Организация Объединенных Наций ECE/TRANS/WP.29/2022/60

Экономический и Социальный Совет

Distr.: General
12 April 2022
Russian
Original: English

Европейская экономическая комиссия

Комитет по внутреннему транспорту

Всемирный форум для согласования правил в области транспортных средств

Сто восемьдесят седьмая сессия
Женева, 21–24 июня 2022 года
Пункт 2.3 предварительной повестки дня
Интеллектуальные транспортные системы и координация деятельности, связанной с автоматизированными транспортными средствами

Предложение о рекомендациях по единообразным предписаниям, касающимся кибербезопасности и обновления программного обеспечения

Представлено Рабочей группой по автоматизированным/автономным и подключенным транспортным средствам*

Воспроизведенный ниже текст был принят Рабочей группой по автоматизированным/автономным и подключенным транспортным средствам (GRVA) на ее двенадцатой сессии (см. ECE/TRANS/WP.29/GRVA/12, п. 47). В его основу положен документ ECE/TRANS/WP.29/GRVA/2022/5. Он представляется Всемирному форуму для согласования правил в области транспортных средств (WP.29) для рассмотрения на его сессии в июне 2022 года.

* В соответствии с программой работы Комитета по внутреннему транспорту на 2022 год, изложенной в предлагаемом бюджете по программам на 2022 год (A/76/6 (часть V, разд. 20), п. 20.76), Всемирный форум будет разрабатывать, согласовывать и обновлять правила ООН в целях повышения эффективности транспортных средств. Настоящий документ представлен в соответствии с этим мандатом.

I. Предложение по рекомендациям относительно кибербезопасности и обновления программного обеспечения автотранспортных средств

A. Часть I — Введение

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 ООН № 155 и № 156, которые распространяются на Договаривающиеся стороны Соглашения 1958 года и касаются кибербезопасности и обновления программного обеспечения соответственно. Дополнительные ссылки в скобках указывают на соответствующий(ие) 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 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 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, R_XSWIN, 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 предоставить 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.

B. Часть II

1. Системы управления

1.1 Система управления кибербезопасностью

1.1.1 Изготовитель транспортного средства должен располагать системой, обеспечивающей управление кибербезопасностью на следующих этапах *(Правила № 155 ООН, пункт 7.2.2.1)*:

a) этап разработки;

b) этап производства; и

c) этап после производства.

1.1.2 В рамках системы управления кибербезопасностью охватываются процессы, связанные с *(Правила № 155 ООН, пункт 7.2.2.2)*:

a) управлением системой кибербезопасности на организационном уровне;

b) выявлением рисков, которым подвергаются транспортные средства, включая рассмотрение угроз, указанных в части A приложения 1, и других соответствующих угроз;

c) оценкой, классификацией и обработкой выявленных рисков;

d) удостоверением в том, что выявленные риски устраняются надлежащим образом;

e) проверкой кибербезопасности транспортного средства;

f) обеспечением постоянного обновления оценки рисков;

g) мониторингом кибератак, киберугроз и факторов уязвимости транспортного средства, их обнаружением и реагированием на них;

h) оценкой того, являются ли принимаемые меры кибербезопасности по-прежнему эффективными в свете новых киберугроз или факторов уязвимости, которые были выявлены; и

i) предоставлением данных с целью поддержки анализа предпринятых попыток проведения кибератак или успешных кибератак.

1.1.3 Система управления кибербезопасностью должна обеспечивать смягчение в разумные сроки последствий выявленных киберугроз и факторов уязвимости, требующих реагирования со стороны изготовителя *(Правила № 155 ООН, пункт 7.2.2.3)*.

1.1.4 Процессы, используемые в рамках системы управления кибербезопасностью, должны обеспечивать непрерывный мониторинг, указанный в подпункте g) пункта 1.1.2, и включают *(Правила № 155 ООН, пункт 7.2.2.4)*:

a) транспортные средства на местах; и

b) возможности анализа и обнаружения киберугроз, факторов уязвимости и кибератак на основе данных о транспортном средстве и журналов учета использования транспортного средства. Эти возможности используются с соблюдением права владельцев и водителей транспортных средств на неприкосновенность частной жизни, особенно в том, что касается согласия.

1.1.5 Система управления кибербезопасностью должна регулировать связанные с кибербезопасностью аспекты взаимозависимости, которая может существовать с поставщиками изделий и услуг, с которыми заключены соответствующие контракты, или с его суборганизациями *(Правила № 155 ООН, пункт 7.2.2.5)*.

1.2 Система управления обновлением программного обеспечения

1.2.1 В рамках системы управления обновлением программного обеспечения охватываются процессы, связанные с:

a) документированием информации, относящейся к обновлению программного обеспечения *(Правила № 156 ООН, пункт 7.1.1.1)*;

b) надежным хранением информации, задокументированной согласно подпункту a) пункта 1.2.1 *(Правила № 156 ООН, пункт 7.1.1.1)*;

c) предоставлением соответствующим органам по запросу информации, задокументированной согласно подпункту a) пункта 1.2.1 *(Правила № 156 ООН, пункт 7.1.1.1)*;

d) однозначной идентификацией информации о первоначальной и всех обновленных версиях программного обеспечения, установленной(ых) на аппаратной части систем транспортного средства, указанных в правилах или законодательстве, включая данные проверки целостности, а также соответствующих аппаратных компонентов *(Правила № 156 ООН, пункт 7.1.1.2)*;

e) получением — причем как до, так и после установки обновленной версии, — доступа к информации относительно любых присвоенных идентификаторов, несущих информацию об установленном на транспортном средстве программном обеспечении, и ее обновлением, включая возможность обновления информации о версиях программного обеспечения и данных проверки целостности всего соответствующего программного обеспечения с присвоенным в каждом случае идентификатором *(Правила № 156 ООН, пункт 7.1.1.3)*;

f) удостоверением — при наличии присвоенных идентификаторов, несущих информацию об установленном на транспортном средстве программном обеспечении, — в том, что версия(и) программного обеспечения, установленная(ые) на аппаратной части системы транспортного средства, соответствует(ют) версиям, которые по своим параметрам аналогичны программному обеспечению с присвоенным идентификатором *(Правила № 156 ООН, пункт 7.1.1.4)*;

g) выявлением взаимосвязей между системой с обновленным программным обеспечением и другой(ими) системой(ами) *(Правила № 156 ООН, пункт 7.1.1.5)*;

h) четким определением «целевых» транспортных средств, на которые надлежит установить обновленную версию программного обеспечения *(Правила № 156 ООН, пункт 7.1.1.6)*;

i) подтверждением совместимости обновленного программного обеспечения с конфигурацией «целевого(ых)» транспортного(ых) средства (средств) до начала процесса установки обновления, включая оценку на предмет совместимости последней известной конфигурации программного/аппаратного обеспечения «целевого(ых)» транспортного(ых) средства (средств) и подлежащей установке обновленной версии программного обеспечения *(Правила № 156 ООН, пункт 7.1.1.7)*;

j) определением того, скажется ли обновление программного обеспечения на какой-либо системе, предусмотренной правилами или законодательством, в том числе, не повлияет ли обновление программного обеспечения на любые параметры, определяющие системы, затрагиваемые таким обновлением, не произойдет ли модификация этих параметров вследствие обновления и не приведет ли обновление к изменению каких-либо параметров, предусмотренных правилами или законодательством *(Правила № 156 ООН, пункт 7.1.1.8)*;

k) определением того, сопряжено ли обновление программного обеспечения с добавлением, изменением или активацией любой(ых) функции(й), которая(ые) отсутствовала(и) либо не активировалась(ись) при сертификации транспортного средства в соответствии с правилами или законодательством, и не приводит ли обновление к изменению или исключению каких-либо других параметров или функций, предусмотренных правилами или законодательством. При этом принимают во внимание следующее:

   i) возникнет ли необходимость внесения изменений в регламентируемую (согласно правилам или законодательству) информацию, касающуюся транспортного средства;

   ii) позволяют ли результаты предыдущих испытаний, проведенных в соответствии с правилами или законодательством, объективно судить о характеристиках транспортного средства после произведенной модификации;

   iii) повлияет ли какое-либо изменение функций транспортного средства на сертификацию данного транспортного средства в соответствии с правилами или законодательством *(Правила № 156 ООН, пункт 7.1.1.9)*;

l) определением того, скажется ли обновление программного обеспечения на любой другой системе, требуемой для безопасной и бесперебойной эксплуатации транспортного средства, и сопряжено ли обновление программного обеспечения с расширением или изменением функциональных возможностей транспортного средства по сравнению с теми, которыми оно обладало на момент сертификации *(Правила № 156 ООН, пункт 7.1.1.10)*;

m) информированием пользователя транспортного средства об установленных обновленных версиях *(Правила № 156 ООН, пункт 7.1.1.11)*.

1.2.2 По каждому обновлению изготовитель транспортного средства регистрирует и хранит у себя следующую информацию *(Правила № 156 ООН, пункт 7.1.2)*:

a) документы с описанием используемых изготовителем данного транспортного средства процедур обновления программного обеспечения и с указанием ссылок на любые соответствующие стандарты *(Правила № 156 ООН, пункт 7.1.2.1)*;

b) документы с описанием конфигурации любых систем, предусмотренных правилами или законодательством, до и после обновления, причем с указанием применительно к аппаратной и программной (включая версии программного обеспечения) частям конкретных идентификаторов, а также любых соответствующих параметров транспортного средства или системы *(Правила № 156 ООН, пункт 7.1.2.2)*;

c) при наличии присвоенных идентификаторов, несущих информацию о программном обеспечении электронных систем управления, поддерживающих системы или функции транспортного средства, предусмотренные правилами или законодательством, — проверяемый журнал учета с описанием всех видов соответствующего программного обеспечения, которым присвоен идентификатор, до и после установки обновления. Он должен включать информацию о версиях программного обеспечения, включая данные проверки их целостности, применительно ко всему соответствующему программному обеспечению *(Правила № 156 ООН, пункт 7.1.2.3)*;

d) документы с указанием «целевых» транспортных средств, на которых надлежит установить обновленную версию, и подтверждением совместимости самой последней известной конфигурации этих транспортных средств с обновленной версией программного обеспечения *(Правила № 156 ООН, пункт 7.1.2.4)*;

e) документы по всем обновленным версиям программного обеспечения с указанием следующего *(Правила № 156 ООН, пункт 7.1.2.5)*:

i) цель обновления;

ii) системы или функции транспортного средства, которые могут оказаться затронутыми обновлением программного обеспечения;

iii) те (возможные) системы или функции из числа перечисленных в подпункте b), наличие которых требуется согласно Правилам или законодательству (если таковые имеются);

iv) если это применимо, затрагивает ли обновление программного обеспечения соблюдение требований, предусмотренных любыми соответствующими правилами или любым соответствующим законодательством, указанными в части 3;

v) сказывается ли обновление программного обеспечения на каком-либо указанном в правилах или законодательстве параметре транспортного средства или системы транспортного средства;

vi) если это применимо, было ли запрошено официальное утверждение обновленной версии у соответствующего национального органа;

vii) каков порядок и условия установки обновленной версии программного обеспечения;

viii) подтверждение того, что обновление программного обеспечения будет проводиться безопасным и надежным образом;

ix) подтверждение того, что обновлению программного обеспечения предшествовали надлежащие процедуры проверки и аттестации.

1.2.3 Изготовитель транспортного средства предоставляет в распоряжение соответствующих национальных органов информацию, указанную в пунктах 1.2.2.3 и 1.2.2.4 *(Правила № 156 ООН, пункт 7.1.1.12)*.

1.2.4 Что касается защищенности обновленных версий программного обеспечения, то изготовитель транспортного средства налаживает и поддерживает процессы, связанные с *(Правила № 156 ООН, пункт 7.1.3)*:

a) обеспечением надлежащей защищенности обновленных версий программного обеспечения от несанкционированного манипулирования на этапе до начала процесса установки обновления *(Правила № 156 ООН, пункт 7.1.3.1)*;

b) обеспечением надлежащей защищенности всех процессов обновления от возможных нарушений, в том числе на стадии разработки программы для обновления системных драйверов и *(Правила № 156 ООН, пункт 7.1.3.2)*;

c) надлежащей проверкой и аттестацией функциональных возможностей программного обеспечения и надлежащим программированием установленных на транспортном средстве программных средств *(Правила № 156 ООН, пункт 7.1.3.3)*.

1.2.5 В случае транспортных средств, позволяющих осуществлять беспроводную установку обновленных версий программного обеспечения, изготовитель транспортного средства налаживает и поддерживает процессы, связанные с *(Правила № 156 ООН, пункт 7.1.4)*:

a) оценкой того, что беспроводное обновление программного обеспечения, если оно производится в состоянии движения, не приведет к созданию угрозы для безопасности и *(Правила № 156 ООН, пункт 7.1.4.1)*;

b) обеспечением того, чтобы беспроводная установка обновленной программной версии, при которой для завершения процесса обновления требуется конкретная специализированная или сложная операция (например, повторная калибровка после программирования сенсорного устройства), допускалась исключительно в присутствии соответствующего лица, которое обладает необходимой квалификацией, позволяющей ему произвести данную операцию или держать под контролем весь процесс *(Правила № 156 ООН, пункт 7.1.4.2)*.

2. Требования в отношении транспортного средства

2.1 Требования к кибербезопасности

2.1.1 Изготовитель идентифицирует критические элементы транспортного средства и проводит исчерпывающую оценку рисков для данного транспортного средства, а также надлежащим образом обрабатывает

выявленные риски/управляет выявленными рисками *(Правила № 155 ООН, пункт 7.3.3)*.

2.1.1.1 При оценке рисков учитываются отдельные элементы транспортного средства и их взаимодействия.

2.1.1.2 В ходе оценки рисков учитываются взаимодействия с внешними системами.

2.1.1.3 При оценке рисков изготовитель транспортного средства учитывает риски, связанные со всеми угрозами, указанными в части A приложения 1, а также любой другой соответствующий риск.

2.1.1.4 При оценке рисков учитываются все риски, связанные с поставщиками *(Правила № 155 ООН, пункт 7.3.2)*.

2.1.2 Изготовитель защищает транспортное средство от рисков, выявленных в ходе оценки рисков *(Правила № 155 ООН, пункт 7.3.4)*.

2.1.2.1 Для защиты транспортного средства принимаются надлежащие и соразмерные меры по смягчению последствий.

2.1.2.2 Осуществляемые меры по смягчению последствий включают все меры по смягчению последствий, о которых говорится в частях B и C приложения 1 и которые касаются выявленных рисков. Если же та или иная мера по смягчению последствий, упомянутая в части B или C приложения 1, не имеет отношения к выявленному риску или является недостаточной, изготовитель транспортного средства обеспечивает осуществление какой-либо другой соответствующей меры по смягчению последствий.

2.1.2.3 Изготовитель транспортного средства проводит надлежащие и достаточные испытания для проверки эффективности принятых мер безопасности *(Правила № 155 ООН, пункт 7.3.6)*.

2.1.3 Изготовитель транспортного средства принимает надлежащие и соразмерные меры для обеспечения безопасности специальных объектов (если таковые предусмотрены) в целях хранения и реализации программного обеспечения, услуг, приложений или данных в интересах вторичного рынка применительно к данному транспортному средству *(Правила № 155 ООН, пункт 7.3.5)*.

2.1.4 Изготовитель транспортного средства принимает в отношении данного транспортного средства соответствующие меры с целью *(Правила № 155 ООН, пункт 7.3.7)*:

a) обнаружения и предотвращения кибератак на транспортное средство;

b) поддержки возможностей мониторинга, осуществляемого изготовителем транспортного средства для обнаружения угроз, факторов уязвимости и кибератак, относящихся к данному транспортному средству;

c) предоставления возможностей криминалистической экспертизы данных для анализа предпринятых попыток проведения кибератак или успешных кибератак.

2.1.5 Криптографические модули должны соответствовать согласованным стандартам. Если используемые криптографические модули не соответствуют согласованным стандартам, то изготовитель транспортного средства должен обосновать их использование *(Правила № 155 ООН, пункт 7.3.8)*.

2.2 Требования в отношении установки обновленных программных версий

2.2.1 Должна обеспечиваться защита подлинности контента и целостности обновленных версий программного обеспечения во избежание их возможного взлома и недопущения установки неверных версий (*Правила № 156 ООН, пункт 7.2.1.1*).

2.2.2 При использовании присвоенных идентификаторов, несущих информацию о программном обеспечении электронных систем управления, поддерживающих системы или функции транспортного средства, предусмотренные правилами или законодательством, должна обеспечиваться однозначная идентификация каждого присвоенного идентификатора. Внесение изготовителем транспортного средства изменений в соответствующее программное обеспечение, сказывающихся на сертификации транспортного средства или его систем, влечет за собой обновление присвоенного идентификатора *(Правила № 156 ООН, пункт 7.2.1.2.1)*.

2.2.3 Версии программного обеспечения электронных систем управления, поддерживающих системы или функции транспортного средства, предусмотренные правилами или законодательством, либо присвоенные идентификаторы, несущие информацию о таком программном обеспечении, должны легко считываться по стандартной процедуре через электронно-коммуникационный интерфейс на транспортном средстве *(Правила № 156 ООН, пункт 7.2.1.2.2)*.

2.2.4 Должна обеспечиваться защита информации о конфигурации установленного на транспортном средстве программного обеспечения от несанкционированного изменения *(Правила № 156 ООН, пункт 7.2.1.2.3)*.

2.2.5 Дополнительные требования при беспроводной (БП) установке обновлений *(Правила № 156 ООН, пункт 7.2.2)*

2.2.5.1 При сбое в процессе обновления либо его прерывании транспортное средство должно обеспечивать восстановление соответствующих систем с возвратом к исходной версии программного обеспечения или же осуществлять перевод в безопасный режим после сбоя в процессе обновления либо его прерывания.

2.2.5.2 Установка обновленных версий программного обеспечения производится только тогда, когда транспортное средство располагает достаточной мощностью для завершения процесса обновления (в том числе необходимой для возможного восстановления с возвратом к исходной версии программного обеспечения или же перевода транспортного средства в безопасный режим).

2.2.5.3 Если установка обновленной версии программного обеспечения может отразиться на безопасности транспортного средства, то состояние данного транспортного средства должно позволять установить обновление безопасным образом.

2.2.5.4 Должна обеспечиваться возможность информирования пользователя транспортного средства об обновлении на этапе до установки обновленной версии. Указанная информация должна содержать:

a) цель обновления; она может указывать на критичность обновленной версии, а также для чего оно служит: для отзыва автомобилей или обеспечения безопасности и/или защиты;

b) любые изменения, привносимые в результате обновления в функции транспортного средства;

c) расчетное время завершения установки обновленной версии;

d) любые функциональные возможности транспортного средства, блокируемые на этапе установки и активации обновления;

e) любые инструкции, позволяющие пользователю транспортного средства установить обновление безопасным образом.

В случае пакетов обновлений с идентичным контентом единый блок информации может относиться ко всему пакету.

2.2.5.5 Если установка обновления во время движения может поставить безопасность под угрозу, то транспортное средство должно:

a) либо исключать возможность движения в процессе установки обновления;

b) либо находиться в состоянии, исключающем возможность использования водителем любой функции транспортного средства, которая сказалась бы на безопасности автомобиля или успешной установке обновления.

2.2.5.6 После установки обновленной версии:

a) должна обеспечиваться возможность информирования пользователя транспортного средства об успешной (или безуспешной) установке обновления;

b) должна обеспечиваться возможность информирования пользователя транспортного средства об изменениях, внесенных в руководство по эксплуатации, и любых обновлениях к нему (если это применимо).

3. Определения

3.1 «*Кибербезопасность*» означает состояние, в котором дорожные транспортные средства и их функции защищены от киберугроз, которым могут подвергаться электрические или электронные компоненты.

3.2 «*Установка*» в контексте обновления программного обеспечения означает процесс установки и активации загруженного обновления.

3.3 «*Информация о конфигурации*» — это данные, дающие представление об установленных на транспортном средстве версиях программного обеспечения. Такие данные могут быть развернутыми или иметь вид идентификатора, присвоенного заданной конфигурации (т. е. R_XSWIN).

3.4 «*Данные проверки целостности*» означают представление цифровых данных, которые позволяют проводить сравнения в целях выявления ошибок или изменений в данных. Это может включать в себя контрольные суммы и значения хеширования.

3.5 «*Смягчение последствий*» означает соответствующую меру, которая позволяет изменить уровень риска.

3.6 «*Беспроводным (БП) способом*» означает любой метод беспроводной передачи данных в отличие от использования кабельного или иного локального соединения.

3.7 «*Риск*» означает вероятность того, что какая-либо угроза реализуется на практике вследствие уязвимостей того или иного транспортного средства и тем самым причинит вред организации или отдельному лицу.

3.8 «*Оценка риска*» означает всесторонний процесс выявления, распознавания и описания рисков (идентификация риска) в целях понимания характера риска и определения его уровня (анализ риска) и сопоставления результатов анализа риска с критериями риска в порядке выяснения того факта, является ли данный риск и/или его масштаб приемлемым или допустимым (оценка риска).

3.9 «*Безопасное состояние*» означает режим работы в случае выхода из строя того или иного изделия в условиях необоснованного уровня риска.

3.10 «*Программное обеспечение*» означает компонент электронной системы управления в виде цифровой информации и соответствующих инструкций.

3.11 «*Обновление программного обеспечения*» означает соответствующий пакет, используемый для обновления программного обеспечения до новой версии, включая изменение параметров конфигурации.

3.12 «*Система*» означает соответствующий набор компонентов и/или подсистем, который воплощает в себе ту или иную функцию или функции.

3.13 «*Угроза*» означает потенциальную причину нежелательного инцидента, который может нанести ущерб системе, организации или отдельному лицу.

3.14 «*Пользователь транспортного средства*» означает лицо, эксплуатирующее транспортное средство или управляющее им, владельца транспортного средства, уполномоченного представителя или служащего оператора парка транспортных средств, уполномоченного представителя или сотрудника изготовителя транспортного средства либо квалифицированного технического специалиста.

3.15 «*Уязвимость*» означает слабость какого-либо материального объекта или средства смягчения последствий, которая дает возможность реализации одной или нескольких угроз.

Приложение 1

Перечень угроз и соответствующих мер по смягчению последствий

1. Настоящее приложение состоит из трех частей. В части A настоящего приложения описываются исходные данные об угрозах, факторах уязвимостях и методах атаки. В части B настоящего приложения описываются меры по смягчению последствий угроз, которые предназначены для типов транспортных средств. В части C описываются меры по смягчению последствий угроз, которые предназначены для зон, расположенных за пределами транспортных средств, например внутренних серверов.

2. Части A, B и C рассматриваются на предмет оценки рисков и мер по смягчению их последствий, которые должны применяться изготовителями транспортных средств.

3. Высокий уровень уязвимости и соответствующие примеры проиндексированы в части A. Та же система индексации используется и в таблицах, содержащихся в частях B и C, с целью увязать каждый случай атаки/фактор уязвимости с перечнем соответствующих мер по смягчению их последствий.

4. Анализ угроз должен также учитывать последствия возможных атак. Это может помочь определить степень риска и выявить дополнительные риски. Возможные последствия атак могут включать следующее:

a) нарушение безопасной работы транспортного средства;

b) отказ некоторых функций транспортного средства;

c) модификацию программного обеспечения, снижение эффективности;

d) модификацию программного обеспечения, но без последствий для эксплуатации;

e) нарушение целостности данных;

f) нарушение конфиденциальности данных;

g) утрату возможности вывода данных;

h) прочие последствия, включая преступные действия.

Часть A
Факторы уязвимости или методы атаки, связанные с угрозами

1. Высокоуровневые описания угроз и связанных с ними факторов уязвимости или методов атаки приведены в таблице A1.

Таблица A1
Перечень факторов уязвимости или методов атак, связанных с угрозами

Высокоуровневые и подуровневые описания уязвимости/угрозы			*Пример уязвимости или метода атаки*	
4.3.1 Угрозы в отношении внутренних серверов, связанных с транспортными средствами на местах	1	Внутренние серверы, используемые в качестве средства кибератаки на транспортное средство или извлечения данных	1.1	Злоупотребление привилегиями штатными сотрудниками (**внутренняя атака**)
			1.2	**Несанкционированный доступ через Интернет** к серверу (который возможен, например, в результате обхода системы защиты, не устраненных факторов уязвимости системы программного обеспечения, атаки методом использования языка структурированных запросов SQL или иными способами)
			1.3	**Несанкционированный физический доступ** к серверу (например, с помощью USB-накопителей или иных средств, подключаемых к серверу)
	2	Нарушение работы внутренних серверов, которое отрицательно сказывается на эксплуатации транспортного средства	2.1	**Атака на внутренний сервер, который прекращает работу**: она, например, не дает ему возможности взаимодействовать с транспортными средствами и оказывать услуги, которые нужны для их работы
	3	Относящиеся к транспортному средству данные, хранящиеся на внутренних серверах, утеряны или скомпрометированы («утечка данных»)	3.1	Злоупотребление привилегиями штатными сотрудниками (**внутренняя атака**)
			3.2	**Потеря информации в облаке**. Конфиденциальные данные могут быть потеряны из-за атак или аварий при хранении данных сторонними поставщиками облачных услуг
			3.3	**Несанкционированный доступ через Интернет к серверу** (который возможен, например, в результате обхода системы защиты, не устраненных факторов уязвимости системы программного обеспечения, атаки методом использования языка структурированных запросов SQL или иными способами)
			3.4	**Несанкционированный физический доступ к серверу** (например, с помощью USB-накопителей или иных средств, подключаемых к серверу)
			3.5	**Утечка информации** в результате непреднамеренного обмена данными (например, ошибки на уровне администрации)
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, 802.11p V2X в ходе формирования автоколонн, сообщения ГНСС и т. д.)
			4.2	**Атака Сибиллы** (для того, чтобы спуфировать другие транспортные средства, как будто на дороге много транспортных средств)
	5	Каналы передачи данных, используемые для осуществления несанкционированных	5.1	Каналы передачи данных допускают **внедрение кода**, например в коммуникационный канал может быть внедрен подложный двоичный код программного обеспечения

Высокоуровневые и подуровневые описания уязвимости/угрозы			*Пример уязвимости или метода атаки*	
		действий, удаления или внесения других изменений в бортовой код/данные транспортного средства	5.2	Каналы передачи данных допускают **манипулирование** бортовым кодом/данными транспортного средства
			5.3	Каналы передачи данных допускают **наложение других данных** на бортовой код/данные транспортного средства
			5.4	Каналы передачи данных допускают **стирание** бортового кода/данных транспортного средства
			5.5	Каналы передачи данных допускают внедрение данных/кода в систему транспортного средства (запись данных/кода)
	6	Каналы передачи данных допускают прием недостоверных/ненадежных сообщений или уязвимы в случае сеансов связи/атаки с повторным навязыванием сообщения	6.1	Прием информации из **ненадежного или недостоверного источника**
			6.2	Атака **через посредника**/перехват сеанса
			6.3	**Атака с повторным навязыванием сообщения**, например атака на коммуникационный шлюз позволяет злоумышленнику снизить эффективность программного обеспечения ЭБУ или встроенных программ шлюза
	7	Информацию можно легко раскрыть. Например, путем подслушивания сообщений или несанкционированного доступа к конфиденциальным файлам или папкам	7.1	**Перехват информации**/помехи в результате излучения/отслеживание сообщений
			7.2	Получение **несанкционированного доступа** к файлам или данным
	8	Атаки по каналам передачи данных в целях нарушения функций транспортного средства в виде отказа в обслуживании	8.1	**Отправка** большого количества ненужных **данных** в информационную систему транспортного средства, **чтобы она не могла предоставлять услуги** в обычном режиме
			8.2	**Атака методом переполнения**: с целью нарушить передачу данных между транспортными средствами злоумышленник может заблокировать передачу сообщений между транспортными средствами
	9	Пользователь со стороны может получить привилегированный доступ к системам транспортного средства	9.1	Пользователь со стороны может **получить привилегированный доступ**, например доступ с полномочиями суперпользователя
	10	Вирусы, занесенные в коммуникационную среду, могут инфицировать системы транспортного средства	10.1	**Вирус**, занесенный в коммуникационную среду, инфицирует системы транспортного средства
	11	Сообщения, полученные транспортным средством (например, X2V или диагностические сигналы) или переданные вместе с ним, содержат вредоносный контент	11.1	Вредоносные **внутренние** (например, местная контроллерная сеть — CAN) **сообщения**
			11.2	Вредоносные **сообщения V2X**, например сообщения «объект инфраструктуры — транспортное средство» или «транспортное средство — транспортное средство» (например, CAM, DENM)
			11.3	Вредоносные диагностические сигналы

Высокоуровневые и подуровневые описания уязвимости/угрозы			*Пример уязвимости или метода атаки*	
			11.4	Вредоносные **частные сообщения** (например, те, которые обычно направляются OEM или поставщиком компонента/системы/функции)
4.3.3 Угрозы в отношении транспортных средств, касающиеся их процедур обновления	12	Злоупотребление процедурами обновления или их нарушение	12.1	Нарушение **процедур обновления программного обеспечения по каналу беспроводной связи**. Это включает подделку программы обновления системы или встроенных программ
			12.2	Нарушение **процедур обновления локального/ физического программного обеспечения**. Это включает подделку программы обновления системы или встроенных программ
			12.3	**Манипулирование программным обеспечением до процесса обновления** (и, как следствие, его нарушение), хотя сам процесс обновления не нарушается
			12.4	**Нарушение** криптографических ключей провайдера программного обеспечения **с целью допустить неполноценное обновление**
	13	Возможность отказа в правомерных обновлениях	13.1	Атака в виде отказа в обслуживании сервера или сети с целью **воспрепятствовать обновлениям важнейшего программного обеспечения** и/или разблокировки конкретных функций пользователя
4.3.4 Угрозы транспортным средствам в связи с непреднамеренным и действиями человека, способствующими кибератаке	15	Правомерные субъекты способны принимать меры, которые могут невольно облегчить кибератаку	15.1	Невинная жертва (например, владелец, оператор или инженер по техническому обслуживанию) **путем обмана предпринимает действия** с целью непреднамеренной загрузки вредоносного ПО или проведения атаки
			15.2	**Заданные процедуры обеспечения** безопасности не соблюдаются
4.3.5 Угрозы транспортным средствам в отношении их внешних подключений и соединений	16	Манипулирование функциями подключения транспортного средства позволяет осуществить кибератаку: это может включать средства телематики; системы, которые дают возможность осуществления дистанционных операций; и системы, использующие средства беспроводной связи ближнего радиуса действия	16.1	Манипулирование **функциями, предназначенными для дистанционного управления системами**, такими как дистанционный ключ, иммобилизатор и уличная зарядка
			16.2	**Манипулирование средствами телематики транспортного средства** (например, измерением температуры грузов, требующих особого обращения, дистанционным открытием дверей грузового отделения)
			16.3	Помехи в работе **систем беспроводной связи ближнего радиуса действия** или датчиков
	17	Размещение программного обеспечения третьей стороной, например развлекательных прикладных программ, используемых в качестве одного из средств для атаки систем транспортных средств	17.1	**Поврежденные приложения** или приложения со слабой программной защитой, используемые в качестве метода атаки на системы транспортных средств
	18	Устройства, подключенные к внешним интерфейсам, например USB-порты, БД-порт, используемые в качестве средства атаки на	18.1	**Внешние интерфейсы**, такие как USB или другие порты, используемые в качестве точки атаки, например путем внедрения кода
			18.2	Программные средства инфицированы **вирусом**, занесенным в систему транспортного средства

Высокоуровневые и подуровневые описания уязвимости/угрозы			*Пример уязвимости или метода атаки*	
		системы транспортных средств	18.3	**Точки диагностического контроля (например, программные ключи, вставляемые в БД-порт)**, которые используются для облегчения атаки, например для манипулирования параметрами транспортного средства (напрямую или опосредованно)
4.3.6 Угрозы данным/коду транспортного средства	19	Извлечение данных/кода транспортного средства	19.1	Извлечение патентованного или собственного программного обеспечения из систем транспортного средства (**фальсификация** продукта)
			19.2	Несанкционированный доступ к такой **персональной информации владельца**, как удостоверение личности, платежные реквизиты, адресная книга, информации о местоположении, электронная идентификация транспортного средства и т. д.
			19.3	Извлечение криптографических ключей
	20	Манипулирование данными/кодом транспортных средств	20.1	Противоправные/несанкционированные изменения в **электронной идентификации транспортного средства**
			20.2	**Мошенничество с использованием персональных данных**. Например, если пользователь желает выдать себя за другое лицо при установлении связи с системами взимания автодорожных сборов или серверным приложением изготовителя
			20.3	Действия с целью **обхода систем мониторинга** (например, взлом/подделка/блокирование таких сообщений, как данные системы регистрации ODR или количество рейсов)
			20.4	Манипулирование данными в целях **фальсификации данных об управлении транспортным средством** (например, данных о пробеге, скорости, направлении движения и т. д.)
			20.5	Несанкционированные изменения **данных системы диагностики**
	21	Стирание данных/кода	21.1	Несанкционированное удаление **журналов регистрации системных событий**/манипулирование **журналами регистрации системных событий**
	22	Внедрение вредоносных программ	22.2	Внедрение **вредоносного программного обеспечения** или создание условий для злонамеренной работы вредоносных программ
	23	Введение в действие нового программного обеспечения или затирание существующего программного обеспечения	23.1	**Фабрикация программного обеспечения** системы контроля или информационный системы транспортного средства
	24	Нарушение работы систем или операций	24.1	**Отказ в обслуживании**: это, например, может быть инициировано во внутренней сети путем лавинного распространения данных по шине сети локальных контроллеров CAN или посредством провоцирования сбоев в ЭБУ вследствие большого количества сообщений

Высокоуровневые и подуровневые описания уязвимости/угрозы			*Пример уязвимости или метода атаки*	
	25	Манипулирование параметрами транспортного средства	25.1	Несанкционированный доступ в целях **фальсификации параметров конфигурации** основных функций транспортного средства, таких как данные о тормозах, пороговом уровне срабатывания подушки безопасности и т. д.
			25.2	Несанкционированный доступ в целях **фальсификации параметров зарядки**, таких как напряжение зарядки, расход энергии на подзарядку, температура батареи и т. д.
4.3.7 Потенциальные факторы уязвимости, которыми можно воспользоваться в случае недостаточной защиты или надежности	26	Криптографические технологии, которые могут быть нарушены или которые применяются недостаточно	26.1	Сочетание коротких **ключей шифрования данных** и длительных сроков их действия дает взломщикам возможность сломать шифровальный код
			26.2	Недостаточное использование шифровальных алгоритмов для защиты чувствительных систем
			26.3	Использование **криптографических алгоритмов**, которые уже устарели или устареют в скором времени
	27	Части или принадлежности компонентов, которые могут быть нарушены в целях создания возможности для атаки транспортных средств	27.1	**Аппаратное или программное обеспечение, разработанное таким образом, что оно создает возможность для атаки** или не удовлетворяет конструктивным критериям для прекращения атаки
	28	Разработка программного обеспечения или аппаратных средств, которая создает возможность возникновения факторов уязвимости	28.1	**Ошибки в программном обеспечении**. Наличие ошибок в программном обеспечении может явиться причиной возникновения потенциальных факторов уязвимости, которыми можно воспользоваться. Это особенно верно в том случае, если программное обеспечение не было протестировано с целью убедиться в том, что известного неудовлетворительного кода/ошибок нет, и снизить риск наличия неизвестного неудовлетворительного кода/ошибок
			28.2	**Использование остаточных устройств и материалов** после разработки (например, отладочных портов, портов JTAG, микропроцессоров, сертификатов разработки, паролей разработчиков и т. д.) может обеспечить доступ к ЭБУ или дать возможность взломщикам получить более высокий статус привилегий
	29	Дизайн сети, который допускает возникновение факторов уязвимости	29.1	**Лишние интернет-порты оставлены открытыми**, что обеспечивает доступ к сетевым системам
			29.2	Обход **разделения сети** для получения контроля. Конкретным примером является использование незащищенных шлюзов или точек доступа (например, шлюзы «грузовой автомобиль — прицеп») для обхода защиты и получения доступа к другим сегментам сети, что позволяет производить злоумышленные действия, такие как передача произвольных сообщений на шину сети локальных контроллеров (CAN)
	31	Может произойти непреднамеренная передача данных	31.1	Утечка информации. В случае **смены пользователя автомобиля** может произойти утечка персональных данных (например, если автомобиль продан или используется напрокат другими лицами)

Высокоуровневые и подуровневые описания уязвимости/угрозы			*Пример уязвимости или метода атаки*	
	32	Физическое манипулирование системами, которое может создать возможность для атаки	32.1	**Манипулирование электронной аппаратурой**, например установка на транспортное средство несанкционированной электронной аппаратуры, что создает возможность для проведения атаки через посредника **Замена санкционированной электронной аппаратуры** (например, датчиков) несанкционированной электронной аппаратурой **Манипулирование информацией**, собираемой датчиком (например, использование магнита для вмешательства в работу датчика, основанного на эффекте Холла и подключенного к коробке передач)

Часть B
Меры по смягчению последствий угроз, предназначенные для транспортных средств

1. Меры по смягчению последствий в случае «Каналов передачи данных транспортных средств»

Меры по смягчению последствий угроз, которые связаны с «Каналами передачи данных транспортных средств», перечислены в таблице B1.

Таблица B1
Смягчение последствий угроз, которые связаны с «Каналами передачи данных транспортных средств»

Ссылка на таблицу A1	*Угрозы, связанные с «Каналами передачи данных транспортных средств»*	*Ссылка*	*Смягчение последствий*
4.1	Спуфинг сообщений (например, 802.11p V2X в ходе формирования автоколонн, сообщения ГНСС и т. д.) в результате атаки путем подмены участника	M10	Транспортное средство проверяет подлинность и целостность сообщений, которые оно получает
4.2	Атака Сибиллы (для того, чтобы спуфировать другие транспортные средства, как будто на дороге много транспортных средств)	M11	В целях хранения криптографических ключей обеспечиваются соответствующие средства контроля защиты (например, использование аппаратных модулей безопасности)
5.1	Каналы передачи данных допускают внедрение кода/данных: например, в коммуникационный канал может быть внедрен подложный двоичный код программного обеспечения	M10 M6	Транспортное средство проверяет подлинность и целостность сообщений, которые оно получает В целях сведения рисков к минимуму защита систем обеспечивается ее конструкцией
5.2	Каналы передачи данных допускают манипулирование бортовым кодом/ данными транспортного средства	M7	В целях защиты данных/кода системы применяют соответствующие методы контроля за доступом и соответствующие конструктивные особенности
5.3	Каналы передачи данных допускают наложение других данных на бортовой код/данные транспортного средства		
5.4 21.1	Каналы передачи данных допускают стирание бортового кода/данных транспортного средства		
5.5	Каналы передачи данных допускают внедрение данных/кода в систему транспортного средства (запись данных/кода)		
6.1	Прием информации из ненадежного или недостоверного источника	M10	Транспортное средство проверяет подлинность и целостность сообщений, которые оно получает
6.2	Атака через посредника/перехват сеанса	M10	Транспортное средство проверяет подлинность и целостность сообщений, которые оно получает
6.3	Атака с повторным навязыванием сообщения, например атака на коммуникационный шлюз позволяет злоумышленнику снизить эффективность программного обеспечения ЭБУ или встроенных программ шлюза		
7.1	Перехват информации/помехи в результате излучения/отслеживание сообщений	M12	Конфиденциальные данные, передаваемые на транспортное средство или транспортным средством, подлежат соответствующей защите

Ссылка на таблицу A1	*Угрозы, связанные с «Каналами передачи данных транспортных средств»*	*Ссылка*	*Смягчение последствий*
7.2	Получение несанкционированного доступа к файлам или данным	M8	Заблокировать доступ неуполномоченному персоналу к персональным данным или важнейшим системным данным можно с помощью соответствующей конструкции системы и контроля за доступом. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)
8.1	Отправка большого количества ненужных данных в информационную систему транспортного средства, чтобы она не могла предоставлять услуги в обычном режиме	M13	Принимают меры по выявлению атаки на функцию отказа в обслуживании и по восстановлению системы
8.2	Атака методом переполнения, нарушение связи между транспортными средствами в результате блокировки передачи сообщений между транспортными средствами	M13	Принимают меры по выявлению атаки на функцию отказа в обслуживании и по восстановлению системы
9.1	Пользователь со стороны может получить привилегированный доступ, например доступ с полномочиями суперпользователя	M9	Применяют меры по предупреждению и выявлению случаев несанкционированного доступа
10.1	Вирус, занесенный в коммуникационную среду, инфицирует системы транспортного средства	M14	Меры по защите от внедренных вирусов/ вредоносных программ подлежат рассмотрению
11.1	Вредоносные внутренние (например, местная контроллерная сеть — CAN) сообщения	M15	Меры по выявлению злонамеренных внутренних сообщений или деятельности подлежат рассмотрению
11.2	Вредоносные сообщения V2X, например сообщения «объект инфраструктуры — транспортное средство» или «транспортное средство — транспортное средство» (например, CAM, DENM)	M10	Транспортное средство проверяет подлинность и целостность сообщений, которые оно получает
11.3	Вредоносные диагностические сигналы		
11.4	Вредоносные частные сообщения (например, те, которые обычно направляются OEM или поставщиком компонента/системы/функции)		

2. Меры по смягчению последствий в случае «Процесса обновления»

Меры по смягчению последствий угроз, которые связаны с «Процессом обновления», перечислены в таблице B2.

Таблица B2
Меры по смягчению последствий угроз, которые связаны с «Процессом обновления»

Ссылка на таблицу A1	*Угрозы, связанные с «Процессом обновления»*	*Ссылка*	*Смягчение последствий*
12.1	Нарушение процедур обновления программного обеспечения по каналу беспроводной связи. Это включает подделку программы обновления системы или встроенных программ	M16	Применяют безопасные процедуры обновления программного обеспечения
12.2	Нарушение процедур обновления локального/физического программного обеспечения. Это включает подделку программы обновления системы или встроенных программ		
12.3	Манипулирование программным обеспечением до процесса обновления (и, как следствие, его нарушение), хотя сам процесс обновления не нарушается		
12.4	Нарушение криптографических ключей провайдера программного обеспечения с целью допустить неполноценное обновление	M11	В целях хранения криптографических ключей обеспечиваются соответствующие средства контроля защиты
13.1	Атака в виде отказа в обслуживании сервера или сети с целью воспрепятствовать обновлению важнейшего программного обеспечения и/или разблокировки конкретных функций пользователя	M3	Средства контроля защиты применяют к внутренним системам. Там, где внутренние серверы имеют исключительно важное значение для обеспечения обслуживания, можно использовать в случае сбоев в работе системы соответствующие меры по восстановлению. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)

3. Меры по смягчению последствий в случае «Непреднамеренных действий человека, способствующих кибератаке»

Меры по смягчению последствий угроз, которые связаны с «Непреднамеренными действиями человека, способствующими кибератаке», перечислены в таблице B3.

Таблица B3
Меры по смягчению последствий угроз, которые связаны с «Непреднамеренными действиями человека, способствующими кибератаке»

Ссылка на таблицу A1	*Угрозы, связанные с «Непреднамеренными действиями человека»*	*Ссылка*	*Смягчение последствий*
15.1	Невинная жертва (например, владелец, оператор или инженер по техническому обслуживанию) путем обмана предпринимает действия с целью непреднамеренной загрузки вредоносного ПО или проведения атаки	M18	В целях определения и проверки ролей пользователей и привилегий доступа, основанных на принципе наименьшей привилегии доступа, принимают соответствующие меры
15.2	Заданные процедуры обеспечения безопасности не соблюдаются	M19	Организации обеспечивают определение и соблюдение процедур безопасности, включая регистрацию действий и доступа, связанных с управлением функциями безопасности

4. Меры по смягчению последствий в случае «Внешних подключений и соединений»

Меры по смягчению последствий угроз, которые связаны с «Внешними подключениями и соединениями», перечислены в таблице B4.

Таблица B4
Меры по смягчению последствий угроз, которые связаны с «Внешними подключениями и соединениями»

Ссылка на таблицу A1	*Угрозы, связанные с «Внешними подключениями и соединениями»*	*Ссылка*	*Смягчение последствий*
16.1	Манипулирование функциями, предназначенными для дистанционного управления такими системами, как дистанционный ключ, иммобилизатор и уличная зарядка	M20	В случае систем, оснащенных функцией дистанционного доступа, применяют соответствующие средства контроля защиты
16.2	Манипулирование средствами телематики транспортного средства (например, измерением температуры грузов, требующих особого обращения, дистанционным открытием дверей грузового отделения)		
16.3	Помехи в работе систем беспроводной связи ближнего радиуса действия или датчиков		
17.1	Поврежденные приложения или приложения со слабой программной защитой, используемые в качестве метода атаки на системы транспортных средств	M21	Программное обеспечение оценивают с точки зрения безопасности, удостоверяют его подлинность и обеспечивают защиту его целостности Для сведения к минимуму риска, связанного с использованием программного обеспечения третьей стороны, которое предназначено для размещения на транспортном средстве, применяют средства контроля защиты
18.1	Внешние интерфейсы, такие как USB или другие порты, используемые в качестве точки атаки, например путем внедрения кода	M22	К внешним интерфейсам применяют соответствующие средства контроля защиты
18.2	Программные средства инфицированы вирусами, занесенными в транспортное средство		
18.3	Точки диагностического контроля (например, программные ключи, вставляемые в БД-порт), которые используются для облегчения атаки, например для манипулирования параметрами транспортного средства (напрямую или опосредованно)	M22	К внешним интерфейсам применяют соответствующие средства контроля защиты

5. Меры по смягчению последствий в случае «Потенциальных целей или мотивировки атаки»

Меры по смягчению последствий угроз, которые связаны с «Потенциальными целями или мотивировкой атаки», перечислены в таблице B5.

Таблица B5

Меры по смягчению последствий угроз, которые связаны с «Потенциальными целями или мотивировкой атаки»

Ссылка на таблицу A1	*Угрозы, связанные с «Потенциальными целями или мотивировкой атаки»*	*Ссылка*	*Смягчение последствий*
19.1	Извлечение патентованного или собственного программного обеспечения из систем транспортного средства (фальсификация продукта/хищение программного обеспечения)	M7	В целях защиты данных/кода системы применяют соответствующие методы контроля за доступом и соответствующие конструктивные особенности. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)
19.2	Несанкционированный доступ к такой персональной информации владельца, как удостоверение личности, платежные реквизиты, адресная книга, информации о местоположении, электронная идентификация транспортного средства и т. д.	M8	Заблокировать доступ неуполномоченному персоналу к персональным данным или важнейшим системным данным можно с помощью соответствующей конструкции системы и контроля за доступом. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)
19.3	Извлечение криптографических ключей	M11	В целях хранения криптографических ключей обеспечиваются соответствующие средства контроля защиты, например модули безопасности
20.1	Противоправные/несанкционированные изменения в электронной идентификации транспортного средства	M7	В целях защиты данных/кода системы применяют соответствующие методы контроля за доступом и соответствующие конструктивные особенности. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)
20.2	Мошенничество с использованием персональных данных. Например, если пользователь желает выдать себя за другое лицо при установлении связи с системами взимания автодорожных сборов или серверным приложением изготовителя		
20.3	Действия с целью обхода систем мониторинга (например, взлом/подделка/блокирование таких сообщений, как данные системы регистрации ODR или количество рейсов)	M7	В целях защиты данных/кода системы применяют соответствующие методы контроля за доступом и соответствующие конструктивные особенности. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP). Атаки на датчики с целью манипулирования данными или последствия для передаваемых данных можно смягчить путем сопоставления данных, полученных из различных источников информации
20.4	Манипулирование данными в целях фальсификации данных об управлении транспортным средством (например, данных о пробеге, скорости, направлении движения и т. д.)		
20.5	Несанкционированные изменения данных системы диагностики		
21.1	Несанкционированное удаление журналов регистрации системных событий/ манипулирование журналами регистрации системных событий	M7	В целях защиты данных/кода системы применяют соответствующие методы контроля за доступом и соответствующие конструктивные особенности. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)

Ссылка на таблицу A1	*Угрозы, связанные с «Потенциальными целями или мотивировкой атаки»*	*Ссылка*	*Смягчение последствий*
22.2	Внедрение вредоносного программного обеспечения или создание условий для злонамеренной работы вредоносных программ	M7	В целях защиты данных/кода системы применяют соответствующие методы контроля за доступом и соответствующие конструктивные особенности. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)
23.1	Фабрикация программного обеспечения системы контроля или информационный системы транспортного средства		
24.1	Отказ в обслуживании: это, например, может быть инициировано во внутренней сети путем лавинного распространения данных по шине сети локальных контроллеров CAN или посредством провоцирования сбоев в ЭБУ вследствие большого количества сообщений	M13	Принимают меры по выявлению атаки на функцию отказа в обслуживании и по восстановлению системы
25.1	Несанкционированный доступ в целях фальсификации параметров конфигурации основных функций транспортного средства, таких как данные о тормозах, пороговом уровне срабатывания подушки безопасности и т. д.	M7	В целях защиты данных/кода системы применяют соответствующие методы контроля за доступом и соответствующие конструктивные особенности. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)
25.2	Несанкционированный доступ в целях фальсификации параметров зарядки, таких как напряжение зарядки, расход энергии на подзарядку, температура батареи и т. д.		

6. Меры по смягчению последствий в случае «Потенциальных факторов уязвимости, которыми можно воспользоваться в случае недостаточной защиты или надежности»

Меры по смягчению последствий угроз, которые связаны с «Потенциальными факторами уязвимости, которыми можно воспользоваться в случае недостаточной защиты или надежности», перечислены в таблице B6.

Таблица B6

Меры по смягчению последствий угроз, которые связаны с «Потенциальными факторами уязвимости, которыми можно воспользоваться в случае недостаточной защиты или надежности»

Ссылка на таблицу A1	*Угрозы, связанные с «Потенциальными факторами уязвимости, которыми можно воспользоваться в случае недостаточной защиты или надежности»*	*Ссылка*	*Смягчение последствий*
26.1	Сочетание коротких ключей шифрования данных и длительных сроков их действия дает взломщикам возможность сломать шифровальный код	M23	В процессе разработки программного обеспечения и аппаратных средств соблюдают современные виды практики в области кибербезопасности
26.2	Недостаточное использование шифровальных алгоритмов для защиты чувствительных систем		
26.3	Использование устаревших криптографических алгоритмов		
27.1	Аппаратное или программное обеспечение, разработанное таким образом, что оно создает возможность для атаки или не удовлетворяет конструктивным критериям для прекращения атаки	M23	В процессе разработки программного обеспечения и аппаратных средств соблюдают современные виды практики в области кибербезопасности

Ссылка на таблицу A1	*Угрозы, связанные с «Потенциальными факторами уязвимости, которыми можно воспользоваться в случае недостаточной защиты или надежности»*	*Ссылка*	*Смягчение последствий*
28.1	Наличие ошибок в программном обеспечении может явиться причиной возникновения потенциальных факторов уязвимости, которыми можно воспользоваться. Это особенно верно в том случае, если программное обеспечение не было протестировано с целью убедиться в том, что известного неудовлетворительного кода/ ошибок нет, и снизить риск наличия неизвестного неудовлетворительного кода/ ошибок	M23	В процессе разработки программного обеспечения и аппаратных средств соблюдают современные виды практики в области кибербезопасности. Тестирование кибербезопасности с достаточным покрытием
28.2	Использование остаточных устройств и материалов после разработки (например, отладочных портов, портов JTAG, микропроцессоров, сертификатов разработки, паролей разработчиков и т. д.) может обеспечить взломщику доступ к ЭБУ или дать ему возможность получить более высокий статус привилегий		
29.1	Лишние интернет-порты оставлены открытыми, что обеспечивает доступ к сетевым системам		
29.2	Обход разделения сети для получения контроля. Конкретным примером является использование незащищенных шлюзов или точек доступа (например, шлюзы «грузовой автомобиль-прицеп») для обхода защиты и получения доступа к другим сегментам сети, что позволяет производить злоумышленные действия, такие как передача произвольных сообщений на шину сети локальных контроллеров (CAN)	M23	В процессе разработки программного обеспечения и аппаратных средств соблюдают современные виды практики в области кибербезопасности. В процессе проектирования системы и системной интеграции соблюдают современные виды практики в области кибербезопасности

7. Меры по смягчению последствий в случае «Потери данных/утечки данных из транспортного средства»

Смягчение последствий угроз, которые связаны с «Потерей данных/утечкой данных из транспортного средства», перечислены в таблице B7.

Таблица B7

Смягчение последствий угроз, которые связаны с «Потерей данных/утечкой данных из транспортного средства»

Ссылка на таблицу A1	*Угрозы, связанные с «Потерями данных/утечкой данных из транспортного средства»*	*Ссылка*	*Смягчение последствий*
31.1	Утечка информации. В случае смены пользователя автомобиля может произойти утечка персональных данных (например, если автомобиль продан или используется напрокат другими лицами)	M24	При хранении персональных данных необходимо следовать передовым методам защиты целостности и конфиденциальности данных

8. Меры по смягчению последствий в случае «Физического манипулирования системами, которое может создать возможность для атаки»

Меры по смягчению последствий угроз, связанных с «Физическим манипулированием системами, которое может создать возможность для атаки», перечислены в таблице B8.

Таблица B8

Меры по смягчению последствий угроз, связанных с «Физическим манипулированием системами, которое может создать возможность для атаки»

Ссылка на таблицу A1	*Угрозы, связанные с «Физическим манипулированием системами, которое может создать возможность для атаки»*	*Ссылка*	*Смягчение последствий*
32.1	Манипулирование электронной аппаратурой, например установка на транспортное средство несанкционированной электронной аппаратуры, что создает возможность для проведения атаки через посредника	M9	Применяют меры по предупреждению и выявлению случаев несанкционированного доступа

Часть C
Меры по смягчению последствий угроз за пределами транспортных средств

1. Меры по смягчению последствий в случае «Внутренних серверов»

Меры по смягчению последствий угроз, которые связаны с «Внутренними серверами», перечислены в таблице C1.

Таблица C1
Меры по смягчению последствий угроз, которые связаны с «Внутренними серверами»

Ссылка на таблицу A1	*Угрозы, связанные с «Внутренними серверами»*	*Ссылка*	*Смягчение последствий*
1.1 и 3.1	Злоупотребление привилегиями штатными сотрудниками (внутренняя атака)	M1	Средства контроля защиты применяют к внутренним системам в целях сведения к минимуму риска угрозы со стороны штатных сотрудников
1.2 и 3.3	Несанкционированный доступ через Интернет к серверу (который возможен, например, в результате обхода системы защиты, не устраненных факторов уязвимости системы программного обеспечения, атаки методом использования языка структурированных запросов SQL или иными способами)	M2	Средства контроля защиты применяют к внутренним системам в целях сведения к минимуму несанкционированного доступа. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)
1.3 и 3.4	Несанкционированный физический доступ к серверу (например, с помощью USB-накопителей или иных средств, подключаемых к серверу)	M8	Заблокировать доступ неуполномоченному персоналу к персональным данным или важнейшим системным данным можно с помощью соответствующей конструкции системы и контроля за доступом
2.1	Атака на внутренний сервер, который прекращает работу: она, например, не дает ему возможности взаимодействовать с транспортными средствами и оказывать услуги, которые нужны для их работы	M3	Средства контроля защиты применяют к внутренним системам. Там, где внутренние серверы имеют исключительно важное значение для обеспечения обслуживания, можно использовать в случае сбоев в работе системы соответствующие меры по восстановлению. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)
3.2	Потеря информации в облаке. Конфиденциальные данные могут быть потеряны из-за атак или аварий при хранении данных сторонними поставщиками облачных услуг	M4	Средства контроля защиты применяют к внутренним системам в целях сведения к минимуму рисков, связанных с облачной обработкой данных. Примеры средств контроля защиты можно найти в проекте OWASP и в руководстве по облачной обработке данных NCSC
3.5	Утечка информации в результате непреднамеренного обмена данными (например, ошибки на уровне администрации, хранение данных на серверах в гаражах)	M5	Средства контроля защиты применяют к внутренним системам в целях предотвращения утечек данных. Примеры средств контроля защиты можно найти в Проекте по обеспечению безопасности открытых веб-приложений (OWASP)

2. Меры по смягчению последствий в случае «Непреднамеренных действий человека»

Меры по смягчению последствий угроз, которые связаны с «Непреднамеренными действиями человека», перечислены в таблице C2.

Таблица C2
Меры по смягчению последствий угроз, которые связаны с «Непреднамеренными действиями человека»

Ссылка на таблицу A1	*Угрозы, связанные с «Непреднамеренными действиями человека»*	*Ссылка*	*Смягчение последствий*
15.1	Невинная жертва (например, владелец, оператор или инженер по техническому обслуживанию) путем обмана предпринимает действия с целью непреднамеренной загрузки вредоносного ПО или проведения атаки	M18	В целях определения и проверки ролей пользователей и привилегий доступа, основанных на принципе наименьшей привилегии доступа, принимают соответствующие меры
15.2	Заданные процедуры обеспечения безопасности не соблюдаются	M19	Организации обеспечивают определение и соблюдение процедур безопасности, включая регистрацию действий и доступа, связанных с управлением функциями безопасности