

4 March 2021

Соглашение

О принятии согласованных технических правил Организации Объединенных Наций для колесных транспортных средств, предметов оборудования и частей, которые могут быть установлены и/или использованы на колесных транспортных средствах, и об условиях взаимного признания официальных утверждений, выдаваемых на основе этих правил Организации Объединенных Наций*

(Пересмотр 3, включающий поправки, вступившие в силу 14 сентября 2017 года)

Добавление 154 – Правила № 155 ООН

Дата вступления в силу в качестве приложения к Соглашению 1958 года: 22 января 2021 года

Единообразные предписания, касающиеся официального утверждения транспортных средств в отношении кибербезопасности и их систем обеспечения кибербезопасности

Настоящий документ опубликован исключительно в информационных целях. Аутентичным и юридически обязательным текстом является документ ECE/TRANS/WP.29/2020/79 (с поправками, содержащимися в документах ECE/TRANS/WP.29/2020/94 и ECE/TRANS/WP.29/2020/97).



Организация Объединенных Наций

* Прежние названия Соглашения:
Соглашение о принятии единообразных условий официального утверждения и о взаимном признании официального утверждения предметов оборудования и частей механических транспортных средств, совершено в Женеве 20 марта 1958 года (первоначальный вариант);
Соглашение о принятии единообразных технических предписаний для колесных транспортных средств, предметов оборудования и частей, которые могут быть установлены и/или использованы на колесных транспортных средствах, и об условиях взаимного признания официальных утверждений, выдаваемых на основе этих предписаний, совершено в Женеве 5 октября 1995 года (Пересмотр 2).



Правила № 155 ООН

Единообразные предписания, касающиеся официального утверждения транспортных средств в отношении кибербезопасности и их систем обеспечения кибербезопасности

Содержание

	<i>Стр.</i>
1. Сфера применения	4
2. Определения	4
3. Заявка на официальное утверждение	5
4. Маркировка	6
5. Официальное утверждение	6
6. Свидетельство о соответствии системы обеспечения кибербезопасности	10
7. Технические требования	11
8. Модификация и распространение официального утверждения типа транспортного средства	14
9. Соответствие производства	14
10. Санкции, налагаемые за несоответствие производства	15
11. Окончательное прекращение производства	15
12. Названия и адреса технических служб, ответственных за проведение испытания для официального утверждения, и органов по официальному утверждению типа	15
Приложения	
1 Информационный документ	16
2 Сообщение	18
3 Схема знака официального утверждения	19
4 Образец свидетельства о соответствии СОКиБ	20
5 Перечень угроз и соответствующих мер по смягчению последствий	21

1. Сфера применения

- 1.1 Настоящие Правила применяются к транспортным средствам категорий М и N в отношении кибербезопасности.
- Настоящие Правила применяются также к транспортным средствам категории О, если они оснащены по меньшей мере одним электронным блоком управления.
- 1.2 Настоящие Правила применяются также к транспортным средствам категорий L₆ и L₇, если они оснащены автоматизированной функцией управления транспортным средством, начиная с уровня 3 и выше, как это определено в справочном документе с определениями термина «автоматизированное вождение» в рамках WP.29 и Общих принципах для разработки правил ООН, касающихся автоматизированных транспортных средств (ECE/TRANS/WP.29/1140).
- 1.3 Настоящие Правила применяются без ущерба для иных правил ООН, а равно регионального или национального законодательства, регулирующих доступ уполномоченных сторон к транспортному средству, его бортовым данным, функциям и ресурсам, а также условия такого доступа. Они также применяются без ущерба для национального и регионального законодательства, регулирующего неприкосновенность частной жизни и защиты физических лиц в части обработки их персональных данных.
- 1.4 Настоящие Правила применяются без ущерба для иных Правил ООН, а равно национального или регионального законодательства, регулирующих разработку и установку/системную интеграцию запасных частей и компонентов, как физических, так и цифровых, в части кибербезопасности.

2. Определения

Для целей настоящих Правил применяются следующие определения:

- 2.1 «*Тип транспортного средства*» означает транспортные средства, не имеющие различий в отношении следующих основных аспектов:
- обозначения изготовителя данного типа транспортного средства;
 - основных аспектов электрической/электронной архитектуры и внешних интерфейсов применительно к кибербезопасности.
- 2.2 «*Кибербезопасность*» означает состояние, в котором транспортные средства и их функции защищены от киберугроз, которым могут подвергаться электрические или электронные компоненты.
- 2.3 «*Система обеспечения кибербезопасности (СОКиБ)*» означает систематический подход на основе оценки риска, определяющий организационные процессы, обязанности и методы обработки риска, связанного с киберугрозами, которым подвергаются транспортные средства, и их защиты от кибератак.
- 2.4 «*Система*» означает совокупность компонентов и/или подсистем, реализующих соответствующую функцию или функции.
- 2.5 «*Этап разработки*» означает период до официального утверждения данного типа транспортного средства.
- 2.6 «*Этап производства*» означает продолжительность производства соответствующего типа транспортного средства.

- 2.7 «*Этап после производства*» означает период, в течение которого данный тип транспортного средства более не производится до окончания срока службы всех транспортных средств данного типа. Транспортные средства, включающие конкретный тип транспортного средства, будут эксплуатироваться на этом этапе, но производиться больше не будут. Данный этап заканчивается в тот момент, когда в эксплуатации больше нет никаких транспортных средств, относящихся к конкретному типу транспортного средства.
- 2.8 «*Смягчение последствий*» означает соответствующую меру, которая позволяет изменить уровень риска.
- 2.9 «*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.
- 2.10 «*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).
- 2.11 «*Управление риском*» означает согласованные действия по руководству и управлению соответствующей организацией в связи с риском.
- 2.12 «*Угроза*» означает потенциальную причину нежелательного инцидента, который может нанести ущерб системе или организации.
- 2.13 «*Уязвимость*» означает слабость какого-либо материального объекта или средства смягчения последствий, которая дает возможность реализации одной или нескольких угроз.

3. Заявка на официальное утверждение

- 3.1 Заявка на официальное утверждение типа транспортного средства в отношении кибербезопасности подается изготовителем транспортного средства или его должным образом уполномоченным представителем.
- 3.2 К заявке прилагаются перечисленные ниже документы в трех экземплярах и следующие дополнительные сведения:
- 3.2.1 описание типа транспортного средства с указанием данных, предусмотренных в приложении 1 к настоящим Правилам;
- 3.2.2 в тех случаях, когда указано, что информация защищена правами интеллектуальной собственности или относится к разряду специальных научных знаний изготовителя или его поставщиков, изготовитель или его поставщики предоставляют достаточную информацию, позволяющую надлежащим образом провести проверки, указанные в настоящих Правилах. С такой информацией обращаются на конфиденциальной основе;
- 3.2.3 свидетельство о соответствии СОКиБ на основании пункта 6 настоящих Правил.
- 3.3 Должна быть доступна документация следующих двух видов:
- а) официальный набор документов для официального утверждения, содержащий материалы, указанные в приложении 1, которые передаются органу по официальному утверждению или технической службе в момент подачи заявки на официальное утверждение типа. Этот набор документации используется органом по официальному утверждению или его технической службой в качестве основного справочного материала для

процесса официального утверждения. Орган по официальному утверждению или его техническая служба обеспечивает доступность этого набора документации в течение 10 лет начиная с момента окончательного прекращения производства данного типа транспортного средства;

- b) дополнительные материалы, относящиеся к требованиям настоящих Правил, могут оставаться на хранении у изготовителя, но должны предоставляться для проверки во время официального утверждения типа. Изготовитель обеспечивает доступность любых материалов, предоставляемых для проверки в ходе официального утверждения, в течение не менее 10 лет начиная с момента окончательного прекращения производства данного типа транспортного средства.

4. Маркировка

- 4.1 На каждом транспортном средстве, соответствующем типу транспортного средства, официально утвержденному на основании настоящих Правил, проставляется на видном и легкодоступном месте, указанном в регистрационной карточке официального утверждения, международный знак официального утверждения, состоящий из:
- 4.1.1 круга с проставленной в нем буквой «E», за которой следует отличительный номер страны, предоставившей официальное утверждение;
- 4.1.2 номера настоящих Правил, за которым следуют буква «R», тире и номер официального утверждения, проставленные справа от круга, предусмотренного в пункте 4.1.1, выше.
- 4.2 Если транспортное средство соответствует типу транспортного средства, официально утвержденному на основании одного или нескольких других прилагаемых к Соглашению правил в той же стране, которая предоставила официальное утверждение на основании настоящих Правил, то обозначение, предписанное в пункте 4.1.1, выше, повторять не нужно; в таком случае номера правил и официального утверждения, а также дополнительные обозначения всех правил, на основании которых было предоставлено официальное утверждение в стране, предоставившей официальное утверждение на основании настоящих Правил, должны быть расположены в вертикальных колонках справа от обозначения, предписанного в пункте 4.1.1, выше.
- 4.3 Знак официального утверждения должен быть четким и нестираемым.
- 4.4 Знак официального утверждения помещается рядом с прикрепляемой изготовителем табличкой, на которой приведены характеристики транспортного средства, или наносится на эту табличку.
- 4.5 В приложении 3 к настоящим Правилам в качестве примера приведены схемы знаков официального утверждения.

5. Официальное утверждение

- 5.1 Органы по официальному утверждению предоставляют в надлежащих случаях официальное утверждение типа в отношении кибербезопасности только таким типам транспортных средств, которые удовлетворяют требованиям настоящих Правил.

- 5.1.1 Орган по официальному утверждению или техническая служба проверяет посредством ознакомления с документацией, что изготовителем транспортного средства приняты необходимые меры, имеющие отношение к данному типу транспортного средства, в целях:
- a) сбора и проверки информации, требуемой на основании настоящих Правил в пределах производственно-сбытовой цепочки, чтобы продемонстрировать, что риски, связанные с поставщиками, выявлены и управляются;
 - b) документального оформления оценки рисков (проводимой на этапе разработки или ретроспективно), результатов испытаний и мер по смягчению последствий применительно к данному типу транспортного средства, включая проектную информацию, подтверждающую оценку рисков;
 - c) принятия надлежащих мер по обеспечению кибербезопасности конструкции данного типа транспортного средства;
 - d) обнаружения возможных атак на кибербезопасность и реагирования на них;
 - e) регистрации данных для поддержки обнаружения кибератак и обеспечения возможностей криминалистической экспертизы данных для анализа предпринятых попыток проведения кибератак или успешных кибератак.
- 5.1.2 Орган по официальному утверждению или техническая служба проводит проверку путем испытания транспортного средства данного типа с целью убедиться в том, что изготовитель данного транспортного средства принял надлежащие меры кибербезопасности и документально зафиксировал их. Испытания проводятся органом по официальному утверждению или самой технической службой либо в сотрудничестве с изготовителем транспортного средства путем отбора образцов. Отбор образцов должен быть сфокусирован на рисках, которые оцениваются как высокие в ходе оценки рисков, но не ограничиваться ими.
- 5.1.3 Орган по официальному утверждению или техническая служба отказывает в предоставлении официального утверждения типа в отношении кибербезопасности, если изготовитель транспортного средства не выполнил одно или несколько требований, упомянутых в пункте 7.3, в частности:
- a) изготовитель транспортного средства не провел исчерпывающей оценки риска, упомянутой в пункте 7.3.3; в том числе в тех случаях, когда изготовитель не учел все риски, связанные с угрозами, указанными в части А приложения 5;
 - b) изготовитель транспортного средства не обеспечил защиты данного типа транспортного средства от рисков, выявленных в ходе оценки риска изготовителем данного транспортного средства, или не были приняты соразмерные меры по смягчению последствий согласно требованиям пункта 7;
 - c) изготовитель транспортного средства не принял надлежащих и соразмерных мер 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 типу транспортного средства;
 - d) изготовитель транспортного средства не провел, до официального утверждения, надлежащих и достаточных испытаний для проверки эффективности принятых мер безопасности.

- 5.1.4 Оценивающий орган по официальному утверждению отказывает также в предоставлении официального утверждения типа в отношении кибербезопасности, если орган по официальному утверждению или техническая служба не получили от изготовителя транспортного средства достаточной информации для оценки кибербезопасности данного типа транспортного средства.
- 5.2 Стороны Соглашения 1958 года, применяющие настоящие Правила, уведомляются об официальном утверждении, распространении официального утверждения или отказе в официальном утверждении типа транспортного средства на основании настоящих Правил посредством карточки, соответствующей образцу, приведенному в приложении 2 к настоящим Правилам.
- 5.3 Органы по официальному утверждению не предоставляют никакого официального утверждения типа, не убедившись в том, что изготовитель ввел в действие удовлетворительные механизмы и процедуры, позволяющие надлежащим образом регулировать аспекты кибербезопасности, охватываемые настоящими Правилами.
- 5.3.1 Орган по официальному утверждению и его технические службы обеспечивают, помимо критериев, изложенных в приложении 2 к Соглашению 1958 года:
- a) наличие у них компетентного персонала, обладающего соответствующими навыками в области кибербезопасности и конкретными знаниями рисков причинения вреда автотранспортными средствами¹;
 - b) выполнение ими процедур единообразной оценки в соответствии с настоящими Правилами.
- 5.3.2 Каждая Договаривающаяся сторона, применяющая настоящие Правила, уведомляет и информирует через свой орган по официальному утверждению другие органы по официальному утверждению Договаривающихся сторон, применяющих настоящие Правила ООН, о методе и критериях, взятых за основу уведомляющим органом для оценки уместности мер, принятых в соответствии с настоящими Правилами, в частности с пунктами 5.1, 7.2 и 7.3.
- Эта информация доводится до сведения а) только перед первым предоставлением официального утверждения на основании настоящих Правил и b) каждый раз при обновлении метода или критериев оценки.
- Эта информация предназначена для сообщения в целях сбора и анализа передовой практики и обеспечения единообразного применения настоящих Правил всеми органами по официальному утверждению, применяющими настоящие Правила.
- 5.3.3 Информация, указанная в пункте 5.3.2, загружается на английском языке в защищенную базу данных в Интернете «ДЕТА»², созданную Европейской экономической комиссией Организации Объединенных Наций, в установленные сроки и не позднее чем за 14 дней до первого предоставления официального утверждения на основании соответствующих методов и критериев оценки. Эта информация должна быть достаточной для понимания того, какие минимальные уровни результативности были приняты органом по официальному утверждению в отношении каждого конкретного требования, указанного

¹ Например, ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434.

² <https://www.unece.org/trans/main/wp29/datasharing.html>.

- в пункте 5.3.2, а также того, какие процессы и меры он применяет для проверки соблюдения этих минимальных уровней результативности³.
- 5.3.4 Органы по официальному утверждению, получающие информацию, указанную в пункте 5.3.2, могут представить замечания уведомляемому органу по официальному утверждению путем их загрузки в ДЕТА в течение 14 дней после дня уведомления.
- 5.3.5 Если органу по официальному утверждению, предоставляемому официальное утверждение, невозможно принять во внимание замечания, полученные в соответствии с пунктом 5.3.4, органы по официальному утверждению, направившие замечания, и орган, предоставляющий официальное утверждение, обращаются за дополнительными разъяснениями в соответствии с приложением 6 к Соглашению 1958 года. Соответствующая вспомогательная Рабочая группа⁴ Всемирного форума для согласования правил в области транспортных средств (WP.29), занимающаяся настоящими Правилами, согласовывает общее толкование методов и критериев оценки⁵. Это общее толкование должно применяться, и все органы по официальному утверждению соответственно предоставляют официальные утверждения типа на основании настоящих Правил.
- 5.3.6 Каждый орган по официальному утверждению, предоставляющий официальное утверждение типа на основании настоящих Правил, уведомляет другие органы по официальному утверждению о предоставленном официальном утверждении. Официальное утверждение типа вместе с дополнительной документацией загружается на английском языке в ДЕТА органом по официальному утверждению в течение 14 дней после дня предоставления официального утверждения⁶.
- 5.3.7 Договаривающиеся стороны могут изучить предоставленные официальные утверждения на основе информации, загруженной в соответствии с пунктом 5.3.6. В случае любого расхождения во мнениях между Договаривающимися сторонами этот вопрос должен решаться в соответствии со статьей 10 и приложением 6 Соглашения 1958 года. Договаривающиеся стороны информируют также соответствующую вспомогательную рабочую группу Всемирного форума для согласования правил в области транспортных средств (WP.29) о расхождениях в толковании по смыслу приложения 6 Соглашения 1958 года. Соответствующая Рабочая группа содействует урегулированию расхождения во мнениях и в случае необходимости может консультироваться с WP.29 по этому вопросу.
- 5.4 Для целей пункта 7.2 настоящих Правил изготовитель обеспечивает реализацию на практике всех аспектов кибербезопасности, охватываемых настоящими Правилами.

³ Руководящие указания в отношении загружаемой подробной информации (например, метода, критериев, уровня результативности) и формата приводятся в пояснительном документе, который в настоящее время готовится целевой группой по вопросам кибербезопасности и беспроводной связи для седьмой сессии GRVA.

⁴ Рабочая группа по автоматизированным/автономным и подключенным транспортным средствам (GRVA).

⁵ Это толкование должно быть отражено в пояснительном документе, упомянутом в сноске к пункту 5.3.3.

⁶ Дополнительная информация о минимальных требованиях к комплекту документации будет разработана GRVA в ходе ее семи сессий.

6. Свидетельство о соответствии системы обеспечения кибербезопасности

- 6.1 Договаривающиеся стороны назначают орган по официальному утверждению для оценки изготовителя и выдачи свидетельства о соответствии СОКиБ.
- 6.2 Заявка на получение свидетельства о соответствии системы обеспечения кибербезопасности подается изготовителем транспортного средства или его должным образом уполномоченным представителем.
- 6.3 К заявке прилагаются перечисленные ниже документы в трех экземплярах и следующие дополнительные сведения:
- 6.3.1 документация с описанием системы обеспечения кибербезопасности;
- 6.3.2 подписанное заявление в соответствии с образцом, определенным в добавлении 1 к приложению 1.
- 6.4 В контексте этой оценки изготовитель заявляет в соответствии с образцом, определенным в добавлении 1 к приложению 1, и подтверждает к удовлетворению органа по официальному утверждению или его технической службы, что у него налажены необходимые процедуры соблюдения всех требований в отношении кибербезопасности в соответствии с настоящими Правилами.
- 6.5 После удовлетворительного завершения этой оценки и получения подписанного заявления от изготовителя в соответствии с образцом, определенным в добавлении 1 к приложению 1, изготовителю выдается соответствующее свидетельство под названием «свидетельство о соответствии СОКиБ», описанное в приложении 4 к настоящим Правилам (здесь и далее – свидетельство о соответствии СОКиБ).
- 6.6 Орган по официальному утверждению или его техническая служба использует для выдачи свидетельства о соответствии СОКиБ образец, содержащийся в приложении 4 к настоящим Правилам.
- 6.7 Свидетельство о соответствии СОКиБ остается действительным в течение не более трех лет со дня его выдачи, если только оно не будет отозвано.
- 6.8 Орган по официальному утверждению, который выдал свидетельство о соответствии СОКиБ, может в любое время проверить, продолжают ли удовлетворяться предъявляемые к нему требования. Орган по официальному утверждению отзывает свидетельство о соответствии СОКиБ, если требования, предусмотренным в настоящих Правилах, больше не соблюдаются.
- 6.9 Изготовитель информирует орган по официальному утверждению или его техническую службу о любом изменении, которое повлияет на применимость свидетельства о соответствии СОКиБ. После консультации с изготовителем орган по официальному утверждению или его техническая служба принимает решение о том, нужны ли новые проверки.
- 6.10 В установленный срок, позволяющий органу по официальному утверждению завершить свою оценку до окончания срока действия свидетельства о соответствии СОКиБ, изготовитель подает заявку на получение нового или на продление срока действия существующего свидетельства о соответствии СОКиБ. Орган по официальному утверждению выдает, на основании соответствующей положительной оценки, новое свидетельство о соответствии СОКиБ или продлевает срок его действия еще на три года. Орган по официальному утверждению проверяет, продолжает ли СОКиБ удовлетворять требованиям

настоящих Правил. Орган по официальному утверждению выдает новое свидетельство в тех случаях, когда до его сведения или до сведения его технической службы были доведены существенные изменения и когда повторная оценка этих изменений дала положительные результаты.

- 6.11 Истечение срока действия или отмена свидетельства о соответствии СОКиБ, выданного изготовителю, рассматривается, в отношении типов транспортных средств, к которым имела отношение соответствующая СОКиБ, как изменение официального утверждения, указанное в пункте 8, что может включать отмену официального утверждения, если условия предоставления официального утверждения больше не выполняются.

7. Технические требования

- 7.1 Общие технические требования
- 7.1.1 Требования настоящих Правил не ограничивают действие положений или предписаний других правил ООН.
- 7.2 Требования, предъявляемые к системе обеспечения кибербезопасности
- 7.2.1 В целях оценки орган по официальному утверждению или его техническая служба удостоверяется в том, что у изготовителя транспортного средства есть соответствующая система обеспечения кибербезопасности, и удостоверяется в ее соответствии настоящим Правилам.
- 7.2.2 Система обеспечения кибербезопасности охватывает следующие аспекты:
- 7.2.2.1 Изготовитель транспортного средства подтверждает органу по официальному утверждению или его технической службе, что их система обеспечения кибербезопасности применяется к следующим этапам:
- a) этап разработки;
 - b) этап реализации;
 - c) этап после реализации.
- 7.2.2.2 Изготовитель транспортного средства подтверждает, что процессы, используемые в рамках его системы обеспечения кибербезопасности, позволяют надлежащим образом учитывать вопросы безопасности, включая риски и меры по смягчению последствий, перечисленные в приложении 5. Они включают следующее:
- a) процессы, используемые в организации изготовителя в целях управления системой кибербезопасности;
 - b) процессы, используемые для выявления рисков, которым подвергаются транспортные средства. В рамках этих процессов рассматриваются угрозы, указанные в части А приложения 5, и другие соответствующие угрозы;
 - c) процессы, используемые для оценки, классификации и обработки выявленных рисков;
 - d) процессы, введенные в действие с целью удостовериться, что выявленные риски устраняются надлежащим образом;
 - e) процессы, используемые для проверки кибербезопасности типа транспортного средства;
 - f) процессы, используемые с целью обеспечить постоянное обновление оценки рисков;

- g) процессы, используемые для мониторинга кибератак, киберугроз и факторов уязвимости соответствующих типов транспортных средств, их обнаружения и реагирования на них, и процессы, используемые для оценки того, являются ли принимаемые меры кибербезопасности по-прежнему эффективными в свете новых киберугроз и факторов уязвимости, которые были выявлены;
 - h) Процессы, используемые для предоставления соответствующих данных с целью поддержки анализа предпринятых попыток проведения кибератак или успешных кибератак.
- 7.2.2.3 Изготовитель транспортного средства подтверждает, что процессы, используемые в рамках его системы обеспечения кибербезопасности, будут обеспечивать, на основе классификации, упомянутой в подпунктах с) и g) пункта 7.2.2.2.2, смягчение в разумные сроки последствий киберугроз и факторов уязвимости, требующих реагирования со стороны изготовителя транспортного средства.
- 7.2.2.4 Изготовитель транспортного средства подтверждает, что процессы, используемые в рамках его системы обеспечения кибербезопасности, будут обеспечивать непрерывный мониторинг, упомянутый в подпункте g) пункта 7.2.2.2. Они включают следующее:
- a) транспортные средства после первой регистрации в рамках мониторинга;
 - 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 пункта 1.3 и права владельцев или водителей автомобилей на неприкосновенность частной жизни, особенно в том, что касается согласия.
- 7.2.2.5 Изготовитель транспортного средства должен продемонстрировать, каким образом его система обеспечения кибербезопасности будет регулировать соответствующие аспекты взаимозависимости, которая может существовать с поставщиками изделий и услуг, с которыми заключены соответствующие контракты, или с его суборганизациями в связи с требованиями пункта 7.2.2.2.
- 7.3 Требования, предъявляемые к типам транспортных средств
- 7.3.1 Изготовитель должен иметь действующее свидетельство соответствия системы обеспечения кибербезопасности, относящееся к официально утверждаемому типу транспортного средства.
- Однако, в случае официальных утверждений типа до 1 июля 2024 года, если изготовитель транспортного средства может продемонстрировать, что данный тип транспортного средства не мог быть разработан в соответствии с СОКиБ, то изготовитель транспортного средства должен продемонстрировать, что на этапе разработки соответствующего типа транспортного средства была должным образом учтена кибербезопасность.
- 7.3.2 Изготовитель транспортного средства идентифицирует, в отношении официально утверждаемого типа транспортного средства, риски, связанные с поставщиками, и управляет ими.
- 7.3.3 Изготовитель транспортного средства идентифицирует критические элементы данного типа транспортных средств и проводит исчерпывающую оценку рисков для данного типа транспортных средств, а также надлежащим образом обрабатывает выявленные риски/управляет выявленными рисками. При оценке рисков учитываются отдельные элементы типа транспортного средства и их взаимодействия. В ходе

оценки рисков учитываются, кроме того, взаимодействия с любыми внешними системами. При оценке рисков изготовитель транспортного средства учитывает риски, связанные со всеми угрозами, указанными в части А приложения 5, а также любой другой соответствующий риск.

- 7.3.4 Изготовитель транспортного средства защищает тип транспортного средства от рисков, выявленных в ходе оценки рисков изготовителем транспортного средства. Для защиты типа транспортного средства принимаются соразмерные меры по смягчению последствий. Осуществляемые меры по смягчению последствий включают все меры по смягчению последствий, о которых говорится в частях В и С приложения 5 и которые касаются выявленных рисков. Однако, если та или иная мера по смягчению последствий, упомянутая в части В или С приложения 5, не имеет отношения к выявленному риску или является недостаточной, изготовитель транспортного средства обеспечивает осуществление какой-либо другой соответствующей меры по смягчению последствий.
- В частности, в случае официальных утверждений типа до 1 июля 2024 года, изготовитель транспортного средства обеспечивает осуществление какой-либо другой соответствующей меры по смягчению последствий, если та или иная мера по смягчению последствий, упомянутая в части В или С приложения 5, технически неосуществима. Соответствующая оценка технической осуществимости предоставляется изготовителем органу по официальному утверждению.
- 7.3.5 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 типу транспортного средства.
- 7.3.6 Изготовитель транспортного средства проводит, до официального утверждения, надлежащие и достаточные испытания для проверки эффективности принятых мер безопасности.
- 7.3.7 Изготовитель транспортного средства принимает в отношении данного типа транспортного средства соответствующие меры с целью:
- a) обнаружения и предотвращения кибератак на транспортные средства данного типа;
 - b) поддержки возможностей мониторинга, осуществляемого изготовителем транспортного средства для обнаружения угроз, факторов уязвимости и кибератак, относящихся к данному типу транспортного средства;
 - c) предоставления возможностей криминалистической экспертизы данных для анализа предпринятых попыток проведения кибератак или успешных кибератак.
- 7.3.8 Криптографические модули, используемые для целей настоящих Правил, должны соответствовать согласованным стандартам. Если используемые криптографические модули не соответствуют согласованным стандартам, то изготовитель транспортного средства должен обосновать их использование.
- 7.4 Положения об отчетности
- 7.4.1 Изготовитель транспортного средства предоставляет по меньшей мере один раз в год или чаще, если это необходимо, органу по официальному утверждению или технической службе отчет о результатах своей деятельности по мониторингу, как она определена в подпункте g) пункта 7.2.2.2, который должен включать соответствующую

информацию о новых кибератаках. Изготовитель транспортного средства также сообщает и подтверждает органу по официальному утверждению или технической службе, что меры по смягчению последствий рисков для кибербезопасности, применяемые в отношении его типов транспортных средств, по-прежнему эффективны, а также любые дополнительные меры, принятые в этой связи.

- 7.4.2 Орган по официальному утверждению или техническая служба проверяет представленную информацию и в случае необходимости требует от изготовителя транспортного средства устранить любую выявленную неэффективность.

Если отчетность или ответ недостаточны, орган по официальному утверждению может принять решение об отзыве СОКиБ в соответствии с пунктом 6.8.

8. Модификация и распространение официального утверждения типа транспортного средства

- 8.1 Любая модификация типа транспортного средства, которая сказывается на его технических характеристиках в части кибербезопасности и/или документации, требуемой в соответствии с настоящими Правилами, доводится до сведения органа по официальному утверждению, предоставившего официальное утверждение данного типа транспортного средства. Орган по официальному утверждению может либо:

8.1.1 прийти к заключению, что внесенные изменения все еще удовлетворяют действующим требованиям и документации, относящейся к существующему официальному утверждению типа; либо

8.1.2 провести необходимую дополнительную оценку в соответствии с пунктом 5 и потребовать, в соответствующих случаях, нового протокола испытания от технической службы, ответственной за проведение испытаний.

8.1.3 Сообщение о подтверждении официального утверждения, о распространении официального утверждения или об отказе в официальном утверждении доводится до сведения посредством карточки сообщения, соответствующей образцу, приведенному в приложении 2 к настоящим Правилам. Орган по официальному утверждению, распространивший официальное утверждение, присваивает такому распространению соответствующий серийный номер и уведомляет об этом другие Стороны Соглашения 1958 года, применяющие настоящие Правила, посредством карточки сообщения, соответствующей образцу, приведенному в приложении 2 к настоящим Правилам.

9. Соответствие производства

- 9.1 Процедуры обеспечения соответствия производства должны соответствовать процедурам, изложенным в приложении 1 к Соглашению 1958 года (E/ECE/TRANS/505/Rev.3), с учетом следующих требований:

9.1.1 Держатель официального утверждения обеспечивает регистрацию данных, полученных в результате испытаний на проверку соответствия производства, а также доступ к прилагаемым документам в течение периода, определенного по договоренности с органом по официальному утверждению или его технической службой. Такой период не должен превышать 10 лет, считая с момента окончательного прекращения производства.

- 9.1.2 Орган по официальному утверждению, предоставивший официальное утверждение типа, может в любое время проверить методы контроля за соответствием производства, применяемые на каждом производственном объекте. Обычно такие проверки проводят один раз в три года.

10. Санкции, налагаемые за несоответствие производства

- 10.1 Официальное утверждение типа транспортного средства, предоставленное на основании настоящих Правил, может быть отменено, если не соблюдаются требования, изложенные в настоящих Правилах, или если образцы транспортного средства не соответствуют требованиям настоящих Правил.
- 10.2 Если орган по официальному утверждению отзывает предоставленное им ранее официальное утверждение, то он немедленно уведомляет об этом Договаривающиеся стороны, применяющие настоящие Правила, посредством карточки сообщения, соответствующей образцу, приведенному в приложения 2 к настоящим Правилам.

11. Окончательное прекращение производства

- 11.1 Если держатель официального утверждения полностью прекращает производство типа транспортного средства, официально утвержденного на основании настоящих Правил, то он информирует об этом орган, предоставивший официальное утверждение. По получении соответствующего сообщения данный орган информирует о нем другие Договаривающиеся стороны Соглашения, применяющие настоящие Правила, посредством копии карточки официального утверждения, в конце которой крупным шрифтом делают отметку «ПРОИЗВОДСТВО ПРЕКРАЩЕНО» и проставляют подпись и дату.

12. Названия и адреса технических служб, ответственных за проведение испытания для официального утверждения, и органов по официальному утверждению типа

- 12.1 Стороны Соглашения, применяющие настоящие Правила, сообщают в Секретариат Организации Объединенных Наций названия и адреса технических служб, ответственных за проведение испытания для официального утверждения, а также органов по официальному утверждению типа, которые предоставляют официальное утверждение и которым надлежит направлять выдаваемые в других странах карточки, подтверждающие официальное утверждение, распространение официального утверждения, отказ в официальном утверждении или отзыв официального утверждения.

Приложение 1

Информационный документ

Когда это применимо, должна предоставляться нижеследующая информация в трех экземплярах, включая оглавление. Любые чертежи представляют в соответствующем масштабе, в достаточно подробном виде и в формате А4 или в кратном ему формате. Фотографии, если они имеются, должны быть достаточно четкими.

1. Марка (торговое наименование изготовителя):
2. Тип и общее(ие) коммерческое(ие) описание(я):
3. Средства идентификации типа, если такая маркировка имеется на транспортном средстве:
4. Место нанесения маркировки:
5. Категория(и) транспортного средства:
6. Фамилия и адрес изготовителя/представителя изготовителя:
7. Название(я) и адрес(а) сборочного(ых) предприятия(й):
8. Фотография(и) и/или чертеж(и) репрезентативного транспортного средства:
9. Кибербезопасность
 - 9.1 Общие характеристики конструкции типа транспортного средства, включая:
 - a) системы транспортных средств, которые имеют отношение к кибербезопасности данного типа транспортного средства;
 - b) компоненты тех систем, которые имеют отношение к кибербезопасности;
 - c) взаимодействие этих систем с другими системами, относящимися к данному типу транспортного средства, и с внешними интерфейсами транспортного средства.
 - 9.2 Схематическое изображение типа транспортного средства
 - 9.3 Номер свидетельства о соответствии СОБиК:
 - 9.4 Документы для официального утверждения типа транспортного средства с описанием результатов оценки рисков и выявленных рисков:
 - 9.5 Документы для официального утверждения типа транспортного средства с описанием мер по смягчению последствий, которые были осуществлены на перечисленных системах, и того, каким образом они позволяют устранить указанные риски:
 - 9.6 Документы для официального утверждения типа транспортного средства с описанием специальных объектов для хранения и реализации программного обеспечения, услуг, приложений или данных в интересах вторичного рынка:
 - 9.7 Документы для официального утверждения типа транспортного средства с описанием испытаний, которые были проведены для проверки кибербезопасности данного типа транспортного средства и его систем, и результатов этих испытаний:
 - 9.8 Описание факторов, связанных с цепочкой поставок, с точки зрения кибербезопасности:

Приложение 1 – Добавление 1

Образец заявления изготовителя о соответствии СОКиБ

Заявление изготовителя о соблюдении требований, предъявляемых к системе обеспечения кибербезопасности

Наименование изготовителя:

Адрес изготовителя:

..... (*Наименование изготовителя*) подтверждает,
что процессы, необходимые для соблюдения требований, касающихся системы
обеспечения кибербезопасности, изложенные в пункте 7.2 Правил ООН 155,
налажены и будут поддерживаться.

Совершено в: (*место*)

Дата:

Имя подписавшего лица:

Функция подписавшего лица:

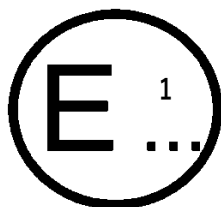
.....

(*Штамп и подпись представителя изготовителя*)

Приложение 2

Сообщение

(Максимальный формат: A4 (210×297 мм))



направленное: Название административного органа:

.....

касающееся²: предоставления официального утверждения
 распространения официального утверждения
 отзыва официального утверждения начиная с дд/мм/гггг
 отказа в официальном утверждении
 окончательного прекращения производства

типа транспортного средства на основании Правил № ООН 155

Официальное утверждение №:

Распространение №:

Основание для распространения:

1. Марка (торговое наименование изготовителя):
2. Тип и общее(ие) коммерческое(ие) описание(я):
3. Средства идентификации типа, если такая маркировка имеется на транспортном средстве:
- 3.1 Место нанесения маркировки:
4. Категория(и) транспортного средства:
5. Фамилия и адрес изготовителя/представителя изготовителя:
6. Название(я) и адрес(а) производственного(ых) предприятия(й):
7. Номер свидетельства о соответствии системы обеспечения кибербезопасности:
8. Техническая служба, ответственная за проведение испытаний:
9. Дата протокола испытания:
10. Номер протокола испытания:
11. Замечания: (при наличии)
12. Место:
13. Дата:
14. Подпись:
15. К настоящему прилагается указатель информационной документации, которая была сдана органу по официальному утверждению и которая может быть получена по запросу.

¹ Отличительный номер страны, которая предоставила/распространила официальное утверждение/отказала в официальном утверждении/отозвала официальное утверждение (см. положения настоящих Правил, касающиеся официального утверждения).

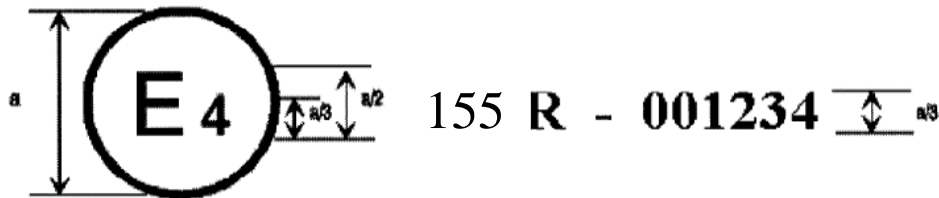
² Ненужное вычеркнуть.

Приложение 3

Схема знака официального утверждения

Образец А

(См. пункт 4.2 настоящих Правил)



$a = 8$ мм мин.

Приведенный выше знак официального утверждения, проставленный на транспортном средстве, указывает, что этот тип транспортного средства был официально утвержден в Нидерландах (E 4) на основании Правил № 155 и под номером официального утверждения 001234. Первые две цифры номера официального утверждения указывают на то, что официальное утверждение было предоставлено в соответствии с предписаниями настоящих Правил в их первоначальном варианте (00).

Приложение 4

Образец свидетельства о соответствии СОКиБ

Свидетельство о соответствии системы обеспечения кибербезопасности

Правилам ООН № [*настоящим Правилам*]
номер свидетельства [*идентификационный номер*]
[..... *орган по официальному утверждению*]
удостоверяет, что

Изготовитель:

Адрес изготовителя:

соблюдает положения пункта 7.2 Правил № 155.

Проверки проведены (дата):

(кем) (название и адрес органа по официальному утверждению или технической
службы):

Номер протокола испытания:

Свидетельство действительно до [..... *дата*]

Совершено в [..... *место*]

[..... *дата*]

[..... *подпись*]

Приложения: описание системы обеспечения кибербезопасности изготовителем.

Приложение 5

Перечень угроз и соответствующих мер по смягчению последствий

1. Настоящее приложение состоит из трех частей. В части А настоящего приложения описываются исходные данные об угрозах, факторах уязвимостях и методах атаки. В части В настоящего приложения описываются меры по смягчению последствий угроз, которые предназначены для типов транспортных средств. В части С описываются меры по смягчению последствий угроз, которые предназначены для зон, расположенных за пределами транспортных средств, например внутренних серверов.
2. Части А, В и С 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 А. Та же система индексации используется и в таблицах, содержащихся в частях В и С, 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 А

Факторы уязвимости или методы атаки, связанные с угрозами

1. Высокоуровневые описания угроз и связанных с ними факторов уязвимости или методов атаки приведены в таблице А1.

Таблица А1

Перечень факторов уязвимости или методов атак, связанных с угрозами

<i>Высокоуровневые и подуровневые описания уязвимости/угрозы</i>			<i>Пример уязвимости или метода атаки</i>	
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)

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, 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 действий, удаления или внесения других изменений в бортовой код/данные транспортного средства	5.1	Каналы передачи данных допускают внедрение кода , например в коммуникационный канал может быть внедрен подложный двоичный код программного обеспечения
			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	8.1	Отправка большого количества ненужных данных в информационную систему транспортного средства, чтобы она не могла предоставлять услуги в обычном режиме

Высокоуровневые и подуровневые описания уязвимости/угрозы		Пример уязвимости или метода атаки	
	виде отказа в обслуживании	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
		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

Высокоуровневые и подуровневые описания уязвимости/угрозы			Пример уязвимости или метода атаки	
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, иммобилайзер 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 системы транспортных средств	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	
		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)

Высокоуровневые и подуровневые описания уязвимости/угрозы		Пример уязвимости или метода атаки		
			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

Высокоуровневые и подуровневые описания уязвимости/угрозы			Пример уязвимости или метода атаки	
	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)
	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 В

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 В1.

Таблица В1

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

Ссылка на таблицу А1	Угрозы, связанные с «Каналами передачи данных транспортных средств»	Ссылка	Смягчение последствий
4.1	Спуфинг сообщений (например, 802.11р 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

<i>Ссылка на таблицу A1</i>	<i>Угрозы, связанные с «Каналами передачи данных транспортных средств»</i>	<i>Ссылка</i>	<i>Смягчение последствий</i>
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
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

<i>Ссылка на таблицу A1</i>	<i>Угрозы, связанные с «Каналами передачи данных транспортных средств»</i>	<i>Ссылка</i>	<i>Смягчение последствий</i>
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»

<i>Ссылка на таблицу A1</i>	<i>Угрозы, связанные с «Процессом обновления»</i>	<i>Ссылка</i>	<i>Смягчение последствий</i>
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

<i>Ссылка на таблицу A1</i>	<i>Угрозы, связанные с «Процессом обновления»</i>	<i>Ссылка</i>	<i>Смягчение последствий</i>
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»

<i>Ссылка на таблицу A1</i>	<i>Угрозы, связанные с «Непреднамеренными действиями человека»</i>	<i>Ссылка</i>	<i>Смягчение последствий</i>
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»

<i>Ссылка на таблицу A1</i>	<i>Угрозы, связанные с «Внешними подключениями и соединениями»</i>	<i>Ссылка</i>	<i>Смягчение последствий</i>
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

Ссылка на таблицу А1	Угрозы, связанные с «Внешними подключениями и соединениями»	Ссылка	Смягчение последствий
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	<p>Программное обеспечение оценивают с точки зрения безопасности, удостоверяют его подлинность и обеспечивают защиту его целостности</p> <p>Для сведения к минимуму риска, связанного с использованием программного обеспечения третьей стороны, которое предназначено для размещения на транспортном средстве, применяют средства контроля защиты</p>
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 В5.

Таблица В5

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

<i>Ссылка на таблицу А1</i>	<i>Угрозы, связанные с «Потенциальными целями или мотивировкой атаки»</i>	<i>Ссылка</i>	<i>Смягчение последствий</i>
19.1	Извлечение патентованного или собственного программного обеспечения из систем транспортного средства (фальсификация продукта/хищение программного обеспечения)	М7	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.	М8	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	М11	В целях хранения криптографических ключей обеспечиваются соответствующие средства контроля защиты, например модули безопасности
20.1	Противоправные/несанкционированные изменения в электронной идентификации транспортного средства	М7	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)	М7	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		

Ссылка на таблицу A1	Угрозы, связанные с «Потенциальными целями или мотивировкой атаки»	Ссылка	Смягчение последствий
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)
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 В6

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

<i>Ссылка на таблицу А1</i>	<i>Угрозы, связанные с «Потенциальными факторами уязвимости, которыми можно воспользоваться в случае недостаточной защиты или надежности»</i>	<i>Ссылка</i>	<i>Смягчение последствий</i>
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
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		

<i>Ссылка на таблицу A1</i>	<i>Угрозы, связанные с «Потенциальными факторами уязвимости, которыми можно воспользоваться в случае недостаточной защиты или надежности»</i>	<i>Ссылка</i>	<i>Смягчение последствий</i>
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 В7.

Таблица В7

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

<i>Ссылка на таблицу A1</i>	<i>Угрозы, связанные с «Потерями данных/утечкой данных из транспортного средства»</i>	<i>Ссылка</i>	<i>Смягчение последствий</i>
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 В8.

Таблица В8

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

<i>Ссылка на таблицу A1</i>	<i>Угрозы, связанные с «Физическим манипулированием системами, которое может создать возможность для атаки»</i>	<i>Ссылка</i>	<i>Смягчение последствий</i>
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 С

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 С1.

Таблица С1

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

<i>Ссылка на таблицу А1</i>	<i>Угрозы, связанные с «Внутренними серверами»</i>	<i>Ссылка</i>	<i>Смягчение последствий</i>
1.1 и 3.1	Злоупотребление привилегиями штатными сотрудниками (внутренняя атака)	М1	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)	М2	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)	М8	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	М3	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	М4	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

<i>Ссылка на таблицу A1</i>	<i>Угрозы, связанные с «Внутренними серверами»</i>	<i>Ссылка</i>	<i>Смягчение последствий</i>
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 С2.

Таблица С2

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

<i>Ссылка на таблицу A1</i>	<i>Угрозы, связанные с «Непреднамеренными действиями человека»</i>	<i>Ссылка</i>	<i>Смягчение последствий</i>
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

3. Меры по смягчению последствий в случае «Физической потери данных»

Меры по смягчению последствий угроз, которые связаны с «Физической потерей данных», перечислены в таблице С3.

Таблица С3

Меры по смягчению последствий угроз, которые связаны с «Физической потерей данных»

<i>Ссылка на таблицу А1</i>	<i>Угрозы, связанные с «Физической потерей данных»</i>	<i>Ссылка</i>	<i>Смягчение последствий</i>
30.1	Ущерб, причиненный третьей стороной. В случае дорожно-транспортного происшествия или кражи конфиденциальные данные могут быть утеряны или скомпрометированы в результате физических повреждений	M24	При хранении персональных данных необходимо следовать передовым методам защиты целостности и конфиденциальности данных. Примеры средств контроля защиты можно найти в ISO/SC27/WG5
30.2	Утрата в результате коллизий на уровне УЦР (управление цифровыми правами). Данные пользователя могут быть удалены в случае проблем с УЦП		
30.3	Целостность конфиденциальных данных или сами данные могут быть утеряны в случае морального и физического износа компонентов, что вызовет потенциальный каскадный эффект (например, в случае изменения ключа)		