Организация Объединенных Наций ECE/TRANS/WP.29/GRSG/2015/16

Экономический и Социальный Совет

Distr.: General
20 February 2015
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

108-я сессия
Женева, 4–8 мая 2015 года
Пункт 3 предварительной повестки дня
Правила № 39 (механизм для измерения скорости)

Предложение по поправкам серии 01 к Правилам № 39 (механизм для измерения скорости)

Представлено экспертом от Международной автомобильной федерации*

Воспроизведенный ниже текст был подготовлен экспертом от Международной автомобильной федерации (ФИА) с целью предложить дальнейшие поправки к предложению, представленному Бельгией по требованиям к эффективности, касающимся установки одометров на транспортных средствах (ECE/TRANS/WP.29/GRSG/2015/15). Изменения к документу ECE/TRANS/WP.29/GRSG/2015/15 выделены жирным шрифтом.

* В соответствии с программой работы Комитета по внутреннему транспорту на 2012−2016 годы (ECE/TRANS/224, пункт 94, и ECE/TRANS/2012/12, подпрограмма 02.4) Всемирный форум будет разрабатывать, согласовывать и обновлять правила в целях улучшения характеристик транспортных средств. Настоящий документ представлен в соответствии с этим мандатом.

GE.15-03207 (R) 240315 240315
1503207

I. Предложение

Название Правил изменить следующим образом:

"ЕДИНООБРАЗНЫЕ ПРЕДПИСАНИЯ, КАСАЮЩИЕСЯ ОФИЦИАЛЬНОГО УТВЕРЖДЕНИЯ ТРАНСПОРТНЫХ СРЕДСТВ В ОТНОШЕНИИ МЕХАНИЗМА ДЛЯ ИЗМЕРЕНИЯ СКОРОСТИ И ОДОМЕТРА, ВКЛЮЧАЯ ИХ УСТАНОВКУ"

Содержание, приложения изменить следующим образом:

"Приложения

…

Приложение 3 − Испытание спидометра **и одометра** на точность в связи с контролем за соответствием производства

Приложение 4 − Испытание одометра на защиту от несанкционированного вмешательства в связи с контролем за соответствием производства

Приложение 5 − Подход на основе общих критериев профиля защиты от противоправного занижения показателей пробега"

Пункт 1 изменить следующим образом (включая сноску [1]):

"1. ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящие Правила применяются к официальному утверждению транспортных средств категорий L, M и N[1].

_____

[1] Согласно определениям, содержащимся в Сводной резолюции о конструкции транспортных средств (СР.3) (документ ECE/TRANS/WP.29/78/Rev.3, пункт 2 − www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29resolutions.html)".

Пункты 2.1−2.6 изменить следующим образом:

"2.1 под *"официальным утверждением транспортного средства"* подразумевается официальное утверждение типа транспортного средства в отношении механизма для измерения скорости и одометра, включая его установку;

2.2 под *"типом транспортного средства в отношении его спидометра и одометра"* подразумеваются транспортные средства, не имеющие между собой существенных различий, когда эти различия могут касаться, в частности, следующих параметров:

2.2.1 обозначение размера шин, выбранных из ассортимента обычных шин;

2.2.2 общее передаточное число коробки передач, включая любые редукторы, передаваемое на спидометр;

2.2.3 тип спидометра, который характеризуется:

2.2.3.1 допусками на измерительный механизм спидометра;

2.2.3.2 технической константой спидометра;

2.2.3.3 диапазоном показываемых скоростей;

2.2.4 тип одометра, который характеризуется:

2.2.4.1 технической константой одометра;

2.2.4.2 числом цифр.

2.3 под *"нормальными шинами"* подразумевается тип или типы шин, которыми изготовитель снабжает данный тип транспортного средства; зимние шины не рассматриваются как нормальные шины;

2.4 *"нормальное рабочее давление"* означает давление холодного воздуха согласно спецификации изготовителя, увеличенное на 0,2 бара;

2.5 под *"спидометром"* подразумевается элемент механизма для измерения скорости, который указывает водителю скорость транспортного средства в любой данный момент[2];

2.5.1 под *"допусками на измерительный механизм спидометра"* подразумевается точность самого спидометра, обозначаемая в виде верхнего и нижнего пределов показываемой скорости для какого-либо диапазона реальных скоростей;

2.5.2 под *"технической константой спидометра"* подразумевается отношение между числом оборотов или импульсов в минуту на входе и конкретной скоростью, показываемой на дисплее;

2.6 под *"одометром"* подразумевается та часть информационного механизма, которая указывает водителю фактический пробег транспортного средства в результате любого его передвижения и включает устройство для (физического) замера, вычислительное устройство и варианты хранения и альтернативного отображения данных.

2.6.1 под *"технической константой спидометра"* подразумевается отношение между числом оборотов или импульсов на входе и расстоянием, пройденным транспортным средством;

2.7 под *"транспортным средством в порожнем состоянии"* подразумевается транспортное средство в снаряженном состоянии с полной заправкой топлива, охлаждающей жидкости, масла, с полным набором инструментов и запасным колесом (в случае, если оно включено изготовителем в комплект стандартного оборудования), с находящимся на нем водителем весом 75 кг, однако без водителя-сменщика, необязательных принадлежностей и без груза".

Пункты 3.1–3.2.1 изменить следующим образом:

"3.1 Заявка на официальное утверждение типа транспортного средства в отношении механизма для измерения скорости и одометра, включая их установку, представляется изготовителем транспортного средства или его надлежащим образом уполномоченным представителем.

[2] Спидометр не включает в себя индикатор скорости и расстояния тахографа, если тахограф удовлетворяет техническим требованиям в отношении официального утверждения типа, в соответствии с которыми абсолютная разность между истинной и показываемой скоростью не должна превышать величин, предписанных в пункте 5.3 ниже.

…

3.2.1 описание типа транспортного средства с точки зрения положений, приведенных в пунктах 2.2, 2.3, 2.4, 2.5 и 2.6 выше; должен быть указан тип транспортного средства".

Пункт 4 изменить следующим образом:

"4.1 Если тип транспортного средства, представленного на официальное утверждение в соответствии с настоящими Правилами, отвечает требованиям Правил в отношении механизма для измерения скорости и одометра, включая их установку, то данный тип транспортного средства считается официально утвержденным".

Включить новый пункт 5.1 следующего содержания:

"5.1 На транспортное средство, подлежащее официальному утверждению, должен быть установлен бортовой механизм для измерения скорости и одометр, которые соответствуют требованиям настоящих Правил".

Пункты 5.1−5.3 (прежние), изменить нумерацию на 5.2−5.4.

Включить новые пункты 5.5 и ***5.5.3*** следующего содержания:

"5.5 Дисплей одометра должен быть видимым и доступным для водителя. Одометр должен отображать целое число, состоящее по меньшей мере из 6 цифр для транспортных средств категорий M и N, и целое число, состоящее по меньшей мере из 5 цифр для транспортных средств категории L. Тем не менее органы по официальному утверждению типа могут допускать отображение целого числа, состоящего по меньшей мере из 5 цифр, также для транспортных средств категорий M и N в том случае, если это обосновано с точки зрения предполагаемой эксплуатации соответствующих транспортных средств. **Если на дисплее одометра достигнуто максимальное значение (например, 999 999 км), то отсчет на дисплее останавливается на этом максимальном значении (например, 999 999 км).**

5.5.1 Если транспортные средства изготовлены для продажи в стране, пользующейся английскими единицами измерения, то одометр может быть отградуирован в милях. **Показатель совокупного пробега, отображаемый на дисплее одометра, не должен отличаться от фактического пробега транспортного средства более чем на ±4%.**

5.5.2 Данные одометра на протяжении всей цепочки обработки (измерения, расчета, хранения и вывод на дисплей) должны быть защищены от несанкционированного вмешательства. Точные данные о пробеге должны надежно − в соответствии с требованиями к безопасности и гарантии достоверности, предусмотренными в профиле защиты (приведенном в приложении 5) − сохраняться в бортовой системе транспортного средства и достоверно анализироваться в соответствии с общими критериями версии 3.1 от сентября 2012 года. Методология, основанная на общих критериях, и соответствующие методы испытания (CEM) признаны на международном уровне и находятся в открытом доступе (www.commoncriteriaportal.org), а также изда-

ны в виде стандартов ISO/IEC 15408 и ISO/IEC 18045. Несанкционированное вмешательство должно быть сопряжено с такими временны́ми и материальными издержками, чтобы оно было невыгодным в сравнении с отпускной ценой, а также с риском подвергнуться смертельной опасности и экологическими рисками, которые могут возникнуть на протяжении всего срока эксплуатации транспортного средства. Данные о пробеге должны быть доступны для считывания с этого электронного модуля управления через 16-контактный разъем системы бортовой диагностики (БД), установленный на транспортном средстве, однако должны быть защищены от записи (поверху) и изменения значений. Эти данные должны быть доступны для всех заинтересованных сторон, например специалистов мастерских, продавцов подержанных транспортных средств, членов автомобильных клубов, соответствующих органов власти и т.д. Информация о любом расхождении между показателем пробега на дисплее и показателем пробега, хранящимся в защищенной части электронного блока управления, должна выводиться на приборную панель и быть видимой для водителя, например в виде сообщения об ошибке или светового сигнала о неисправности.

5.5.3 **После ремонта или замены одометра или замены соответствующих компонентов число, отображенное на дисплее, должно быть тем же, что и до ремонта или замены оборудования, либо соответствовать этому числу после прохождения незначительного расстояния. В случае этих методов замены или ремонта необходимо также предусмотреть проверенные меры, позволяющие противодействовать несанкционированному вмешательству или искажению числовых данных. После ремонта техническая константа одометра должна оставаться неизменной; точный показатель пробега должен надежно сохраняться и защищаться от несанкционированного вмешательства в бортовой системе транспортного средства. Этот защищенный показатель должен быть доступен для надежного считывания с устройств БД, с тем чтобы его можно было сравнить с показателем, фактически отображенным на дисплее**".

Включить новые пункты 10−10.4 следующего содержания:

"10. ПЕРЕХОДНЫЕ ПОЛОЖЕНИЯ

10.1 Начиная с официальной даты вступления в силу поправок серии 01 ни одна Договаривающаяся сторона, применяющая настоящие Правила, не отказывает в предоставлении или признании официальных утверждений типа, предоставленных на основании настоящих Правил с внесенными в них поправками серии 01.

10.2 Начиная с 1 сентября 2017 года Договаривающиеся стороны, применяющие настоящие Правила, предоставляют новые официальные утверждения типа только в том случае, если тип транспортного средства, подлежащий официальному утверждению, отвечает требованиям настоящих Правил с внесенными в них поправками серии 01.

10.3 Договаривающиеся стороны, применяющие настоящие Правила, не отказывают в распространении официальных утверждений на существующие типы, предоставленных на основании поправок предыдущих серий к настоящим Правилам.

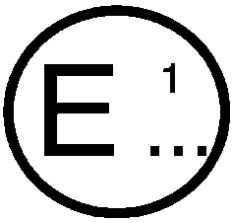
10.4 После даты вступления в силу поправок серии 01 к настоящим Правилам Договаривающиеся стороны, применяющие настоящие Правила, продолжают признавать официальные утверждения типа, предоставленные на основании поправок предыдущих серий к настоящим Правилам".

Приложения 1 и 2 изменить следующим образом:

"Приложение 1

Сообщение

(максимальный формат: A4 (210 x 297 мм)),



направленное: Название административного органа:
.....
.....
.....

касающееся[2]: ОФИЦИАЛЬНОГО УТВЕРЖДЕНИЯ
РАСПРОСТРАНЕНИЯ ОФИЦИАЛЬНОГО УТВЕРЖДЕНИЯ
ОТКАЗА В ОФИЦИАЛЬНОМ УТВЕРЖДЕНИИ
ОТМЕНЫ ОФИЦИАЛЬНОГО УТВЕРЖДЕНИЯ
ОКОНЧАТЕЛЬНОГО ПРЕКРАЩЕНИЯ ПРОИЗВОДСТВА

типа транспортного средства в отношении механизма для измерения скорости и одометра, включая их установку, на основании Правил № 39.

Официальное утверждение № ..... Распространение № .....

1. Фабричная или торговая марка транспортного средства .....
2. Тип транспортного средства .....
3. Изготовитель и его адрес .....
4. В соответствующих случаях − фамилия и адрес представителя изготовителя .....
5. Описание механизма для измерения скорости .....
5.1 Характеристики обычных шин .....
5.2 Характеристики шин, установленных при испытании .....
5.3 Передаточное число механизма для измерения скорости .....
6. Описание одометра**, в том числе фактические данные по итогам оценки** .....
7. Масса транспортного средства при испытании и ее распределение между осями .....
8. Варианты .....
9. Транспортное средство представлено на официальное утверждение (дата) .....
10. Название технической службы, уполномоченной проводить испытания для официального утверждения .....
11. Дата протокола, выданного этой службой .....

12. Номер протокола, выданного этой службой .....

13. Официальное утверждение предоставлено/в официальном утверждении отказано/официальное утверждение распространено/официальное утверждение отменено[2]

14. Место проставления на транспортном средстве знака официального утверждения .....

15. Место .....

16. Дата .....

17. Подпись .....

---

[1] Отличительный номер страны, предоставившей официальное утверждение/распространившей официальное утверждение/отказавшей в официальном утверждении/отменившей официальное утверждение (см. положения настоящих Правил, касающиеся официального утверждения).

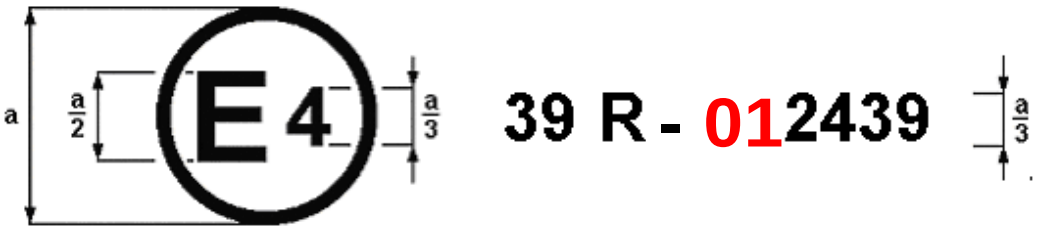
[2] Ненужное вычеркнуть".

Приложение 2

Схемы знаков официального утверждения

Образец A

(См. пункт 4.4 настоящих Правил)

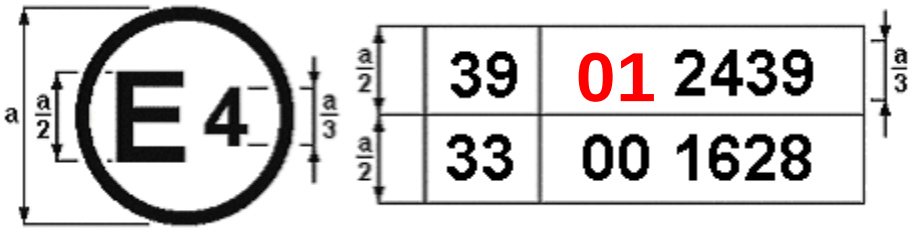


a = 8 мм мин.

Приведенный выше знак официального утверждения, проставленный на транспортном средстве, указывает, что этот тип транспортного средства официально утвержден в Нидерландах (E 4) в соответствии с Правилами № 39. Номер официального утверждения указывает на то, что официальное утверждение было предоставлено в соответствии с требованиями Правил № 39 **с внесенными в них поправками серии 01.**

Образец B

(См. пункт 4.5 настоящих Правил)



a = 8 мм мин.

Приведенный выше знак официального утверждения, проставленный на транспортном средстве, указывает, что этот тип транспортного средства официально утвержден в Нидерландах (E 4) в соответствии с правилами № 39 и 33[1]. Номера официального утверждения указывают на то, что в момент предоставления соответствующих официальных утверждений **Правила № 39 включали поправки серии 01, а Правила № 33 были** по-прежнему в первоначальном варианте.

_____

[1] Второй номер приведен лишь в качестве примера".

Включить новые приложения 4 и 5 следующего содержания:

"Приложение 4

Испытание одометра на защиту от несанкционированного вмешательства в связи с контролем за соответствием производства

(подлежит разработке)

Приложение 5

Подход на основе общих критериев профиля защиты от противоправного занижения показателей пробега

1. Цель

1.1 В основе концепции защиты от противоправного искажения показателей пробега лежит профиль защиты, который должен быть разработан заинтересованными сторонами в соответствии с общими критериями версии 3.1 от сентября 2012 года, изложенными в стандарте ISO/IEC 15408[3].

1.2 Настоящий профиль защиты имеет целью обеспечить соответствие показателя пробега транспортного средства, выведенного на дисплей для водителя, покупателя, продавца, специалиста по ремонту или соответствующего должностного лица, фактическому пробегу этого транспортного средства в результате его любых передвижений.

1.3 Для обеспечения приемлемого уровня затрат на защиту от противоправного занижения показателей пробега с учетом потенциальной выгоды от такого занижения, изготовитель транспортного средства может выбрать надлежащую защиту для своих транспортных средств путем определения контрольных показателей защиты на основе данного профиля защиты. Не реже чем раз в два года группа, состоящая из всех заинтересованных сторон, принимает решение о необходимости обновления данного профиля защиты с учетом технического прогресса.

2. Объект оценки (ОО): обзор

Профиль защиты охватывает всю систему одометра в связи с противоправным искажением показателей пробега, а также все соответствующие сценарии использования, возникающие на протяжении всего срока эксплуатации транспортного средства. Таким образом, применительно к профилю защиты ОО состоит из соответствующих подсистем. С учетом граничных параметров категорий подсистем и систем, можно выделить четыре подсистемы, подверженные противоправному занижению показателей пробега:

[3] См. также: http://www.commoncriteriaportal.org/.

2.1 Подсистема расчета пробега

В эту подсистему входят все электронные блоки управления (ЭБУ) и датчики, задействованные в расчете пробега транспортного средства. Особую опасность, которую необходимо нейтрализовать при помощи мер, предусмотренных настоящим профилем защиты, представляют собой попытки заблокировать регистрацию дополнительного пробега при движении транспортного средства, например путем подачи на блоки расчета ложных сигналов, имитирующих сигналы датчиков движения колеса.

2.2 Подсистема хранения показателя пробега

В эту подсистему входят ЭБУ и модули ЭБУ, в которых хранится показатель фактического пробега. При условии соблюдения функциональных требований безопасности и гарантии достоверности данного профиля защиты изготовители транспортных средств могут выбирать способы их реализации по своему усмотрению. Они могут сделать выбор в пользу хранения данных о пробеге в специальном ЭБУ либо избрать стратегию распределенного и/или реплицированного хранения данных в нескольких ЭБУ, с тем чтобы облегчить обнаружение факта взлома конкретного ЭБУ.

2.3 Подсистема устройства выведения показателя пробега на дисплей

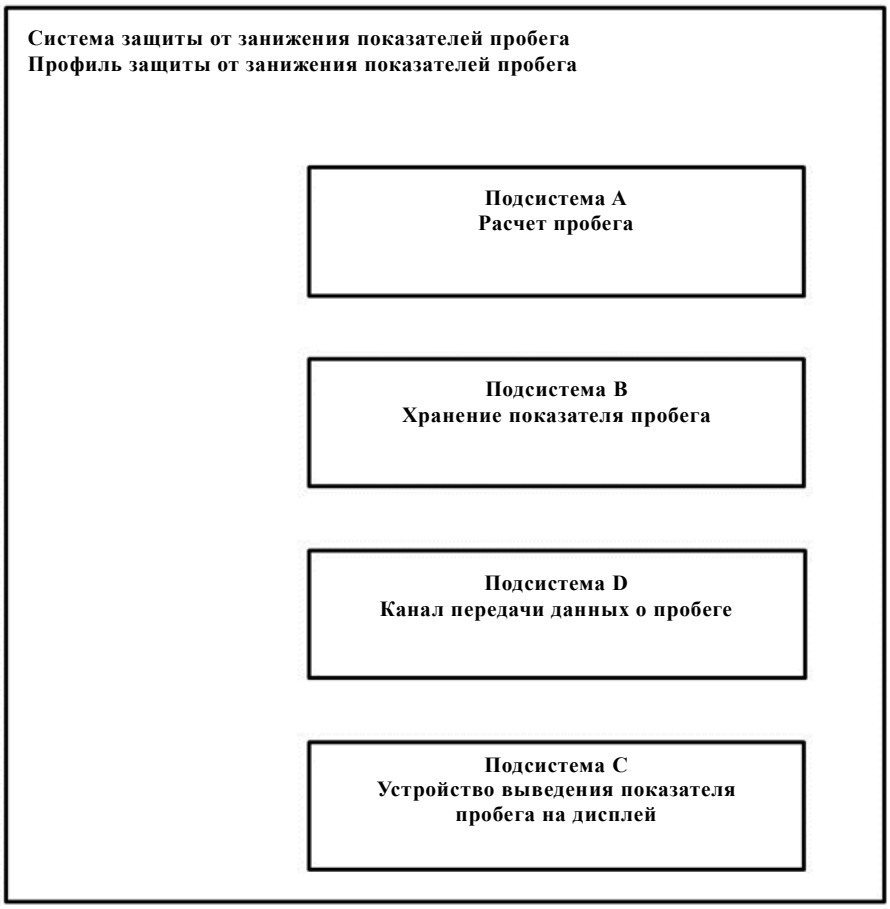
В эту подсистему входит устройство вывода данных на дисплей, которое используется заинтересованной стороной для извлечения показателя фактического пробега и его вывода на дисплей. Таким устройством может служить внешнее сертифицированное устройство, используемое в мастерской, и/или бортовой дисплей транспортного средства. При условии соблюдения требований профиля защиты, касающихся данной подсистемы, допустим любой из вариантов. Однако с точки зрения безопасности потенциальному злоумышленнику гораздо проще попытаться нарушить работу встроенного дисплея, к которому есть прямой доступ, в сравнении с усилиями, которые требуются для того, чтобы исказить данные, поступающие из транспортного средства на внешнее устройство, которое до этого не подвергалось несанкционированному вмешательству.

2.4 Подсистема канала передачи данных о пробеге

В эту подсистему входят канал и процесс передачи данных, которые служат для передачи показателя фактического пробега на устройство выведения данных на дисплей. Этот канал, образующий четвертую соответствующую подсистему общей системы противодействия противоправному занижению показателей пробега, также должен быть защищен профилем защиты в целях предотвращения попыток взлома, совершаемых по методу "активного вмешательства" в работу системы. Например, если показатель пробега является абсолютно точным и надежно сохранен в системе транспортного средства, но передача данных между разъемом БД и устройством вывода на дисплей происходит с использованием незашифрованных сообщений, то злоумышленник может легко применить небольшое устройство, подключив его к системе транспортного средства, которое будет получать доступ к системной шине, перехватывать команду на выдачу показателя пробега и передавать искаженное значение на устройство вывода данных на дисплей. Поэтому профиль защиты предписывает

обязательное использование самой современной технологии шифрования при передаче через канал связи сохраненного значения (подсистема B) на устройство вывода данных на дисплей (подсистема C).

Рис. 1
Объект оценки (обзор системы)



3. Эксплуатация

3.1 Как только система установлена и испытана в ходе сборки транспортного средства, каждое "передвижение" транспортного средства, будь то по дороге или на испытательном стенде (например, в ходе периодических технических осмотров) всегда приводит к наращиванию показателя пробега этого транспортного средства, хранящегося в подсистеме "хранение показателя пробега". Показатель, хранящийся в подсистеме "хранение показателя пробега", ни при каких обстоятельствах не может быть уменьшен или снова обнулен.

3.2 При этом даже полная замена подсистемы "хранение показателя пробега" (что может означать замену одного или нескольких ЭБУ в зависимости от избранной продавцом стратегии реализации настоящего профиля защиты) не должна приводить к искажению значения пробега.

3.3 Цель использования профиля защиты от занижения показателей пробега состоит в том, чтобы затраты злоумышленника превышали

потенциальную финансовую выгоду от вмешательства, поэтому добиться этой цели можно посредством распределения защиты сохраненных данных о пробеге в таком количестве ЭБУ, что производить дорогостоящую замену всех ЭБУ, в которых хранятся данные, с финансовой точки зрения для злоумышленника было бы просто невыгодно, даже в случае транспортных средств высшего класса.

3.4 В ответ на любую команду на выдачу показателя пробега, поданную сертифицированным устройством вывода данных на дисплей (подсистема C) через сертифицированный канал передачи данных (подсистема D), подсистема хранения показателя пробега (подсистема B) выдает любой заинтересованной стороне показатель фактического пробега, который рассчитывается и постоянно обновляется подсистемой расчета пробега (подсистема A).

4. Требования к соответствию

4.1 Требование к соответствию (CC)

Настоящий профиль защиты соответствует общим критериям оценки безопасности информационных технологий (часть 1-3), версия 3.1, пересмотр 4, 2012 год.

4.2 Заявление о соответствии

Настоящий профиль защиты предполагает необходимость обеспечения строгого соответствия настоящему профилю защиты любого контрольного показателя защиты или профиля защиты, подтверждающего такое соответствие.

Пояснение: Это гарантирует, что никакой документ, предписывающий контрольные показатели защиты, который используется изготовителем транспортного средства в целях контроля за их соблюдением, не устанавливает, в случае использования данного решения, менее жесткие требования к безопасности и гарантии достоверности по сравнению с теми, которые предусмотрены в настоящем профиле защиты.

5. Определение проблемы в плане безопасности

5.1 Приоритетный информационный параметр: показатель фактического пробега

Пояснение: Исходя из конструктивных особенностей − структуры общей системы, состоящей из четырех взаимодействующих подсистем, − защита этого приоритетного информационного параметра предполагает необходимость обеспечения защиты определенного комплекса параметров на основе профилей защиты соответствующих подсистем.

Например, подсистема "хранение показателя пробега" должна обеспечивать защиту по меньшей мере двух следующих параметров:

a) показателя фактического пробега (защита заданного параметра данной подсистемой, пользующаяся приоритетом на уровне всей системы) и

b) криптографического ключа, который используется этой подсистемой для обеспечения безопасной и надежной связи с подсистемой "устройство вывода показателя пробега на дисплей".

5.2 Субъекты и внешние устройства

Перечень всех субъектов, которые либо взаимодействуют с системой правомерно, например в качестве регулярных пользователей, применяющих устройство выведения данных на дисплей в мастерской для извлечения и выведения на дисплей показателя фактического пробега, либо взломщики, которые пытаются нарушить целостность системы. Настоящий профиль защиты предусматривает, что подсистема "расчет пробега" охватывает датчики на колесе, поэтому никакие внешние устройства здесь не описываются.

6. Факторы опасности

Для описания факторов опасности, которые ставят под угрозу информационные параметры, в настоящем профиле защиты используется обозначение "T.", за которым следует уникальное наименование опасности. Составители профилей защиты или документов с описанием контрольных показателей защиты могут по своему усмотрению использовать любое наименование при условии, что оно является уникальным. В общем профиле защиты "защита от неправомерного занижения показателей пробега" следует учитывать следующие основные опасности:

6.1 T.Mileage_Corrupted (Пробег искажен)

Фактор опасности, состоящий в том, что показатель, отображенный в подсистеме "устройство вывода показателя пробега на дисплей", может не соответствовать фактическому пробегу этого транспортного средства.

Пояснение: При определении профилей защиты для конкретных подсистем этот фактор опасности делится на несколько различных видов опасностей, ставящих по угрозу соответствующие подсистемы.

6.2 T.Fake_Mileage_Computing (Расчет ложного пробега)

Фактор опасности, состоящий в том, что взломщик попытается смоделировать и/или исказить последовательность приращений показателя пробега, результат которых передается подсистемой "расчет пробега" в подсистему "хранение значения пробега".

6.3 T.Hardware_Memory_Loss (Потеря физической памяти)

В прошлом взлом сводился к тому, что электрически стираемые перепрограммируемые постоянные запоминающие устройства (ЭСППЗУ) теряли свою память, теряя тем самым показатель фактического пробега, и могли быть перепрограмированы с использованием искаженного значения.

6.4 T.Intercepted_Communication (Перехват сообщений)

Этот фактор опасности необходимо распространять на подсистему "устройство выведения показателя пробега на дисплей".

7. Организационные принципы безопасности

Организационные принципы безопасности (OSP) − это правила, процедуры, практические меры и руководящие указания в области безопасности, которые та или иная организация устанавливает для своих операций в порядке достижения целей защиты и которые могут

накладывать ограничения на TOE или его среду. Для их описания используется обозначение "OSP.", за которым следует уникальное имя.

7.1 OSP.Audit (Контроль)

Подсистема "хранение значения пробега" проверяет неудачные попытки аутентификации со стороны подсистемы "устройство вывода показателя пробега на дисплей" и сообщает о них.

7.2 OSP.Crypto (Крипто)

Органы, отвечающие за генерирование ключа для декодирования сообщений (доверенные центры), должны убедиться в том, что ключи для использования с устройствами вывода показателя пробега на дисплей выдаются только сторонам, имеющим на это право.

8. Допущения относительно среды TOE

Перечень допущений относительно среды TOE также является обязательным элементом профиля защиты.

8.1 A.System_Activation (Активация системы)

Изготовители транспортных средств в обязательном порядке активируют систему расчета и хранения показателя пробега после сборки транспортного средства.

Такие допущения сужают возможные сценарии взлома, которые следует учитывать применительно к TOE; например, совершенно очевидно, что без активации можно очень легко пользоваться транспортным средством без регистрации пробега.

9. Цели защиты

Перечень целей защиты для TOE должен быть полным, так чтобы каждому фактору опасности соответствовала по крайней мере одна цель защиты и чтобы, таким образом, ни один фактор опасности не оставался неохваченным. С другой стороны, нет нужды ставить те цели защиты, в которых нет необходимости, с тем чтобы сэкономить усилия и средства, требуемые для разработки. Для обеспечения надлежащего учета факторов опасности и целей защиты в профиле защиты используют матрицу, в которой эти два аспекта находятся во взаимной зависимости типа "множество−множество". Подсистема "хранение значения пробега" содержит в том числе следующие цели:

9.1 O.Access (Доступ)

TOE должен контролировать доступ пользователей к функциям активации (хранения показателей пробега) и вывода данных (показателя фактического пробега).

9.2 O.Audit (Контроль)

TOE должен производить проверку попыток нарушить безопасность системы.

9.3 O.Authentication (Аутентификация)

TOE должен производить аутентификацию подключенных к нему устройств, то есть подсистемы "расчет пробега" и подсистемы "устройство вывода показателя пробега на дисплей".

9.4 O.Integrity (Целостность)

TOE должен поддерживать целостность данных, хранящихся в качестве показателя пробега.

9.5 O.Output (Вывод данных)

TOE должен следить за тем, чтобы данные, которые выводятся на подсистему "устройство вывода показателя пробега на дисплей", точно соответствовали сохраненным данным.

TOE защищен от всех перечисленных факторов опасностей лишь в том случае, если он обеспечивает выполнение всех целей защиты.

10. Требования к безопасности

10.1 Требования к безопасности − это подробно изложенные виды "оптимальной практики" в области разработки защищенных систем. Группа по общим критериям разработала комплексы требований и объединила их в иерархическую систему, состоящую из:

a) функциональных классов;

b) функциональных семейств;

c) функциональных компонентов;

d) функциональных элементов.

10.2 Функциональные классы охватывают следующие аспекты:

a) класс FAU − Контроль безопасности;

b) класс FDP − Защита данных;

c) класс FCO − Связь.

10.3 Таким образом, составители профиля защиты могут легко выбрать требования безопасности из каталога, приведенного в части 2 ОК, адаптировать их для своих нужд и соответствующим образом применить. По аналогии с подтверждением того факта, что все виды опасности покрываются целями защиты, необходимо затем подтвердить в виде матрицы тот факт, что каждая цель защиты охвачена, как минимум, одним функциональным требованием защиты из соответствующего перечня.

Например, цель "O.Output" (Вывод) может быть охвачена при помощи требования FCO_NRO.1 из каталога, приведенного в части 2 Общих критериев.

При этом FCO_NRO.1 расшифровывается следующим образом:

a) FCO (название функционального класса) − Связь;

b) NRO (название функционального семейства) − Предотвращение отказа источника;

c) 1 (номер функционального компонента семейства) − Избирательное доказательство источника.

В случае выбора этого компонента профиль защиты потребует от любого разработчика учесть все три функциональных элемента из каталога. Ниже приведен пример для подсистемы "хранение показателя пробега":

FCO_NRO.1.1: TOE должен иметь возможность получать доказательство источника для передаваемого показателя фактического пробега по команде подсистемы "устройство вывода показателя пробега на дисплей".

Эта возможность, вместе с требованиями функционального класса FCS (криптографическая поддержка), гарантирует, что устройство вывода показателя пробега на дисплей принимает показатель, выданный подсистемой хранения показателя пробега, что обеспечивает, таким образом, отображение истинного значения для пользователя.

10.4 Требования безопасности обычно подразделяют на два класса:

a) Функциональные требования безопасности (виды оптимальной практики), изложенные в части 2 Общих критериев (ISO/IEC 15408), предусматривают набор функций по защите, например возможность проверять попытки получения доступа или возможность производить аутентификацию пользователя.

b) С другой стороны, требования к гарантии безопасности, определяют то, каким образом эти функции разрабатываются и реализуются в системе для обеспечения защиты всех уязвимых мест.

В соответствии с Общими критериями требования к гарантии безопасности сгруппированы исходя из семи оценочных уровней доверия (EAL) 1−7, которые определяют требуемые усилия по проектированию и тестированию и строгость оценки.

К профилю защиты от неправомерного снижения показателя пробега следует применять уровень 4, который предусматривает использование подхода, основанного на методическом проектировании, а также функционального тестирования по принципу "белого ящика" и "черного ящика", однако при этом не требует полуформального и формального проектирования и тестирования, которые необходимы для более высоких EAL.

Оценка защиты от несанкционированного вмешательства и устойчивости к нему одометра должна осуществляться в соответствии с процедурой оценки, определенной в Общих критериях (ISO/IEC 15408), и описана в подробной спецификации процедуры тестирования и оценки, изложенной в "Общей методологии оценки безопасности информационных технологий" (CEM издана в качестве стандарта ISO/IEC 18045). Она, в частности, определяет мероприятия по тестированию и оценке факторов уязвимости. Оценка должна подтвердить, что несанкционированное вмешательство сопряжено с такими временны́ми и материальными издержками, что оно является невыгодным в сравнении с более высокой отпускной ценой, а также с риском подвергнуться смертельной опасности и экологическими рисками, которые могут возникнуть на протяжении всего срока эксплуатации транспортного средства. Эти методы тестирования и оценки признаны на международном уровне и, как следствие, оформлены в виде стандарта в документе ИСО".

II. Обоснование

1. Цель настоящего предложения − дополнить документ ECE/TRANS/WP.29/GRSG/2015/15, представленный экспертом от Бельгии.

2. Неправомерные действия, направленные на искажение показателей пробега, являются причиной непредвиденных сбоев в работе транспортных средств, что может ставить под угрозу безопасность водителя и пассажиров, например в случае выхода из строя транспортного средства.

3. Неправомерные действия, направленные на искажение пробега, приводят к нарушению нормативных требований, определяющих срок службы компонентов, важных с экологической точки зрения[1], и могут ухудшить уровень экологических показателей транспортных средств.

4. Неправомерные действия, направленные на искажение пробега, являются причиной убытков европейских потребителей на сумму 5,6−9,6 млрд. евро ежегодно[2]. Убытки возникают у потребителей не только из-за переплаты при покупке подержанных транспортных средств, но и из-за более высоких издержек на их ремонт и обслуживание. Общая цель защиты от неправомерного вмешательства состоит в том, чтобы противоправные действия, направленные на искажение показателей одометра, было экономически невыгодно на протяжении всего срока службы транспортного средства. Несанкционированное вмешательство должно быть сопряжено с такими временны́ми и материальными издержками, чтобы оно было невыгодным в сравнении с отпускной ценой на протяжении всего срока службы транспортного средства.

5. Неправомерные действия, направленные на искажение пробега, является трансграничной проблемой. Этот вид подлога затрагивает 5−12% от объема продаж подержанных транспортных средств, а в случае трансграничных сделок такой подлог характерен для 30−50% сделок[2].

6. Предлагаемый подход состоит в том, чтобы защитить данные о пробеге от несанкционированного вмешательства с помощью методологии, основанной на общих критериях, которые изложены в приложении 5 и закреплены в стандарте ISO 15408. Он позволяет органам по официальному утверждению типа осуществлять проверку различных контрольных показателей защиты, указанных изготовителем, на их соответствие единому, общему профилю защиты. Этот профиль защиты сначала должен быть согласован соответствующими заинтересованными сторонами. Положения приложения 5 отражают основные этапы разработки этого профиля защиты; их следует использовать в качестве руководящих указаний для экспертов, разрабатывающих профиль защиты.

_____

1 Регламенты (ЕС) № 698/2008, приложение 1, пункт 2.2, и № 692/2008, приложение VII, пункты 1.2 и 1.3.

2 В 25 государствах − членах Европейского союза, статистические данные Европейской комиссии, публикация "Пригодность транспортных средств к эксплуатации на дорогах, оценка последствий" (Roadworthiness Package, Impact Assessment, page 17, Brussels, 13 July 2012).