации цифрового ключа;**

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

**5. Эффективность системы не должна зависеть от кибератак, киберугроз и уязвимости к ним. 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 быть компетентны
в качестве контролеров/экспертов 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 устанавливать 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**».

 II. Обоснование

 До завершения разработки этих Правил ООН было начато выполнение задачи по обновлению Правил № 116 ООН для введения технических требований одинакового уровня в отношении цифровых ключей. Эти технические требования были разработаны целевой группой по цифровым ключам.

1. \* В соответствии с программой работы Комитета по внутреннему транспорту на 2021 год, изложенной в предлагаемом бюджете по программам на 2021 год (A/75/6 (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. [↑](#footnote-ref-1)