Экономический и Социальный Совет

Distr.: General
27 July 2020
Russian
Original: 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 девятнадцатая сессия
Женева, 6–9 октября 2020 года
Пункт 9 предварительной повестки дня
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 экспертом от Международной организации предприятий автомобильной промышленности*

Воспроизведенный ниже текст был подготовлен экспертом от Международной организации предприятий автомобильной промышленности (МОПАП) для изменения определения ключей, в котором учитываются такие инновационные системы сигнализации транспортных средств, как бесшумная сигнализация или отпирание дверей с помощью смартфона, если таковое будет представлено. В его основу положен документ GRSG-117-31-Rev.1. Изменения к нынешнему тексту Правил № 116 ООН выделены жирным шрифтом.

* В соответствии с программой работы Комитета по внутреннему транспорту на 2020 год, изложенной в предлагаемом бюджете по программам на 2020 год (A/74/6 (часть V, разд. 20), п. 20.37), Всемирный форум будет разрабатывать, согласовывать и обновлять Правила Организации Объединенных Наций в целях повышения эффективности автотранспортных средств. Настоящий документ представлен в соответствии с этим мандатом.

I. Предложение

Пункт 5.1.5 изменить следующим образом:

«5.1.5 "*ключ*" означает любое ~~устройство~~ **физическое 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~~ **физического или электронного решения**.

5.1.5.1 "*виртуальный ключ*" означает ключ, который спроектирован в качестве чисто электронного решения и ~~реализован~~ работает через аппаратное (например, смартфон) и/или программное обеспечение и который может предоставляться другой стороной, помимо изготовителя транспортного средства. Это электронное решение не включает в себя аппаратное/программное обеспечение, в котором оно реализовано».

Добавить новый пункт 5.2.16 следующего содержания:

«**5.2.16 Виртуальные ключи должны соответствовать положениям приложения 11**».

Пункт 6.1.8 изменить следующим образом:

«6.1.8 "*ключ*" означает любое ~~устройство~~ **физическое 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~~ **физического или электронного решения**;

6.1.8.1 "*виртуальный ключ*" означает ключ, который спроектирован в качестве чисто электронного решения и реализован через аппаратное (например, смартфон) и/или программное обеспечение и который может предоставляться другой стороной, помимо изготовителя транспортного средства. Электронное решение не включает в себя аппаратное/программное обеспечение, в котором оно реализовано;»

Добавить новый пункт 6.2.11 следующего содержания:

«**6.2.11 Виртуальные ключи должны соответствовать положениям приложения 11**».

Добавить новый пункт 7.3.6.3 следующего содержания:

«**7.3.6.3 Виртуальные ключи должны соответствовать положениям приложения 11**».

Пункт 8.1.6 изменить следующим образом:

«8.1.6 "*ключ*" означает любое ~~устройство~~ **физическое 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~~ **физического или электронного решения**;

8.1.6.1 "*виртуальный ключ*" означает ключ, который спроектирован в качестве чисто электронного решения и реализован через аппаратное (например, смартфон) и/или программное обеспечение и который может предоставляться другой стороной, помимо изготовителя транспортного средства. Электронное решение не

включает в себя аппаратное/программное обеспечение, в котором оно реализовано;»

Добавить новый пункт 8.3.5.1.4 следующего содержания:

«**8.3.5.1.4 Виртуальные ключи должны соответствовать положениям приложения 11**».

«Приложение 11

Безопасность виртуальных ключей

1. Общие положения

Целью настоящего приложения является уточнение требований в отношении документации и проверки виртуальных ключей, которые используются для управления устройством для предотвращения несанкционированного использования, управления сигнализацией и/или управления иммобилизатором транспортного средства и для которых запрашивается официальное утверждение типа.

2. Определения

2.1 "*Пользователь*" означает лицо, управляющее транспортным средством и имеющее действительный ключ от этого транспортного средства.

2.2 "*Владелец транспортного средства*" означает физическое или юридическое лицо, являющееся владельцем свидетельства о регистрации данного транспортного средства.

2.3 "*Система виртуальных ключей*" означает систему транспортного средства, которая позволяет управлять блокирующей системой с помощью виртуальных ключей.

2.4 "*Авторизация*" виртуального ключа означает, что с помощью данного виртуального ключа пользователь может управлять устройством для предотвращения несанкционированного использования, управлять сигнализацией и/или управлять иммобилизатором транспортного средства. Авторизованный виртуальный ключ является действительным ключом.

2.5 "*Деактивация*" виртуального ключа означает любой метод снятия авторизации с виртуального ключа. Деактивированный виртуальный ключ является недействительным ключом.

2.6 "*Концепция безопасности*" — это описание мер безопасности, разработанных в рамках системы виртуальных ключей, для обеспечения безопасной эксплуатации транспортного средства.

2.7 "*Пределами функциональных возможностей*" определяются внешние физические границы (например, расстояние), в пределах которых виртуальный ключ способен управлять устройством для предотвращения несанкционированного использования, управлять сигнализацией и/или управлять иммобилизатором транспортного средства.

3. Документация

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

3.1 описание системы виртуальных ключей, объясняющее основные функции системы;

3.2 **описание методов авторизации виртуального(ых) ключа(ей) владельцем транспортного средства;**

3.3 **описание методов предоставления пользователю авторизованного виртуального ключа;**

3.4 **описание методов деактивации виртуального ключа;**

3.5 **описание пределов функциональных возможностей;**

3.6 **концепцию безопасности — стратегию безопасного использования свойств "виртуального ключа".**

4. **Требования к безопасной эксплуатации**

Необходимо убедиться в том, что были приняты меры по обеспечению безопасности транспортного средства. Процесс функционирования устройства для предотвращения несанкционированного использования, системы сигнализации и/или иммобилизатора должен предполагать использование средств безопасности, позволяющих предотвратить любой риск блокировки или случайного выхода из строя, которые могли бы негативно сказаться на безопасности дорожного движения. Деактивация виртуального ключа не должна приводить к небезопасному состоянию.

5. **Проверка**

Проверку функциональности виртуального ключа проводят согласно представленной изготовителем документации, указанной в пункте 3».

Добавить новый пункт [9] следующего содержания:

«**9.** **Эффективность системы не должна страдать от кибератак, киберугроз и уязвимостей. Меры безопасности считаются эффективными, если соблюдены положения Правил № 15Z ООН**».

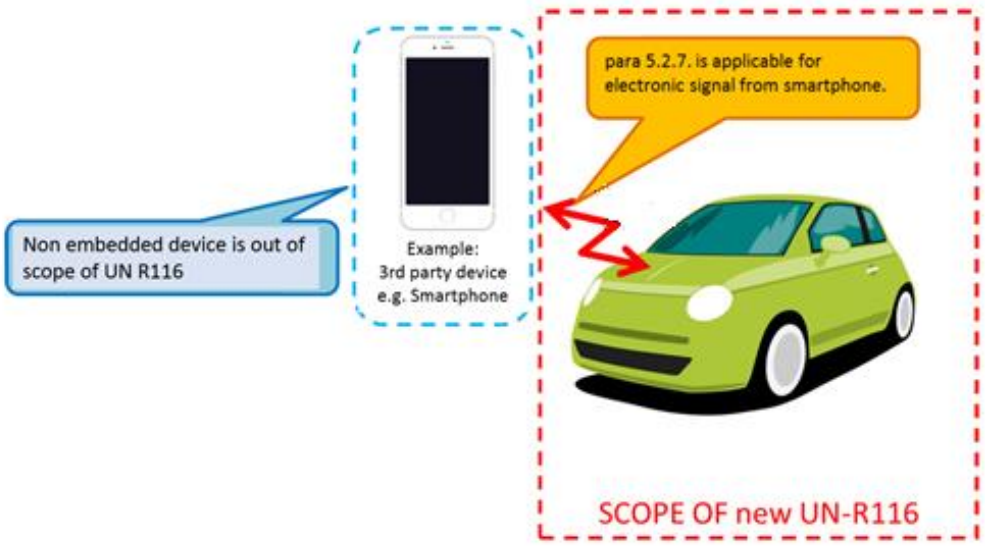
II. Обоснование

1. На сто шестой сессии Рабочей группы по общим предписаниям, касающимся безопасности (GRSG), в мае 2014 года, эксперт от Европейской комиссии (ЕК) проинформировал GRSG о новых инновационных системах охранной сигнализации транспортных средств, таких как беззвучная сигнализация или отпирание дверей с помощью смартфона (GRSG-106-38), и поставил под сомнение необходимость разработки соответствующей поправки к Правилам № 116 ООН. Этот вопрос был дополнительно обсужден на сто седьмой сессии GRSG (сентябрь 2014 года). Эксперт от Германии представил информацию (GRSG-107-08) о том, что в официальном утверждении типа некоторых из этих решений было отказано на том основании, что сигнал смартфона рассматривается как дополнительный ключ, не предоставленный изготовителем транспортного средства, что потенциально может повлиять на работу первоначальной системы сигнализации, установленной изготовителем.

2. Однако сам ключ является не предохранительным (противоугонным) устройством, а лишь средством активации. В соответствии с данными Правилами ООН каждое устройство (противоугонное устройство, система охранной сигнализации или иммобилизатор) может иметь свой собственный ключ для блокировки/разблокировки. Так, например, блокировка и разблокировка системы дверных замков в сферу действия Правил № 116 ООН не входит.

3. Для доступа к транспортному средству могут использоваться не только физические, но и чисто электронные ключи.

4. В соответствии с действующим определением термина «ключ» распространять понятие «только при помощи этого устройства» на смартфон нельзя. Именно по этой причине в определение было добавлено понятие «электронное решение». Аппаратные средства (например, смартфон) и программное обеспечение, передающее «электронное решение» на транспортное средство, под действие Правил № 116 ООН не подпадают. Если электронное решение определяется в качестве соответствующего ключа, то было бы разумным предусмотреть, чтобы это электронное решение, передаваемое с помощью аппаратных средств, отвечало требованиям пункта 5.2.7 (электрические/электронные системы блокировки — см. рисунок ниже).



5. Данное предложение позволяет провести различие между ключом в качестве электронного решения и аппаратным и программным обеспечением, используемым для его передачи, и внести соответствующие поправки в Правила № 116 ООН, позволяющие должным образом отразить в них такие новые инновационные системы. В новых инновационных системах используются компоненты, которые не встроены в транспортное средство: к ним, например, относятся устройства, оборудование, аппаратные средства, операционные системы, каналы связи и внутренние серверы, которые используются для включения или выключения блокирующих систем путем передачи соответствующего варианта электронного решения.

6. В предложении разъясняется, что рассматриваемое здесь электронное решение должно отвечать требованиям Правил № 116 ООН в качестве соответствующего ключа, в то время как все аппаратные и программные средства, используемые только для передачи данного электронного решения, под действие Правил № 116 ООН не подпадают. Вместе с тем согласно пункту 5.4 изготовитель в любом случае должен обеспечить безопасность транспортного средства.

7. В каждое определение «ключа» был добавлен новый подпункт (пункты 5.1.5, 6.1.8 и 8.1.6), с тем чтобы четко отделить чисто электронное решение («виртуальный ключ») от любых других решений для ключей, когда изготовитель транспортного средства предоставляет аппаратное обеспечение (например, карточки с «умными ключами»), используемое для передачи электронного решения. Само определение ключа было пересмотрено таким образом, чтобы оно допускало одновременное наличие различных физических и/или электронных решений для соответствующего устройства.

8. В каждую часть Правил был добавлен соответствующий пункт (5.2.16, 6.2.10, 7.3.6.3 и 8.3.5.1.4) со ссылкой на специальные положения о виртуальных ключах, содержащиеся в новом приложении 11.

9. Было добавлено приложение 11, содержащее положения, касающиеся виртуальных ключей.

До тех пор пока ключ был «устройством», которое физически передавалось владельцу транспортного средства, последний контролировал процесс или был в курсе следующих действий:

a) количество ключей, которыми он располагает;

b) передача ключа какому-либо лицу на время;

c) получение ключа обратно от какого-либо лица;

d) передача ключа при продаже автомобиля;

e) уничтожение ключа или потеря ключом своего функционала при разрядке аккумуляторной батареи.

10. Эти «обычные» действия не были прямо упомянуты в Правилах, поскольку они относятся к ключу как к физическому устройству, которое передается одним человеком другому.

11. В ходе обсуждений с экспертом от Германии, состоявшихся в последние месяцы, была выявлена необходимость конкретизации аналогичных ситуаций, применимых к виртуальному ключу, поскольку в случае виртуального ключа эти действия имеют некоторые отличия, которые не всегда очевидны. Так, в приложение 11 предлагается включить нижеследующие аспекты.

a) Требования к управлению авторизацией как процессу, аналогичному передаче ключей от одного лица другому. Следует отметить, что традиционно эти действия охватывают только вовлеченных лиц (например, владельца транспортного средства и водителя либо покупателя транспортного средства), а также физический ключ. В случае виртуального ключа все вовлеченные лица должны в дополнение к этому идентифицировать себя через посредство программного обеспечения, которое предназначено для управления авторизацией и которое может быть собственностью изготовителя транспортного средства либо третьей стороны. Такая идентификация и обработка данных, связанных с управлением авторизацией виртуальных ключей, должны соответствовать национальным регламентам в области защиты данных и не охватываются Правилами № 116 ООН.

b) Деактивация ключей аналогична процессу получения ключа обратно от какого-либо лица, однако эти функции не являются на 100 % идентичными, поскольку деактивация дает возможность забрать ключ у человека без его ведома; является ли это законным или нет, зависит от национального законодательства, касающегося защиты права собственности. Как бы то ни было, настоящее предложение подразумевает требование о том, чтобы процесс деактивации осуществлялся таким образом, чтобы не создавалось опасных условий.

c) Пределы функциональных возможностей: для традиционного физического ключа на 100 % ясно, что пределом функциональных возможностей является вставка ключа в физическое устройство блокирующей системы. Для систем с «умными ключами» функциональные возможности расширены за счет пространства вокруг транспортного средства. Полностью же виртуальный ключ в принципе может быть передан из любой точки мира на транспортное средство в зависимости от выбранной технологии. Сюда относятся случаи, когда лицо, управляющее устройством для предотвращения несанкционированного использования, сигнализацией или иммобилизатором, может не иметь достаточной информации о текущем состоянии транспортного средства (припарковано, находится в движении). Национальные законодательства, касающиеся дистанционного управления, в настоящее время не гармонизированы, в

то время как некоторые автоматизированные функции (например, дистанционная парковка) требуют использования дистанционного управления. Некоторые органы власти, например, требуют возможности расширять пределы функциональных возможностей при особых правовых условиях. С тем чтобы сохранить нейтральный подход с точки зрения технологий, а также нейтральность по отношению к национальным законодательствам, в настоящем предложении пределы функциональных возможностей четко не устанавливаются, однако они должны быть такими, которые не создают небезопасных условий.

d) Применение вышеуказанных функций может варьироваться в зависимости от регионов и изготовителей транспортных средств. Именно поэтому приложение 11 содержит требование о предоставлении изготовителем транспортного средства соответствующей документации и пояснений относительно концепции безопасности применяемых функций. Проверку проводят на основе сценариев использования, указанных в представленной документации.