|  |  |  |
| --- | --- | --- |
|  | Организация Объединенных Наций | ECE/TRANS/WP.29/GRSG/2021/11 |
| _unlogo | **Экономический и Социальный Совет** | Distr.: General29 January 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 первая сессия**

Женева, 12–16 апреля 2021 года

Пункт 10 а) предварительной повестки дня

**Поправки к правилам, касающимся устройств
для предотвращения несанкционированного использования,
иммобилизаторов и систем охранной сигнализации
Правила № 116 ООН (противоугонные системы
и системы охранной сигнализации)**

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

 Представлено экспертами Целевой группы GRSG
по Правилам № 116 (ключ)[[1]](#footnote-1)\*

 Воспроизведенный ниже текст был подготовлен экспертами Целевой группы GRSG по Правилам № 116 (ключ) в качестве замены предложения МОПАП, содержащегося в документе GRSG/2020/24. Изменения к существующему тексту Правил № 116 ООН выделены жирным шрифтом.

 I. Предложение

*Пункт 5.1.5* изменить следующим образом:

«5.1.5 "*Ключ*" означает любое ~~устройство~~ **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 ~~только~~ при помощи этого ~~устройства~~ **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.** **Число основных пользователей может составлять более одного человека.**

**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, не превышающем [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 ~~устройство~~ **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 ~~только~~ при помощи этого ~~устройства~~ **механического и/или электронного решения**».

*Включить новые пункты 6.1.13–6.1.15* следующего содержания:

«**6.1.13** **"*Основной пользователь*" — это пользователь, который может осуществлять авторизацию цифровых ключей.** **Число основных пользователей может составлять более одного человека.**

**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.**

**6.1.15** **"*В непосредственной близости*" означает на расстоянии, не превышающем [6 м]**».

*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 ~~устройство~~ **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 ~~только~~ при помощи этого ~~устройства~~ **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.** **Число основных пользователей может составлять более одного человека.**

**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, не превышающем [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 предполагаемой функциональности, 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 [1 м/2 м] 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 должны быть 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 более [1 м/2 м] 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 согласно определению, содержащемуся в Правилах № 79 ООН.**

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

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

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

**5. На эффективность системы не должна оказываться под угрозой в результате кибератак, киберугроз и уязвимости к ним. Эффективность мер безопасности считается продемонстрированной, если соблюдены положения 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 располагают 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 предполагаемой функциональности 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. Компетенция контролеров/ оценщиков должна быть подтверждена наличием у них соответствующей квалификации или другими эквивалентными свидетельствами о профессиональной подготовке**».

 II. Обоснование

1. Пункты 5.1.5, 6.1.8 и 8.1.6 (уточнение, касающееся определения «ключа»): Устройство рассматривается как носитель ключа; использование в отношении ключа слова «решение» призвано уточнить, что ключ вовсе не обязательно должен быть механическим устройством. На сегодняшний день для управления одной блокирующей системой транспортного средства (устройством для предотвращения несанкционированного использования, системой сигнализации, иммобилизатором) допускается использование нескольких устройств (нескольких типов ключей, нескольких решений). Исключение слова «только» проясняет этот вопрос.

2. Пункты 5.1.7, 6.1.13 и 8.1.11 (включение определения «основного пользователя»): В ходе обсуждения, состоявшегося на четвертом заседании Целевой группы, стало понятно, что необходимо говорить о двух группах пользователей транспортных средств. Согласно концепции, применяющейся в правилах ООН, различия проводятся только между водителем и пассажирами. Однако, поскольку цифровые ключи могут легко передаваться от одного водителя другому, было предложено проводить различия между водителями, которые управляют своим собственным транспортным средством, и водителями, которые пользуются транспортным средством временно или арендуют его. Пример: компания, предлагающая автомобили в аренду, может выступать в качестве основного пользователя, который может передавать цифровой ключ водителю, арендующему транспортное средство. При этом компания не предоставляет водителю, берущему автомобиль на прокат, возможность передавать ключ другим лицам. Таким образом, этот водитель не приобретает статус основного пользователя, который имеет право осуществлять авторизацию цифровых ключей. Включение определения «основного пользователя» позволяет отразить возможность существования нескольких групп пользователей, обладающих разными полномочиями.

3. Пункты 5.1.8, 6.1.14 и 8.1.12 (включение определения «цифрового ключа»): Основным отличительным признаком цифрового ключа является возможность его передачи на несколько устройств с помощью процесса, предусмотренного изготовителем транспортного средства. Именно этот отличительный признак был взят за основу при добавлении нового определения. В отношении этого особого электронного решения было решено использовать термин «цифровой ключ», чтобы подчеркнуть, что в данном случае речь идет о той же технологии, которую понимает под этим термином консорциум «CCC» («Консорциум за подключенные автомобили»).

4. Пункты 5.1.9, 6.1.15 и 8.1.13: Было добавлено определение «в непосредственной близости».

5. Пункты 5.2.16, 6.2.10, 7.2.7 и 8.2.11: Были добавлены новые дополнительные положения о цифровых ключах, касающиеся приложения 11 (см. подробную информацию ниже).

6. Пункты 2.1, 3.1 и 4.1 приложения 11: Предписание о наличии установленной процедуры авторизации цифровых ключей.

7. Пункты 2.2, 3.2, 3.4 и 4.2 приложения 11: Предписание о наличии установленной процедуры отмены авторизации цифровых ключей. Было отмечено, что отмена авторизации представляет собой основной фактор риска при эксплуатации транспортных средств, и поэтому для обеспечения безопасности эксплуатации должны быть предусмотрены конкретные меры безопасности.

8. Приложение 11, пункты 4.2.1 и 7: Добавлены предписания в отношении стандартизированной методологии анализа рисков. За основу текста для пункта 4.2.1 был взят текст из Правил № 100 ООН с некоторыми изменениями, отражающими предпочтение, отдаваемое стандартам ИСО. Текст для пункта 7 был взят из Правил № 157 ООН.

9. Приложение 11, пункты 2.3, 3.3 и 4.3: Необходимо установить ограничения в отношении дистанционного использования цифровых ключей для разблокировки устройства для предотвращения несанкционированного использования, а также для отключения иммобилизатора.

 Нынешний текст Правил № 116 ООН не содержит ограничений в отношении радиуса действия устройств дистанционного управления. Радиус действия используемых систем зависит от применяемой технологии; при этом условия испытаний предусматривают использование расстояния от 6 до 11 метров.

Данное предложение предусматривает три уровня ограничений в отношении дистанционного управления с использованием цифровых ключей (в зависимости от устройств и связанных с ними вариантов использования):

а) Отсутствие каких-либо ограничений для систем охранной сигнализации, с тем чтобы у пользователей была возможность использовать багажник своего транспортного средства для приема посылок, а также контролировать настройки охранной сигнализации. Пользователь может установить временной интервал, в течение которого охранная сигнализации транспортного средства будет отключена, так чтобы доставленную посылку можно было оставить в багажнике.

b) Приложение 11, пункт 4.3.1: Установление ограничения, в соответствии с которым устройства для предотвращения несанкционированного использования будут действовать только в непосредственной близости. Устройства для предотвращения несанкционированного использования предназначены главным образом для предотвращения угона транспортных средств. Поэтому предлагается определить границы зоны, находясь в которой пользователь будет оповещаться о том, что кто-то пытается угнать его транспортное средство.

с) Приложение 11, пункт 4.3.2: Установление ограничения, согласно которому устройства для отключения иммобилизатора будут срабатывать либо только внутри салона транспортных средств с пассивными системами запуска (смарт-запуск), в которых до начала запуска двигателя требуется обнаружение цифрового ключа с действующей авторизацией, либо в качестве альтернативного варианта в непосредственной близости от транспортного средства, при условии совершения пользователем целенаправленных действий с устройством, используемым в качестве ключа транспортного средства. Включенный иммобилизатор препятствует запуску двигателя с целью начала движения. Ограничение расстояния для дистанционного управления иммобилизатором устанавливается, в частности, для обеспечения защиты от угона в тот момент, когда пользователь находится рядом с транспортным средством. Положение о нахождении пользователя в непосредственной близости должно выполняться одновременно с положением о наличии у пользователя соответствующего намерения. Слово «целенаправленно» было добавлено для уточнения того, что, если пользователь находится в непосредственной близости от транспортного средства, то для срабатывания устройства необходимо сознательное действие со стороны пользователя (например, введение PIN-кода, сканирование
QR-кода или штрих-кода, отпечатков пальцев и т. д.).

Зона охвата приемника/антенны, как правило, очерчена кругом, в то время как периметр транспортного средства круглым не является. Приемник сигнала иммобилизатора, как правило, в большей степени обращен в сторону водителя, а не пассажира. Электромагнитные поля в этом случае не искажаются под влиянием материалов, используемых в кузове транспортного средства. Таким образом, существуют технические ограничения, не позволяющие обеспечить полное совпадение зоны приема сигнала с очертаниями салона автомобиля. В свете этих ограничений была добавлена процедура испытания с учетом допусков относительно того, что следует считать салоном транспортного средства, а также добавлены уточнения в отношении критериев прохождения/не прохождения испытания в случае варианта использования с пассивными системами запуска (смарт-запуск).

10. Приложение 11, пункт 4.4: Предписание о наличии в транспортном средстве дополнительной информации о цифровых ключах (например, в руководстве по эксплуатации).

11. Приложение 11, пункт 5: Предписание о соответствии цифровых ключей положениям Правил № 155 ООН о кибербезопасности.

12. Пункты 13.3 и 13.4: Включение переходных положений в соответствии с положениями Регламента по общей безопасности Европейского союза (второй пересмотренный вариант) о кибербезопасности и решением WP.29, принятым на его сто восемьдесят второй сессии (ноябрь 2020 года).

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)