Организация Объединенных Наций ECE/TRANS/WP.29/2017/46

Экономический и Социальный Совет

Distr.: General
23 December 2016
Russian
Original: English

Европейская экономическая комиссия

Комитет по внутреннему транспорту

Всемирный форум для согласования правил в области транспортных средств

171-я сессия
Женева, 14–17 марта 2017 года
Пункт 4.14 предварительной повестки дня
Соглашение 1958 года − Предложения по поправкам к Сводной резолюции о конструкции транспортных средств (СР.3), представленные рабочими группами Всемирному форуму для рассмотрения

Предложение по проекту руководящих положений о кибербезопасности и защите данных

Представлено неофициальной рабочей группой по интеллектуальным транспортным системам/автоматизированному вождению*

Воспроизведенный ниже текст был подготовлен экспертом от неофициальной рабочей группы (НРГ) по интеллектуальным транспортным системам/автоматизированному вождению (ИТС/АВ). В его основу положен рабочий документ ITS/AD-10-11-Rev.1, распространенный в ходе десятой сессии неофициальной рабочей группы по ИТС/АВ. НРГ по ИТС/АВ предлагает Всемирному форуму для согласования правил в области транспортных средств (WP.29) принять настоящие Руководящие положения о кибербезопасности и защите данных на его мартовской сессии 2017 года.

* В соответствии с программой работы Комитета по внутреннему транспорту на 2016−2017 годы (ECE/TRANS/254, пункт 159, и ECE/TRANS/2016/28/Add.1, направление деятельности 3.1) Всемирный форум будет разрабатывать, согласовывать и обновлять правила в целях улучшения характеристик транспортных средств. Настоящий документ представлен в соответствии с этим мандатом.

GE.16-22882 (R) 060117 060117

1622882

Просьба отправить на вторичную переработку

I. Предложение

"Руководящие положения о кибербезопасности и защите данных

Руководящие положения о мерах по обеспечению кибербезопасности и защиты данных подключенных транспортных средств и транспортных средств, оснащенных технологиями автоматизированного вождения

1. Преамбула

1.1 В связи с переходом к цифровым технологиям в области мобильности и сопутствующим ему увеличением объема данных к безопасности транспортных средств и инфраструктуре, а также к защите прав и свобод субъектов данных предъявляются новые требования.

1.2 По мере увеличения степени автоматизации и взаимосвязанности функций управления будет расти значимость вопросов шифрования данных и кибербезопасности.

1.3 Следовательно, необходимы четкие правила в области кибербезопасности и защиты данных для подключенных транспортных средств и транспортных средств, оснащенных технологиями автоматизированного вождения (ТАВ). Транспортные средства должны быть защищены от внешнего вмешательства и манипулирования.

1.4 Настоящие руководящие положения призваны довести до сведения автопроизводителей, поставщиков компонентов/систем и поставщиков услуг требования, предъявляемые с целью обеспечения высокого уровня кибербезопасности и защиты данных систем, устанавливаемых на транспортных средствах. Они могут использовать альтернативные подходы при условии, что такие подходы доказуемо обеспечивают по меньшей мере эквивалентный уровень безопасности.

1.5 Настоящие руководящие положения следует рассматривать в качестве временного руководства до завершения ведущихся исследований и совместных разработок, а также подготовки более подробных и согласованных на глобальном уровне требований к кибербезопасности и защите данных.

1.6 Настоящие руководящие положения послужат основой для разработки в рамках правил ООН предписаний, направленных на обеспечение кибербезопасности и защиты данных.

1.7 Настоящие руководящие положения не затрагивают существующее законодательство о защите данных. Они не направлены на уменьшение или увеличение содержания законодательных норм о защите данных.

2. Область применения

2.1 В настоящих руководящих положениях рассматриваются меры для подключенных транспортных средств и транспортных средств с ТАВ в плане кибербезопасности и защиты данных.

3. Определения

3.1 (Зарезервирован)

3.2 "*Подключенное транспортное средство*" означает транспортное средство с установленным на нем устройством, предназначенным для обеспечения беспроводной связи или коммуникации – возможно в связи с технологиями автоматизированного вождения – с внешними устройствами, автомобилями, сетями или сервисами.

3.3 "*Кибербезопасность*" означает сохранение конфиденциальности, целостности и доступности информации в "киберпространстве", т.е. в сложной среде, создаваемой в результате взаимодействия людей, программного обеспечения и сервисов (например, в Интернете) через подключенные к ней технические устройства и сети, которая не существует в какой-либо физической форме.

3.4 "*Защита данных*" означает право физического лица на уважение его личной и семейной жизни, жилища и сообщений в связи с обработкой персональных данных.

3.5 "*Субъект данных*" означает физическое лицо, являющееся субъектом персональных данных (например, владелец или водитель транспортного средства).

3.6 "*Защита данных по умолчанию*" означает обязанность оператора осуществлять технические и организационные меры, обеспечивающие по умолчанию обработку только тех персональных данных, которые необходимы для достижения каждой конкретной цели обработки.

3.7 "*Защита данных специальная*" означает обязанность оператора осуществлять технические и организационные меры, адаптированные к действиям оператора по обработке и направленные на обеспечение принципов защиты прав субъектов данных путем снижения вероятности и степени риска для их личной и семейной жизни, жилища и сообщений.

4. Предъявляемые руководящими положениями требования

Для подключенных транспортных средств и транспортных средств с ТАВ должны приниматься меры обеспечения кибербезопасности и защиты данных, и они должны отвечать нижеизложенным требованиям.

4.1 Общие положения

a) Должно уважаться право каждого человека на неприкосновенность частной жизни и сообщений.

b) Обработка персональных данных должна вестись законным, справедливым и транспарентным по отношению к субъекту данных образом.

c) Автопроизводители, поставщики компонентов/систем и поставщики услуг должны соблюдать принципы защиты данных по умолчанию и специальной защиты данных (см. определения в пунктах 3.6 и 3.7).

d) Автопроизводители, поставщики компонентов/систем и поставщики услуг должны обеспечивать надлежащую защиту как технических конструкций, так и данных и процессов от манипулирования и незаконного использования.

e) В целях предотвращения несанкционированного доступа к транспортным средствам через "киберпространство" автопроизводители, поставщики компонентов/систем и поставщики услуг должны обеспечивать надежное шифрование данных и сообщений.

f) Применительно к системе необходимо предусмотреть возможность проверки мер, принятых автопроизводителями, поставщиками компонентов/систем и поставщиками услуг для обеспечения кибербезопасности и защиты данных, путем независимого санкционированного аудита.

4.2 Защита данных

4.2.1 Принцип обработки персональных данных законным, справедливым и транспарентным образом означает, что необходимо, в частности:

a) уважать личность и неприкосновенность частной жизни субъекта данных;

b) не допускать дискриминации субъектов данных на основании их персональных данных;

c) учитывать разумные ожидания субъектов данных в отношении транспарентности и контекста обработки данных;

d) сохранять целостность и надежность систем информационных технологий и, в частности, не осуществлять тайных манипуляций при обработке данных;

e) учитывать преимущества обработки данных в условиях свободы потока информации, коммуникации и инноваций, причем субъекты данных должны соглашаться на обработку персональных данных, продиктованную превалирующими общественными интересами;

f) обеспечивать сохранение данных об индивидуальной мобильности, руководствуясь соображениями необходимости и целевого использования.

4.2.2 Необходимо использовать технологии анонимизации и псевдонимизации данных.

Субъекты данных должны получать полную информацию о том, какие данные, для каких целей и кем собираются и обрабатываются в процессе внедрения подключенных транспортных средств и транспортных средств с ТАВ. Субъекты данных должны давать свое информированное и добровольное согласие на сбор и обработку данных.

4.2.3 Сбор и обработка персональных данных ограничиваются данными, актуальными в конкретном контексте их сбора. Если применимо, то субъект данных имеет право отозвать свое согласие, если речь идет о функциях, не являющихся необходимыми для эксплуатации его/ее транспортного средства или обеспечения безопасности дорожного движения.

4.2.4 Кроме того, должны осуществляться надлежащие технические и организационные меры и процедуры, призванные обеспечить неприкосновенность частной жизни субъекта данных как при определении способов обработки, так и во время обработки. В конструкцию систем обработки данных, устанавливаемых на транспортных средствах, должна быть заложена функция защиты данных, т.е. при планировании компонентов ("специальная конфиденциальность") и в процессе разработки основных заводских настроек ("конфиденциальность по умолчанию") надлежит учитывать аспекты кибербезопасности и защиты данных.

4.3 Защита

4.3.1 С учетом требований, связанных с обеспечением безопасности подключенных транспортных средств и транспортных средств, оснащенных ТАВ, к важнейшим электрическим и электронным компонентам или системам транспортных средствах должны применяться стандарты функциональной безопасности, например ИСО 26262.

4.3.2 Подключение и связь подключенных транспортных средств и транспортных средств с ТАВ:

a) не должны – без принятия соответствующих мер – влиять на генерирование внутренними устройствами и системами внутренней информации, необходимой для контроля над транспортным средством;

b) должны проектироваться таким образом, чтобы не допускать мошеннических действий с программным обеспечением подключенных транспортных средств и транспортных средств с ТАВ, а также мошеннического доступа к бортовой информации в результате кибератак по каналам:

i) беспроводного подключения;

ii) проводного подключения через порт диагностики и т.д.;

c) должны предусматривать меры обеспечения безопасного режима на случай сбоя в работе системы, например за счет дублирования в системе.

4.3.3 В случае обнаружения подключенными транспортными средствами и транспортными средствами с ТАВ мошеннических действий, совершаемых путем кибератаки, система должна предупредить водителя и, при необходимости, контролировать безопасность транспортного средства в соответствии с вышеуказанными требованиями.

4.4 Безопасность

4.4.1 Для защиты подключенных транспортных средств и транспортных средств с ТАВ необходимы поддающиеся проверке меры безопасности, соответствующие стандартам безопасности (например, серии ИСО 27000, ИСО/МЭК 15408).

4.4.2 Для подключенных транспортных средств и транспортных средств с ТАВ должны быть предусмотрены:

a) меры защиты целостности информации, обеспечивающие, например, безопасное обновление программного обеспечения;

b) надлежащие меры контроля криптографических ключей.

4.4.3 Целостность внутренних сообщений между контроллерами внутри подключенных транспортных средств и транспортных средств с ТАВ должна быть защищена, например, путем аутентификации.

4.4.4 Онлайновые сервисы для удаленного доступа к подключенным транспортным средствам и транспортным средствам с ТАВ должны предусматривать строгую процедуру взаимной аутентификации и обеспечивать защищенность обмена сообщениями (защита конфиденциальности и целостности) между заинтересованными субъектами".

II. Справочная информация и административное предложение

A. Справочная информация

1. В рамках настоящих руководящих положений основное внимание уделяется подключенным транспортным средствам и транспортным средствам с ТАВ.

2. В связи с переходом к цифровым технологиям в области мобильности и сопутствующим ему увеличением объема данных к безопасности транспортных средств и инфраструктуре, а также к защите личных прав предъявляются новые требования. Следовательно, необходимо сформулировать четкие требования в отношении кибербезопасности и защиты данных для подключенных транспортных средств и транспортных средств с ТАВ.

3. Подключенные транспортные средства и транспортные средства с ТАВ должны функционировать безопасно и надежно на территориях, не ограниченных национальными границами. Права на данные о личной мобильности должны четко регулироваться.

4. Цель – обеспечить защиту транспортных средств от внешнего вмешательства и манипулирования. К защите данных применяются принципы глобального права о конфиденциальности данных.

5. Необходимые шаги по обеспечению кибербезопасности и защиты данных должны проходить проверку, например проверку системы внешними организациями.

B. Административное предложение

6. Настоящие руководящие положения касаются конструкции транспортных средств, содержат информацию о нормативных текстах, применимых к конструкции транспортных средств, и нацелены на повышение уровня безопасности и охрану окружающей среды. Цель данных руководящих положений совпадает с целью, сформулированной в Сводной резолюции о конструкции транспортных средств (СР.3). Предлагается включить текст настоящих руководящих положений (раздел I) в СР.3 в качестве нового приложения 6.