|  |  |  |
| --- | --- | --- |
|  | Организация Объединенных Наций | ECE/TRANS/WP.29/2023/87 |
| _unlogo | **Экономический и Социальный Совет** | Distr.: General1 September 2023RussianOriginal: English |

**Европейская экономическая комиссия**

Комитет по внутреннему транспорту

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

**Сто девяносто первая сессия**

Женева, 14–16 ноября 2023 года

Пункт 2.3 предварительной повестки дня

**Интеллектуальные транспортные системы
и координация деятельности, связанной
с автоматизированными транспортными средствами**

 Предложение по обновлению рекомендаций относительно кибербезопасности и обновления программного обеспечения автотранспортных средств

 Представлено Рабочей группой по автоматизированным/
автономным и подключенным транспортным средствам[[1]](#footnote-1)\*

Воспроизведенный ниже текст был принят Рабочей группой по автоматизированным/автономным и подключенным транспортным средствам (GRVA) на ее шестнадцатой сессии (см. ECE/TRANS/WP.29/GRVA/16, п. 53). Он представляет собой предложение по поправкам к документу ECE/TRANS/
WP.29/2022/60, основанное на неофициальном документе GRVA-16-15. Этот текст представляется Всемирному форуму для согласования правил в области транспортных средств (WP.29) и Административному комитету (AC.1) для рассмотрения на их сессиях в ноябре 2023 года.

*Часть I — Введение* изменить следующим образом:

«1. Отдельные лица и организации, причастные к разработке, производству или сборке автотранспортных средств, должны внести свою лепту в обеспечение кибербезопасности автомобиля.

2. Настоящий документ призван служить для Договаривающихся сторон Соглашения 1998 года в качестве руководства при разработке правил или законодательства по кибербезопасности автотранспортных средств и/или правил либо законодательства, касающихся обновления программного обеспечения транспортного средства и порядка установки обновленных версий. Целью руководства является обеспечение согласованного подхода к введению таких правил или такого законодательства. Поэтому изложенные в настоящем документе технические требования в максимально возможной степени приближены к требованиям правил № 155 и № 156 ООН, которые распространяются на Договаривающиеся стороны Соглашения 1958 года и касаются кибербезопасности и обновления программного обеспечения соответственно. Дополнительные ссылки в скобках указывают на соответствующий(е) раздел(ы) конкретных Правил.

В документе приводится перечень технических требований, предъявляемых как к транспортному средству, так и к системам управления. Что касается технических требований к системам управления, то перечисляются требования, хотя и носящие по отношению к транспортному средству сторонний характер, введение которых все же необходимо для эффективного управления кибербезопасностью транспортного средства в течение всего срока его эксплуатации, равно как и для обеспечения надлежащей оценки и защищенности обновленных версий программного обеспечения до их установки на транспортное средство.

Рекомендуется, чтобы при выработке правил или законодательства в полной мере учитывались как минимум технические требования, относящиеся к транспортному средству. По возможности следует также вводить требования к системе управления. В тех случаях, когда принять требования, касающиеся системы управления, в рамках правил или законодательства не представляется возможным, предлагается отразить их в национальном руководстве для изготовителей автомобилей.

Применительно к этим требованиям в документе не оговорены ни критерии приемлемости, ни критерии испытания.

Упомянутые в настоящем документе этапы жизненного цикла транспортного средства четко не определены; они подлежат установлению в правилах или законодательстве. Отраслевые рекомендации по всем соответствующим этапам можно найти в международных стандартах, например ISO/SAE 21434, ISO PAS 5112
и ISO 24089. Однако следует отметить, что «этапом после производства» охватываются все аспекты уже после изготовления транспортного средства, причем два важнейших, на которые необходимо обратить внимание, — это окончание срока службы транспортного средства (именуемое также как «вывод из эксплуатации») и истечение срока обеспечения кибербезопасности транспортного средства. Поскольку Соглашение 1998 года рассчитано на применение в контексте самых различных систем нормативного и правового регулирования, неофициальная рабочая группа по кибербезопасности и беспроводной установке обновлений не определила в настоящем документе минимальный срок обеспечения кибербезопасности транспортных средств.

В настоящем документе излагается метод, позволяющий управлять информацией о конфигурации программного обеспечения и аппаратных средств, особенно применительно к системам транспортного средства, предусмотренным правилами или законодательством, и трактовать ее для целей сертификации транспортного средства. Благодаря использованию присвоенного идентификатора (например, ИНПО ПX, как он определен в Правилах № 156 ООН), дающего представление о конфигурации программного обеспечения и аппаратных средств той или иной конкретной системы, можно понять, в каких случаях обновление программного обеспечения повлияет на сертификацию данной системы, поскольку — когда это произойдет — присвоенный идентификатор должен измениться. Чтобы этот метод работал, изготовитель транспортного средства должен быть в состоянии представить информацию об аппаратном и программном обеспечении, обозначенным данным присвоенным идентификатором. Применительно к конкретному транспортному средству должна иметься возможность определить, какое именно программное обеспечение установлено на нем, с тем чтобы проверить, соответствует ли оно программному обеспечению, обозначенному присвоенным идентификатором».

*Приложение 1, часть A, таблица A1, пункт 4.3.2, позицию 4.1* изменить следующим образом:

|  |  |
| --- | --- |
| *Высокоуровневые и подуровневые описания уязвимости/угрозы* | *Пример уязвимости или метода атаки* |
| … | … | … | … | … |
| 4.3.2 Угрозы в отношении транспортных средств, касающиеся их каналов передачи данных | 4 | Умышленное искажение сообщений или данных, полученных транспортным средством | 4.1 | **Спуфинг сообщений** в результате атаки путем подмены участника (например, сообщений массового оповещения или координационных сообщений V2X-связи, сообщений ГНСС и т. д.) |
| … | … |
| … | … | … | … | … |

*Приложение 1, часть B, таблица B1, ссылка на таблицу A1, позицию 4.1* изменить следующим образом:

| *Ссылка на таблицу A1* | *Угрозы, связанные с «Каналами передачи данных транспортных средств»* | *Ссылка* | *Смягчение последствий* |
| --- | --- | --- | --- |
| 4.1 | Спуфинг сообщений (например, сообщений массового оповещения или координационных сообщений V2X-связи, сообщений ГНСС и т. д.) в результате атаки путем подмены участника  | M10 | Транспортное средство проверяет подлинность и целостность сообщений, которые оно получает |
| … | … | … | … |

1. \* В соответствии с программой работы Комитета по внутреннему транспорту на 2023 год, изложенной в предлагаемом бюджете по программам на 2023 год (A/77/6 (разд. 20), п. 20.6), 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)