Экономический и Социальный Совет

Distr.: General
19 November 2018
Russian
Original: English

Европейская экономическая комиссия

Комитет по внутреннему транспорту

Всемирный форум для согласования правил в области транспортных средств

Рабочая группа по автоматизированным/автономным и подключенным транспортным средствам*

Вторая сессия
Женева, 28 января – 1 февраля 2019 года
Пункт 5 b) предварительной повестки дня
Автоматизированные/автономные и подключенные транспортные средства: кибербезопасность и защита данных

Предложение по рекомендации, касающейся кибербезопасности

Представлено экспертами Целевой группы по вопросам кибербезопасности и беспроводной связи**

Настоящее предложение было подготовлено экспертами Целевой группы по вопросам кибербезопасности и беспроводной связи в целях обновления соответствующих вопросов в порядке осуществления мандата, согласованного Всемирным форумом для согласования правил в области транспортных средств (WP.29), который отражен в документах ECE/TRANS/WP29/1126, пункт 28, и ECE/TRANS/WP29/1131, пункт 27. В его основу положен неофициальный документ GRVA-01-17, представленный ранее на первой сессии Рабочей группы по автоматизированным/автономным и подключенным транспортным средствам (GRVA) в сентябре 2018 года. В приложении A к настоящему документу содержится проект правил ООН по вопросам кибербезопасности. Этот проект правил содержит четыре приложения (приложения 1–4), относящиеся к приложению A.

* Прежнее название: **Рабочая группа по вопросам торможения и ходовой части (GRRF)**.

** В соответствии с программой работы Комитета по внутреннему транспорту на 2018–2019 годы (ECE/TRANS/274, пункт 123, и ECE/TRANS/2018/21/Add.1, направление деятельности 3) Всемирный форум будет разрабатывать, согласовывать и обновлять правила ООН в целях улучшения характеристик транспортных средств. Настоящий документ представлен в соответствии с этим мандатом.

GE.18-19708 (R) 171218 181218

1819708

Содержание

Стр.

I. Введение 3

A. Преамбула 3

B. Сфера применения 4

C. Подход 4

II. Определения (и сокращения) 5

III. Принципы кибербезопасности 6

IV. Угрозы для транспортных средств 7

V. Смягчение последствий 9

VI. Требования, касающиеся процессов кибербезопасности и способов подтверждения их применения 11

VII. Заключение и рекомендация по поводу дальнейшей работы 13

Приложения

A Проект предложения по введению в действие Правил ООН по кибербезопасности 17

B Перечень угроз и соответствующих мер по смягчению последствий 29

C Перечень средств защиты, связанной со смягчением последствий 44

D Перечень справочных документов 59

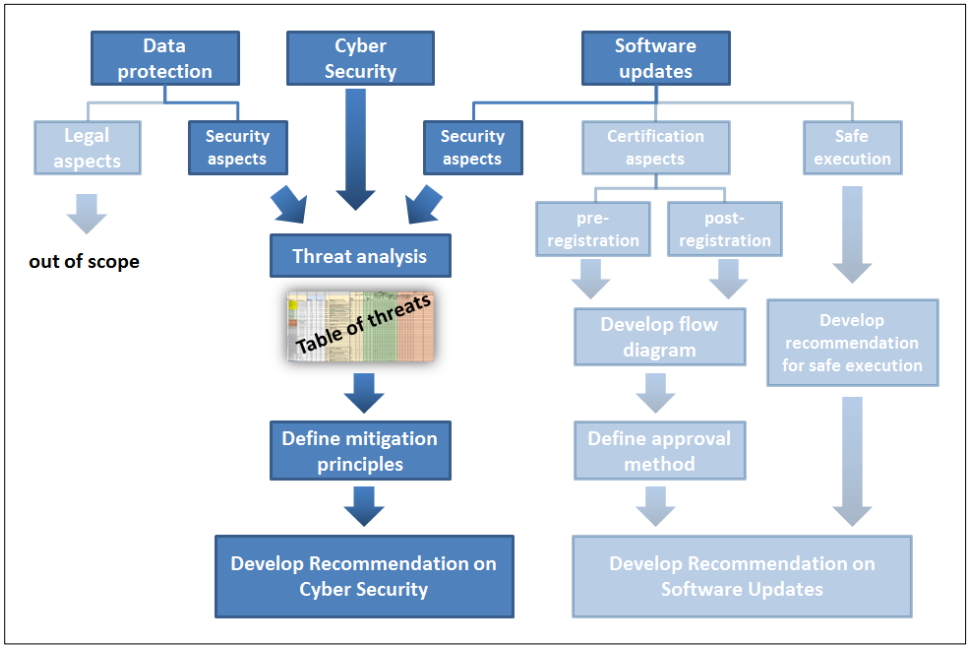
I. Введение

A. Преамбула

1.1 Эта Целевая группа была создана в качестве одной из подгрупп в рамках неофициальной рабочей группы по интеллектуальным транспортным системам/автоматизированному вождению (НРГ по ИТС/АВ) WP.29 в целях решения вопросов кибербезопасности и беспроводной связи. В состав этой Целевой группы входили члены, представляющие Договаривающиеся стороны и неправительственные организации, в частности Европейскую ассоциацию поставщиков автомобильных деталей (КСАОД), Международный комитет по техническому осмотру автотранспортных средств (МКТАС), Международную автомобильную федерацию (МАФ), Международный союз электросвязи (МСЭ) и Международную организацию предприятий автомобильной промышленности (МОПАП).

1.2 Сфера применения тех позиций, которые охватываются настоящей рекомендацией, наглядно отображена на рисунке 1. В этой связи следует отметить, что между защитой данных, кибербезопасностью и обновлением программного обеспечения есть общие черты. Для обновления программного обеспечения характерны аспекты безопасности, аспекты сертификации и аспекты безопасной реализации, которые необходимо тщательно рассмотреть. Целевая группа определила, что вопросы кибербезопасности и беспроводной связи – это разные вопросы, которые будут анализироваться отдельно. Здесь изложены результаты рассмотрения проблемы кибербезопасности, включая проблему обновления программного обеспечения. Проблемы управления процессами обновления программного обеспечения и официального утверждения типа рассматриваются в отдельном документе под названием «Рекомендация по вопросам беспроводной связи Целевой группы по вопросам кибербезопасности и беспроводной связи НРГ по ИТС/АВ WP.29 ЕЭК ООН».

Рис. 1.
Деятельность и результаты работы Целевой группы



1.3 В своей работе Целевая группа учла документ под названием ECE/TRANS/WP.29/2017/46 «Руководящие положения по кибербезопасности и защите данных», разработанные НРГ по ИТС/АВ, и

другие соответствующие стандарты, виды практики, директивы и правила, касающиеся кибербезопасности. Они включают некоторые положения, которые находятся на стадии разработки, а также существующие стандарты, которые применяются в отрасли автомобилестроения. Ссылки на эти документы указаны в приложении D.

1.4 В настоящем документе находят отражение современные подходы, которые использовались на этапе подготовки этого документа. По этой причине содержащиеся здесь рекомендации нуждаются в периодическом пересмотре с целью обеспечить учет новых и возникающих угроз и вариантов смягчения их последствий и, по мере необходимости, в их обновлении. В этой связи GRVA необходимо осуществлять надзор за их осуществлением и инициировать эти обновления.

B. Сфера применения

1.5 В этом документе определяются принципы устранения основных выявленных угроз и факторов уязвимости в киберпространстве с целью обеспечить безопасность транспортного средства в случае кибератак. Кроме того, в нем содержатся подробные указания или меры, касающиеся способов соблюдения этих принципов, а также примеры соответствующих процессов и технических подходов. И наконец, в нем рассматриваются оценки или фактические данные, которые могут потребоваться для подтверждения соответствия любым выявленным требованиям или их сертификации.

1.6 Транспортные средства обрабатывают целый ряд различных типов данных. В настоящем документе определяются принципы, которые должны быть разработаны в целях защиты таких данных в результате несанкционированного доступа, а также их изменения или удаления как во время их хранения, так и во время их передачи.

C. Подход

1.7 В целях идентификации основных угроз и факторов уязвимости транспортных средств был проведен соответствующий анализ, после чего были определены основные меры по смягчению их последствий, которые необходимы для их ограничения или сведения к минимуму. Это было сделано преднамеренно с целью убедиться в том, что полученные результаты не предполагают необходимость принятия конкретных технических решений (тем не менее их можно привести в качестве примера). Затем эти основные меры по смягчению последствий были представлены в качестве соответствующих принципов.

1.8 Анализ соответствующих угроз был проведен с учетом самых последних технических достижений. Перечень угроз был составлен с учетом многих источников (см. приложение B). Полученный перечень нельзя считать исчерпывающим, однако он позволяет весьма наглядно проиллюстрировать возможные киберугрозы, которым могут подвергаться транспортные средства. В нем рассматривается то, каким образом могут проявляться эти угрозы, и приводятся конкретные примеры того, каким образом они могут сказаться на том или ином транспортном средстве.

1.9 Эти угрозы были распределены по группам на основе аналогии их характеристик, и по каждой группе был составлен соответствующий перечень мер по смягчению последствий. Они предусматривают один или несколько способов, с помощью которых можно было бы смягчить последствия выявленных примеров угроз (см. приложение C). Меры по смягчению последствий были оформлены в качестве принципов, которые необходимо соблюдать; в некоторых случаях предусматриваются

конкретные решения в качестве примера того, каким образом можно было бы обеспечить их соблюдение, однако включать их в правила не планируется.

II. Определения

2. Для целей настоящей рекомендации применяются следующие определения:

2.1 «*рынок послепродажного обслуживания*» означает вторичный рынок автомобильной промышленности, включающий изготовление, восстановление, распределение, розничную торговлю и монтаж всех частей транспортного средства, программное обеспечение, услуги, химикаты, оборудование и вспомогательные приспособления после продажи автомобиля потребителю изготовителем транспортного средства для клиента;

2.2 «*аутентификация*» означает способ подтверждения гарантии того, что заявленные характеристики данного материального объекта соответствуют действительности;

2.3 «*доступ*» означает получение права на использование того или иного ресурса»;

2.4 «*автомобильная промышленность*» означает изготовители, поставщики, субъекты технического обслуживания, поставщики систем и услуг, которые взаимодействуют с транспортными средствами;

2.5 «*кибербезопасность*» означает условия, в которых автотранспортные средства и их функции защищены от угроз, которым могут подвергаться электрические и электронные компоненты;

2.6 «*система обеспечения кибербезопасности (СОКиБ)*» означает систематический подход, основанный на оценке риска организационных процессов, обязанностей и системы руководства в целях смягчения киберугроз и защиты транспортных средств от кибератак;

2.7 «*защита данных*» означает реализацию соответствующих административных, технических или физических средств в целях защиты от несанкционированного, преднамеренного или случайного разглашения, изменения или уничтожения данных;

2.8 «*глубокоэшелонированная защита*» означает систему с несколькими уровнями защиты, которая обеспечивает полную защиту даже в случае отказа или обхода одного из уровней защиты;

2.9 «*жизненный цикл*» означает временной интервал существования транспортного средства с момента его первоначальной разработки, на протяжении его периода сбыта и активной эксплуатации и до момента его возможного физического и морального износа.

2.10 «*срок службы*» означает срок службы транспортного средства с точки зрения кибербезопасности в течение всего периода с момента первоначальной регистрации транспортного средства до момента его изъятия из эксплуатации.

2.11 «*смягчение последствий*» означает соответствующую меру, которая позволяет изменить степень риска.

2.12 «*организация*» означает лицо или группу лиц, у которого или у которой есть свои собственные функции, предусматривающие соответствующие обязанности, полномочия и взаимоотношения, необходимые для достижения своих целей;

2.13 «*обновление беспроводной связи*» означает любой метод, позволяющий производить беспроводную передачу данных без использования проводов или другой локальной системы связи;

2.14 «*риск*» означает эффект воздействия неопределенности на цели в области безопасности;

2.15 «*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);

2.16 «*управление риском*» означает согласованные действия по руководству и управлению соответствующей организацией в связи с риском;

2.17 «*система*» означает набор компонентов и подсистем, который воплощает в себе некоторую особенность

2.18 «*угроза*» означает потенциальную причину нежелательного инцидента, который может нанести ущерб системе или организации;

2.19 «*уязвимость*» означает слабость какого-либо материального объекта или средства контроля, которая дает возможность реализации одной или нескольких угроз.

III. Принципы кибербезопасности

3.1 Принципы кибербезопасности можно использовать для того, чтобы показать каким образом организациям следует обеспечивать кибербезопасность на протяжении всего жизненного цикла транспортного средства. Их могут использовать изготовители транспортных средств, субподрядчики, поставщики и провайдеры услуг.

3.2 Процедура наглядного подтверждения того, каким образом можно соблюдать эти принципы, в настоящем документе конкретно не определена. Вместе с тем организациям рекомендуется быть в состоянии подтвердить – на основе использования соответствующих стандартов (таких как ISO/SAE 21434), процессов и мер по смягчению последствий – то, каким образом они соблюдают те принципы, которые соответствуют требованиям органов власти.

3.3 Принципы кибербезопасности включают следующее:

3.3.1 вопросы безопасности в организации должны быть подотчетны, регулироваться и продвигаться на самом высоком организационном уровне;

3.3.2 риски в области безопасности оценивают и регулируют надлежащим и соразмерным образом, в том числе те, которые специфичны для данной производственно-сбытовой цепочки;

3.3.3 организациям следует осуществлять мониторинг и реагировать на инциденты в сфере кибербезопасности с целью обеспечивать безопасность систем на протяжении их срока службы;

3.3.4 всем организациям, включая субподрядчиков, поставщиков и потенциальных третьих сторон, следует работать сообща в целях повышения уровня безопасности всей системы;

3.3.5 Транспортное средство следует проектировать с учетом принципа глубокоэшелонированной защиты. Изготовитель транспортного средства должен разрабатывать архитектуру транспортного средства таким образом, чтобы снизить вероятность того, что ослабление параметров одного архитектурного элемента может привести к распространению угрозы на другие архитектурные элементы;

3.3.6 безопасность программного обеспечения должна находиться под контролем на протяжении всего срока службы;

3.3.7 процесс хранения и передачи данных должен быть безопасным и находиться по контролем;

3.3.8 изготовитель транспортного средства должен оценивать функции обеспечения безопасности с помощью соответствующих процедур тестирования;

3.3.9 транспортное средство должно быть спроектировано таким образом, чтобы оно было устойчивым к кибератакам;

3.3.10 транспортное средство должно быть спроектировано таким образом, чтобы оно было в состоянии выявлять кибератаки и реагировать на них надлежащим образом.

IV. Угрозы для транспортных средств

4.1 Угрозы, определенные в настоящем документе, могут использоваться сторонами, участвующими в процессе внедрения, разработки или модификации соответствующих продуктов или услуг, которые являются частью транспортных средств или взаимодействуют с ними. Угрозы, включенные в перечень, отражают современное состояние техники на момент его закрепления в письменной форме, но в случае их использования эти угрозы необходимо будет подвергать повторной оценке на предмет их полноты. Их следует использовать в качестве основы для обеспечения надлежащего снижения рисков. Их можно также использовать в качестве подспорья при определении уровня уязвимости в случае потенциальных киберугроз и в процессе принятия надлежащих мер для снижения этих рисков.

4.2 В настоящем разделе приводится подробная информация об угрозах и факторах уязвимости, которые могут существовать. Более подробный перечень примеров возможных угроз, которыми можно воспользоваться, приводится в приложении B.

4.3 Ниже содержится описание уровня возможных угроз и факторов уязвимости, которые необходимо рассмотреть при разработке новых или модифицированных продуктов или услуг. Номера, указанные в каждом подпункте, представляют собой перекрестную ссылку, указывающую на то, как они изложены в приложении B:

4.3.1 Угрозы в отношении внутренних серверов:

a) внутренние серверы, используемые в качестве средства кибератаки на транспортное средство или извлечения данных (1.);

b) нарушение работы внутренних серверов, которое отрицательно сказывается на эксплуатации транспортного средства (2.);

c) данные, хранящиеся на внутренних серверах, утрачены или нарушены («уязвимость» данных) (3.).

4.3.2 Угрозы в отношении транспортных средств, касающиеся их каналов передачи данных:

a) умышленное искажение сообщений или данных, полученных транспортным средством (4.);

b) каналы передачи данных, используемые для осуществления несанкционированных действий, удаления или внесения других изменений в бортовой код/данные транспортного средства (5.);

c) каналы передачи данных допускают прием недостоверных/ненадежных сообщений или уязвимы в случае сеансов связи/атаки с повторным навязыванием сообщения (6.);

d) информацию можно легко раскрыть, например путем подслушивания сообщений или несанкционированного доступа к секретным файлам или папкам (7.);

e) атаки по каналам передачи данных в целях нарушения функций транспортного средства в виде отказа в обслуживании (8.);

f) пользователь со стороны может получить привилегированный доступ к системам транспортного средства (9.);

g) вирусы, занесенные в коммуникационную среду, могут инфицировать системы транспортного средства (10.);

h) сообщения, полученные транспортным средством (например, X2V или диагностические сигналы) или переданные вместе с ним, содержат вредоносный контент (11.).

4.3.3 Угрозы в отношении транспортных средств, касающиеся их процедур обновления:

a) злоупотребление процедурами обновления или их нарушение (12.);

b) возможность отказа в правомерном обновлении (13.).

4.3.4 Угрозы в отношении транспортных средств, касающиеся непреднамеренных действий человека:

a) нарушение конфигурации оборудования или систем правомерным субъектом, например владельцем или организацией технического обслуживания (14.);

b) правомерные субъекты способны принимать меры, которые могут невольно облегчить кибератаку (15.).

4.3.5 Угрозы в отношении транспортных средств, касающиеся взаимодействия с внешними объектами и подключения к ним:

a) манипуляция со средствами взаимодействия функций транспортного средства открывает возможность для кибератаки: это может включать средства телематики; системы, которые дают возможность осуществления дистанционных операций; и системы, использующие средства беспроводной связи ближнего радиуса действия (16.);

b) размещение программного обеспечения третьей стороной, например развлекательных прикладных программ, используемых в качестве одного из средств для атаки систем транспортных средств (17.);

c) устройства, подключенные к внешним интерфейсам, например порты USB или порты OBD, используемые в качестве одного из средств для атаки систем транспортных средств (18.).

4.3.6 Потенциальные цели или мотивировка атаки:

a) извлечение данных/кода транспортного средства (19.);

b) манипуляция с данными/кодом (20.);

c) стирание данных/кода (21.);

d) внедрение вредоносных программ (22.);

e) введение в действие нового программного обеспечения или затирание существующего программного обеспечения (23.);

f) нарушение работы систем или операций (24.);

g) манипуляция с параметрами транспортного средства (25.).

4.3.7 Потенциальные факторы уязвимости, которыми можно воспользоваться в случае недостаточной защиты или надежности:

a) криптографические технологии, которые могут быть нарушены или которые применяются неадекватно (26.);

b) части или принадлежности компонентов, которые могут быть нарушены в целях создания возможности для атаки транспортных средств (27.);

c) разработка программного обеспечения или аппаратных средств, которая создает возможность возникновения факторов уязвимости (28.);

d) дизайн сети, который допускает возникновение факторов уязвимости (29.);

e) возможность физической утраты данных (30.);

f) возможность непреднамеренной передачи данных (31.);

g) физическая манипуляция с системами, которая может создать возможность для атаки (32.).

4.3.8 Анализ угроз должен также учитывать последствия возможных атак. Они могут оказать помощь в выяснении степени того или иного риска и выявлении дополнительных рисков. Возможные последствия атаки могут включать:

a) нарушение безопасной работы транспортного средства;

b) отказ некоторых функций транспортного средства;

c) модификация программного обеспечения, снижение эффективности;

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

e) нарушение целостности данных;

f) нарушение конфиденциальности данных;

g) утрата возможности вывода данных;

h) другие, включая преступные действия.

4.4 Более детальные примеры факторов уязвимости или способов осуществления атаки приводятся напротив каждой позиции в таблице 1 приложения B. Ими можно воспользоваться в целях более глубокого понимания позиций, приведенных выше. Можно предположить, что с течением времени будут возникать новые и непредвиденные примеры факторов уязвимости и способов осуществления атак. По этой причине ни содержащийся выше перечень, ни приведенные здесь примеры нельзя считать исчерпывающими.

V. Смягчение последствий

5.1 В настоящем разделе приводится перечень мер, которые следует рассмотреть в процессе разработки новых или модифицированных продуктов или услуг в целях уменьшения выявленных угроз и рисков. В этом перечне на английском языке используются позиции «shall», которые носят характер обязательства, и позиции «should», которые носят характер долженствования и в случае применимости будут рассмотрены позднее.

5.1.1 В целях сведения к минимуму риска атаки штатным персоналом к серверным системам применяют соответствующие средства защиты.

5.1.2 В целях сведения к минимуму риска несанкционированного доступа к серверным системам применяют соответствующие средства защиты.

5.1.3 Если для целей обслуживания решающее значение имеют внутренние серверы, то в случае перебоев в работе следует предусмотреть систему мер по восстановлению данных.

5.1.4 В целях сведения к минимуму рисков, связанных с облачной обработкой компьютерных данных, применяют соответствующие средства защиты.

5.1.5 В целях предотвращения нарушения целостности данных к внутренним серверным системам применяют соответствующие средства защиты.

5.1.6 В целях сведения к минимуму воздействия атаки на транспортное средство применяют соответствующий принцип безопасности на этапе проектирования.

5.1.7 В целях защиты данных/кода системы применяют соответствующие методы контроля за доступом и соответствующие конструктивные особенности.

5.1.8 Возможность несанкционированного доступа к личным данным или важнейшим данным системы необходимо исключить на этапе проектирования системы и контроля за доступом.

5.1.9 Применяют меры по предупреждению и выявлению случаев несанкционированного доступа.

5.1.10 Транспортное средство проверяет аутентичность и целостность сообщений, которые оно получает.

5.1.11 В целях хранения криптографических ключей обеспечиваются соответствующие средства защиты.

5.1.12 Конфиденциальные данные, передаваемые на транспортное средство или транспортным средством подлежат соответствующей защите.

5.1.13 Меры по выявлению взлома функции отказа в обслуживании и ее восстановлению подлежат рассмотрению.

5.1.14 Меры по защите от внедренных вирусов/вредоносных программ подлежат рассмотрению.

5.1.15 Меры по выявлению злонамеренных внутренних сообщений или деятельности подлежат рассмотрению.

5.1.16 Применяют безопасные процедуры обновления программного обеспечения.

5.1.17 В целях определения процедуры технического обслуживания и контроля за ними принимают соответствующие меры.

5.1.18 В целях определения и проверки ролей пользователей и привилегий доступа, основанных на принципе наименьшей привилегии доступа, принимают соответствующие меры.

5.1.19 Организации обеспечивают безопасность процедур и следят за их применением.

5.1.20 В случае систем с дистанционным доступом применяют соответствующие средства защиты.

5.1.21 Программное обеспечение оценивают, удостоверяют его подлинность и обеспечивают защиту его целостности.

5.1.22 К внешним интерфейсам применяют соответствующие меры защиты.

5.1.23 В процессе разработки программного обеспечения и аппаратных средств соблюдают современные виды практики в области кибербезопасности.

5.1.24 В целях хранения частных и конфиденциальных данных соблюдают современные виды практики.

5.1.25 Системы следует проектировать таким образом, чтобы они надлежащим образом реагировали в случае выявления атаки на транспортное средство.

5.2 В приложениях B и C приводятся примеры смягчения последствий, которые можно использовать. Они не носят исчерпывающий характер и могут не подходить для применения в конкретных случаях реализации данного изделия или данной услуги на практике.

5.3 В целях оказания содействия в выявлении конкретных мер по смягчению последствий каждый пример угрозы можно оценить с помощью «расширенного подхода КЦД». В процессе этой оценки следует рассмотреть вопрос о том, каким образом можно инициировать и распространить атаку, связанную с угрозой или уязвимостью, на все сети того или иного транспортного средства. В указанном выше расширенном подходе КЦД определены семь целей:

a) конфиденциальность,

b) целостность,

c) доступность,

d) отказоустойчивость,

e) аутентичность,

f) контролируемость,

g) разрешение.

VI. Требования, касающиеся процессов обеспечения кибербезопасности и способов подтверждения их применения

6.1 В настоящем разделе описывается, какие данные должны представить изготовители того или иного транспортного средства соответствующему компетентному органу, которые свидетельствовали бы о том, что они учитывают угрозы, меры по смягчению последствий и принципы, применимые к их изделиям, с целью дать этим компетентным органам возможность подтвердить соответствие этих изделий установленным требованиям.

6.2 В данном разделе не указывается, каким образом изготовитель транспортного средства должен собрать необходимую информацию. Она может носить в данной организации внутренний характер или предполагать необходимость взаимодействия между различными организациями в рамках производственно-сбытовой цепочки (например, между изготовителем и поставщиком).

6.3 Сертификация системы обеспечения кибербезопасности

6.3.1 Соответствующую систему обеспечения кибербезопасности осуществляют изготовители транспортного средства.

6.3.2 Соответствующую систему обеспечения кибербезопасности осуществляют также поставщики и провайдеры услуг.

6.3.3 Поставщики и провайдеры услуг должны иметь возможность представить соответствующие данные об осуществлении своей системы обеспечения кибербезопасности.

6.3.4 Изготовитель транспортного средства подтверждает соответствующему компетентному органу, что их система обеспечения кибербезопасности строится с учетом следующих этапов:

6.3.4.1 этап разработки,

6.3.4.2 этап реализации,

6.3.4.3 этап после реализации.

6.3.5 Изготовитель транспортного средства подтверждает соответствующему компетентному органу, каким образом его система обеспечения кибербезопасности будет регулировать соответствующие аспекты взаимозависимости, которые могут существовать в его договорных отношениях с поставщиками изделий и провайдерами услуг.

6.3.6 Изготовитель транспортного средства организует процессы мониторинга рисков и угроз для своего транспортного средства и соответствующие процедуры реагирования на инциденты, определенные в своей системе обеспечения кибербезопасности.

6.4 Требования на этапе после изготовления транспортного средства:

6.4.1 Система кибербезопасности должна быть встроена и действовать в течение всего жизненного цикла транспортных средств.

6.4.2 Изготовитель транспортного средства показывает, каким образом он планирует поддерживать надлежащую защиту и соблюдение принципов кибербезопасности, изложенных в настоящем документе, на протяжении всего жизненного цикла транспортных средств. Эта способность необходима для того, чтобы он мог подтвердить тот факт, что безопасность и доступность его транспортного средства и системных функций будет поддерживаться и в условиях изменяющихся киберугроз. Это имеет особенно важное значение для обеспечения безопасности важнейших систем, в том числе для систем официального утверждения типа.

6.4.3 Организации, действующие в автомобильной промышленности, должны быть в состоянии определить, каким образом меняются с течением времени угрозы и факторы уязвимости для транспортных средств или систем, а также выявлять угрозы, которые не были выявлены или учтены на стадии разработки.

6.4.4 Организации, действующие в автомобильной промышленности, должны быть в состоянии оценить, являются ли принятые ими меры безопасности все еще эффективными в свете новых киберугроз или факторов уязвимости, которые они выявили. Они должны рассматривать вопрос о том, не снизился ли уровень безопасности или доступности данного транспортного средства или его функций.

6.4.5 Организации, действующие в автомобильной промышленности, должны располагать соответствующими процедурами реагирования на инциденты.

6.5 Официальное утверждение типа транспортного средства:

6.5.1 Официальное утверждение типа транспортного средства производят только в том случае, если система обеспечения кибербезопасности изготовителя данного транспортного средства получила свидетельство о соответствии СОКиБ.

6.5.2 Изготовитель транспортного средства подтверждает оценку риска для данного типа транспортного средства с точки зрения систем данного транспортного средства, взаимодействия различных систем этого транспортного средства и всего транспортного средства в целом.

6.5.3 Изготовитель транспортного средства обеспечивает реализацию важнейших конструктивных элементов транспортного средства, предназначенных для защиты от рисков, выявленных в ходе оценки риска изготовителем данного транспортного средства. Для защиты таких элементов принимаются соразмерные меры по смягчению их последствий.

6.5.4 Изготовитель транспортного средства осуществляет надлежащие и соразмерные меры для защиты специальных объектов (если таковые предусмотрены) в целях хранения и реализации программного обеспечения, услуг, приложений или данных в интересах вторичного рынка.

6.5.5 Данные, необходимые для официального утверждения транспортного средства, должны включать:

6.5.5.1 информацию о том, каким образом изготовитель данного транспортного средства учитывает угрозы и факторы уязвимости, в том числе те, которые подробно изложены в приложении A, в свою оценку рисков;

6.5.5.2 меры по смягчению последствий, которые принимает изготовитель транспортного средства в целях сведения к минимуму выявленных рисков до уровня, приемлемого для компетентного органа, посредством описания:

a) архитектуры и систем транспортного средства,

b) важнейших компонентов архитектуры и (под-)систем, имеющих отношение к кибербезопасности,

c) взаимодействия этих архитектур и систем с другими архитектурами, системами и внешними интерфейсами транспортного средства,

d) рисков, создаваемых для этих архитектур и систем, которые были выявлены в ходе оценки рисков,

e) мер по смягчению последствий, которые были приняты в случае перечисленных систем, и каким образом они позволяют устранить указанные риски.

6.5.6 В качестве доказательства в интересах официального утверждения типа изготовитель транспортного средства может указать, каким образом он применяет принципы кибербезопасности, определенные в настоящем документе.

VII. Заключение и рекомендация по поводу дальнейшей работы

7.1 Заключение этой рекомендации состоит в том, что:

7.1.1 Данная оценка была сделана на основе результатов проведенной работы и накопленных знаний и опыта заинтересованных сторон (см. приложение D) в целях разработки соответствующей рекомендации по кибербезопасности. Целевая группа считает, что она решила задачу, предусмотренную ее кругом ведения.

7.1.2 Уточнение технических решений было бы нецелесообразным, поскольку они не выдержали бы испытания временем и сдерживали бы процесс инноваций и конкуренции. По этой причине данная рекомендация не содержит таких решений, но при этом она включает примеры процессов, процедур и технологий, которые можно было бы рассмотреть в интересах обеспечения кибербезопасности;

7.1.3 Подтверждение способов, с помощью которых можно было бы выполнить требования, содержащиеся в настоящей рекомендации, не нуждается в четком определении. Вместо этого рекомендуется сделать так, чтобы изготовитель транспортного средства был в состоянии подтвердить органу по официальному утверждению – посредством использования соответствующих стандартов, процессов и применения надлежащих мер по смягчению последствий – каким образом он выполняет действующие требования;

7.1.4 Действие этой рекомендации охватывает весь жизненный цикл транспортного средства. Вопрос о том, каким образом оно выводится из эксплуатации и что происходит с данным транспортным средством после этого, в сферу действия этой рекомендации не входит.

7.2 В целях регулирования кибербезопасности будет необходимо представить следующее:

7.2.1 результаты проверки органом по официальному утверждению, подтверждающие, что процессы и процедуры изготовителя транспортного средства (как описано в его системе обеспечения кибербезопасности) подкрепляют осуществление рекомендации, содержащейся в настоящем документе,

7.2.2 одобрение органом по официальному утверждению того факта, что риски, выявленные в случае конкретного типа транспортного средства, были надлежащим образом оценены и что принятые меры по смягчению последствий в целях устранения этих рисков являются подходящими.

7.3 В целях оказания помощи в оценке системы обеспечения кибербезопасности, проведенного анализа рисков и принятых мер по смягчению их последствий в рекомендацию включено следующее:

7.3.1 принципы кибербезопасности, которые можно использовать для подтверждения того, каким образом организации должны обеспечивать кибербезопасность в течение всего срока эксплуатации транспортного средства,

7.3.2 примеры угроз, рисков, факторов уязвимости и произведенных атак, которые необходимо принять во внимание,

7.3.3 примеры мер по смягчению последствий, которые необходимо принять во внимание.

7.4 Ожидается, что со временем будут появляться примеры новых и непредвиденных факторов уязвимости и методов атаки. В этой связи приведенный здесь перечень примеров не следует рассматривать ни как исчерпывающий перечень, ни как перечень, который применим к каждой конструкции транспортного средства, – напротив, в тех случаях, когда они используются, их следует оценивать на предмет их полноты и применимости.

7.5 Целевая группа рекомендует доработать этот документ, разбив его на две части:

7.5.1 Основной текст (главы 1–6) и приложения B и C подлежат доработке в качестве официального рабочего документа для WP. 29. Кроме того, его можно использовать в качестве основы для резолюции по кибербезопасности, но при этом его, возможно, придется дополнительно подработать с целью привести его в соответствие с требуемым форматом.

7.5.2 Приложение A, в котором рассматриваются рекомендации, высказанные в пункте 7.2 выше, подлежит дальнейшей доработке в качестве правил ООН в соответствии с Соглашением 1958 года. Оно включает требования, касающиеся:

7.5.2.1 свидетельства изготовителя транспортного средства СОКиБ о соответствии системы обеспечения кибербезопасности,

7.5.2.2 официального утверждения типа транспортного средства в отношении кибербезопасности.

7.5.3 Приложение C может оказаться полезным для соответствующих заинтересованных сторон в качестве справочного документа. Для Правил ООН оно не подходит, поскольку оно носит информационный характер.

7.5.4 Приложение D для правил или резолюции не подходит. Оно предназначено только для данного документа.

7.5.5 Головная группа должна принять решение по поводу последующих шагов, например по поводу разработки соответствующих ГТП по кибербезопасности. Целевая группа отмечает, что для разработки таких ГТП потребуется дальнейшая работа.

7.5.6 Что касается нормативного приложения, то в него можно было бы включить категории L, O, R, S и T, но в Целевой группе они представлены недостаточно (в случае категории L) или не представлены вообще (в других случаях). Поэтому следует рассмотреть вопрос о том, нужно ли распространять данные правила и на эти категории транспортных средств.

7.5.7 Данное нормативное приложение предусматривает, что срок действия свидетельства о допущении СОКиБ должен составлять три года и что проверки соответствия производства следует также проводить раз в три года.

7.5.8 Целевая группа рекомендует проверить положения, содержащиеся в предлагаемых Правилах (приложение A), с целью удостовериться в том, что они являются юридически допустимыми в соответствии с Соглашением 1958 года, в частности, вопрос о том, не будут ли пункты 7.2.2.1 и 7.2.2.2 приложения A выходить за рамки того, что допускается нормативными положениями, регламентирующими официальное утверждение типа. По мнению Целевой группы, они должны быть допустимыми, но этот момент следует уточнить.

7.6 Будущие подвижки, которые можно было бы рассмотреть, включают:

7.6.1 Угрозы в области кибербезопасности могут возникнуть в любое время в течение всего срока службы транспортного средства. Целевая группа определяет соответствующие требования в пункте 7 приложении A «Спецификации» (и более конкретно в пункте 7.2 «Требования к организации изготовителя транспортного средства»). Эти требования в области кибербезопасности могут действовать в течение всего жизненного цикла транспортного средства (проектирование, производство и этап после производства). Вместе с тем Целевая группа признает, что после окончательного прекращения производства (в соответствии с Соглашением 1958 года) официальное утверждение типа может не действовать. Соответствующая правовая основа, регламентирующая совершенствование системы учета требований на этапе после производства, помимо тех, которые уже действуют, например требования к официальному утверждению типа, нуждается в дальнейшем рассмотрении.

7.6.2 В ходе анализа угроз, были выявлены определенные риски, которые, по мнению группы, выходят за рамки настоящего документа. Вместе с тем эти риски не следует упускать из виду, в связи с чем рекомендуется передать эти вопросы на рассмотрение соответствующему органу ООН.

7.6.3 Следует отметить, что проблематика кибербезопасности носит весьма динамичный характер. В этой связи рекомендуется обратить внимание на необходимость проведения периодического обзора этого документа с целью обеспечить отражение в нем новых и появляющихся угроз и мер по смягчению их последствий и по мере необходимости его обновления. Кроме того, необходимо будет контролировать и инициировать эти обзоры, восстанавливая по мере необходимости данную Целевую группу для проведения этой работы.

7.6.4 На момент составления настоящей рекомендации ИСО и ОИАТ разрабатывали новый совместный стандарт на инженерное обеспечение кибербезопасности автотранспортных средств «ISO/SAE 21434 Road Vehicles – Cybersecurity engineering». После того как этот стандарт будет находиться на подходящем этапе разработки, этот документ должен быть пересмотрен и при необходимости обновлен.

7.6.5 Было отмечено, что в будущем необходимо будет наладить диалог между соответствующими компетентными органами с целью обеспечить последовательный подход к официальному утверждению и что WP.1 ЕЭК ООН могла бы способствовать налаживанию этого диалога.

7.7 Рекомендации для осуществления

7.7.1 Целевая группа рекомендует предусмотреть соответствующий этап проверки этих Правил до их полного осуществления. Цель такого этапа будет заключаться в том, чтобы подтвердить и убедиться в том, что процедуры, предусмотренные как для изготовителей транспортных средств, так и для органов по официальному утверждению, работают так, как и планировалось, и разрешить в случае необходимости дальнейший пересмотр этих Правил. GRVA следует рассмотреть вопрос о том, что может потребоваться для такого этапа испытания.

7.7.2 Целевая группа рекомендует дать изготовителям транспортных средств и органам по официальному утверждению некоторое время до вступления этих Правил в силу для адаптации своих процессов с целью обеспечить их соответствие этим Правилам. GRVA следует рассмотреть вопрос о том, какой подходящий срок мог бы понадобится для этих целей, а также соответствующий график поэтапного введения в действие. Следует также отметить, что этот момент требуется увязать с необходимостью соответствующих действий в этой области.

Приложение A Проект предложения по введению в действие Правил ООН по кибербезопасности

Организация Объединенных Наций ECE/TRANS/WP.29/201x/xx

Экономический и Социальный Совет

Distr.: General
DD MM YYYY
Russian
Original: English

Европейская экономическая комиссия

Комитет по внутреннему транспорту

Всемирный форум для согласования правил в области транспортных средств

xxx сессия
Женева, DD–DD MM YYYY
Пункт XXX предварительной повестки дня
Проект новых Правил ООН, касающихся обновления программного обеспечения

Проект новых Правил ООН о единообразных предписаниях, касающиеся официального утверждения кибербезопасности

Представлено экспертом от xxx

Воспроизведенный ниже текст был подготовлен экспертом от xxx

I. Предложение

Проект новых Правил ООН о единообразных предписаниях, касающиеся официального утверждения системы кибербезопасности

Содержание

Стр.

1. Сфера действия
2. Определения
3. Заявка на официальное утверждение
4. Маркировка
5. Официальное утверждение
6. Свидетельство о соответствии системы обеспечения кибербезопасности (СОКИБ)
7. Технические требования
8. Модификация и распространение официального утверждения типа транспортного средства
9. Соответствие производства
10. Санкции, налагаемые за несоответствие производства
11. Названия и адреса технических служб, уполномоченных проводить испытания для официального утверждения, и органов по официальному утверждению типа

Приложения

1. Информационный документ
2. Карточка сообщения
3. Схема знака официального утверждения
4. Образец свидетельства о соответствии СОКиБ

1. Сфера действия

1.1 Настоящие правила применяются к транспортным средствам категорий [L], M, N, [O, R, S и T].

2. Определения

Для целей настоящих Правил применяются следующие определения:

2.1 «*Тип транспортного средства*» означает транспортные средства конкретной категории, не имеющие различий в отношении следующих основных аспектов:

a) изготовитель;

b) обозначение типа, используемое изготовителем;

c) основные элементы конструкции транспортного средства в отношении кибербезопасности

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

2.3 «*Система обеспечения кибербезопасности (СОКиБ)*» означает систематический подход на основе оценки риска организационных процессов, обязанностей и управления в деле смягчения последствий киберугроз и защиты транспортных средств от кибератак.

3. Заявка на официальное утверждение

3.1 Заявка на официальное утверждение типа транспортного средства в отношении кибербезопасности представляется изготовителем транспортного средства или его надлежащим образом уполномоченным представителем.

3.2 К заявке прилагаются перечисленные ниже документы в трех экземплярах и указываются следующие данные:

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 в соответствии с пунктом 6 настоящих Правил.

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.

5.2 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, не убедившись в том, что изготовитель ввел в действие удовлетворительные механизмы и процедуры, позволяющие надлежащим образом регулировать аспекты кибербезопасности, охватываемые настоящими Правилами.

5.4 Для целей пункта 7.2 настоящих Правил изготовитель обеспечивает реализацию на практике всех аспектов кибербезопасности, охватываемых настоящими Правилами.

6. Свидетельство о соответствии системы обеспечения кибербезопасности (СОКиБ)

6.1 Договаривающиеся Стороны назначают орган по официальному утверждению или техническую службу для предварительной оценки изготовителя и выдачи свидетельства о соответствии СОКиБ.

6.2 В контексте предварительной оценки изготовителя орган по официальному утверждению или техническая служба удостоверяется в том, что изготовитель ввел в действие процессы, необходимые для соблюдения всех правовых требований, которые имеют отношение к кибербезопасности в соответствии с настоящими Правилами.

6.3 После проведения этой предварительной оценки изготовителю выдают свидетельство под названием «Свидетельство о соответствии СОКиБ»,

описанное в приложении 4 к настоящим Правилам (здесь и далее свидетельство о соответствии СОКиБ).

6.4. Орган по официальному утверждению или техническая служба используетдля выдачи свидетельства о соответствии СОКиБ образец, содержащийся в приложении 4 к настоящим Правилам.

6.5 Свидетельство о соответствии СОКиБ остается действительным в течение трех лет со дня его выдачи.

6.6 Орган по официальному утверждению, который выдал свидетельство о соответствии СОКиБ, может в любое время проверить его срок действия. Свидетельство о соответствии СОКиБ может быть отменено, если требования, изложенные в настоящих Правилах, более не выполняются.

6.7 Изготовитель информирует компетентный орган по официальному утверждению или техническую службу о любом существенном изменении, которое могло бы повлиять на применимость свидетельства о соответствии СОКиБ. После консультации с изготовителем орган по официальному утверждению или техническая служба принимает решение о том, нужны ли новые проверки.

6.8 В конце срока действия свидетельства о соответствии СОКиБ орган по официальному утверждению выдает в соответствующих случаях новое свидетельство о соответствии СОКиБ или продлевает срок его действия еще на три года. Орган по официальному утверждению выдает новое свидетельство в тех случаях, когда до сведения компетентного органа по официальному утверждению или технической службы были доведены существенные изменения.

6.9 Существующие официальные утверждения типа транспортного средства не утрачивают свою годность по причине истечения срока действия свидетельства о соответствии СОКиБ, выданного изготовителю.

7. Технические требования

7.1 Общие технические требования

7.1.1 Требования настоящих Правил не ограничивают действие положений или предписаний других правил ООН.

7.1.2 Изготовитель транспортного средства может ссылаться на [рекомендации/резолюции о кибербезопасности] в своей оценке рисков и факторов уязвимости в области кибербезопасности и методов их смягчения, а также при описании используемых процессов.

7.2 Требования к системе обеспечения кибербезопасности

7.2.1 В целях предварительной оценки орган по официальному утверждению или техническая служба удостоверяется в том, что у изготовителя транспортного средства есть соответствующая система обеспечения кибербезопасноси 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 технической службе, что их система обеспечения кибербезопасности строится с учетом следующих этапов:

– этап разработки;

– этап реализации;

– этап после реализации.

7.2.2.2 Изготовитель транспортного средства подтверждает, что процессы, используемые в рамках его системы обеспечения кибербезопасности, обеспечивают надлежащий учет вопросов безопасности. Они включают следующее:

a) процессы, используемые в организации изготовителя в целях управления системой кибербезопасности;

b) процессы, используемые для выявления рисков, которым подвергаются транспортные средства;

c) процессы, используемые для оценки, классификации и устранения выявленных рисков;

d) процессы, введенные в действие с целью удостовериться, что выявленные риски устраняются надлежащим образом;

e) процессы, используемые для проверки безопасности системы на протяжении всех этапов ее разработки и реализации;

f) процессы, используемые с целью обеспечить постоянное обновление оценки рисков;

g) процессы, используемые в целях мониторинга и обнаружения кибератак на типы транспортных средств и реагирования на них;

h) процессы, используемые в целях выявления новых и возникающих киберугроз и факторов уязвимости для типов транспортных средств;

i) процессы, используемые в целях надлежащего реагирования на новые и возникающие киберугрозы и факторы уязвимости.

7.2.2.3 Изготовитель транспортного средства может ссылаться на [рекомендации/резолюции о кибербезопасности] при описании используемых им процессов.

7.2.2.4 Изготовитель транспортного средства должен показать, каким образом его система обеспечения кибербезопасности будет регулировать соответствующие аспекты взаимозависимости, которые могут существовать в его договорных отношениях с поставщиками изделий и провайдерами услуг в связи с требованиями пункта 7.2.2.2.

7.3 Требования, предъявляемые к типам транспортных средств

7.3.1 Перед оценкой типа транспортного средства для целей официального утверждения типа изготовитель транспортного средства подтверждает органу по официальному утверждению или технической службе, что его система обеспечения кибербезопасности имеет действительное свидетельство о соответствии КСиБ, имеющее отношение к данному типу транспортного средства, подлежащему официальному утверждению.

7.3.2 Орган по официальному утверждению или техническая служба удостоверяется в том, что изготовителем приняты необходимые меры, имеющие отношение к данному типу транспортного средства, в целях:

a) сбора и проверки соответствующей информации, требуемой на основании настоящих Правил, в пределах всей производственно-сбытовой цепочки;

b) поддержания соответствующей системы разработки и информации, касающейся испытаний;

c) принятия надлежащих мер безопасности применительно к конструкции транспортного средства и его систем;

7.3.3 Изготовитель транспортного средства подтверждает оценку риска для данного типа транспортного средства применительно к системам этого транспортного средства, взаимодействию различных систем этого транспортного средства и всему транспортному средству в целом.

7.3.4 Изготовитель транспортного средства показывает, каким образом обеспечивается защита важнейших конструктивных элементов транспортного средства от рисков, выявленных в ходе оценки риска изготовителем данного транспортного средства. Для защиты таких элементов принимаются соразмерные меры по смягчению их последствий.

7.3.5 Изготовитель транспортного средства показывает, каким образом он осуществляет надлежащие и соразмерные меры для защиты специальных объектов (если таковые предусмотрены) в целях хранения и реализации программного обеспечения, услуг, приложений или данных в интересах вторичного рынка.

7.3.6 Изготовитель транспортного средства описывает испытания, которые были проведены для проверки эффективности принятых мер безопасности, и результаты этих испытаний.

8. Модификация и распространение официального утверждения типа транспортного средства

8.1 Любая модификация типа транспортного средства доводится до сведения органа по официальному утверждению типа. Орган по официальному утверждению типа может:

8.1.1 либо прийти к заключению, что внесенные изменения не будут иметь значительных отрицательных последствий и что в любом случае это транспортное средство по-прежнему отвечает предписаниям;

8.1.2 либо потребовать нового протокола технической службы, уполномоченной проводить испытания.

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 типа, 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 должен обеспечить 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 типа или технической службой. Такой период не должен

превышать 10 лет, считая с момента окончательного прекращения производства.

9.1.2 Орган по официальному утверждению типа, 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 образец этого транспортного средства не соответствует требованиям настоящих Правил.

10.2 Если орган по официальному утверждению отменяет 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. Названия и адреса технических служб, уполномоченных проводить испытания для 12официального утверждения, и органов по официальному утверждению типа

11.1 Стороны Соглашения, применяющие настоящие Правила, сообщают в Секретариат Организации Объединенных Наций названия и адреса технических служб, уполномоченных проводить испытания для официального утверждения, а также органов по официальному утверждению типа, которые представляют официальное утверждение и которым надлежит направлять выдаваемые в других странах карточки, подтверждающие официальное утверждение, распространение официального утверждения, отказ в официальном утверждении или отмену официального утверждения.

Приложение 1

Информационный документ

Нижеследующая информация, если это применимо, должна представляться в трех экземплярах и включать оглавление. Любые чертежи должны иметь соответствующий масштаб, быть достаточно подробными и представляться в формате A4 или в виде складывающейся страницы формата A4. Фотографии, если таковые имеются, должны быть достаточно подробными.

0. Общие сведения

0.1 Марка (торговое наименование изготовителя):

0.2. Тип:

0.2.0.1 Шасси:

0.2.1 Коммерческое(ие) наименование(я) (если имеется(ются)):

0.3 Средства идентификации типа, если такая маркировка имеется на транспортном средстве (b):

0.3.1 Местоположение этой маркировки:

0.4 Категория транспортного средства (c):

0.8 Наименование(я) и адрес(а) сборочного(ых) завода(ов):

0.9 Наименование и адрес представителя изготовителя (если имеется):

12. ПРОЧЕЕ

12.8 Кибербезопасность

12.8.1 Общие характеристики конструкции типа транспортного средства

12.8.1.1 Схематическое изображение типа транспортного средства:

12.8.1.2 Документация на тип транспортного средства, подлежащего официальному утверждению, описывающая:

a) результаты оценки рисков для данного типа транспортного средства;

b) системы транспортных средств (как официально утвержденного типа, так и официально утвержденные безотносительно к типу), которые имеют отношение к кибербезопасности данного типа транспортного средства;

c) компоненты тех систем, которые имеют отношение к кибербезопасности;

d) взаимодействие этих систем с другими системами, относящимися к данному типу транспортного средства, и с внешними интерфейсами транспортного средства;

e) риски, которым подвергаются эти системы и которые были выявлены в ходе оценки рисков применительно к данному типу транспортного средства;

f) меры по смягчению последствий, которые были осуществлены на перечисленных системах и каким образом они позволяют устранить указанные риски;

g) какие испытания были проведены для проверки кибербезопасности данного типа транспортного средства и его систем и результаты этих испытаний.

12.8.2 Номер свидетельства о соответствии СОКиБ

Приложение 2

Карточка сообщения

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

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

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

типа транспортного средства в отношении оборудования xxx на основании Правил № **X**

Официальное утверждение №…….. .....

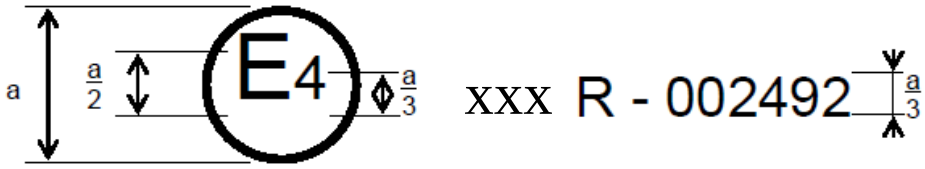
…

x.y ……

Приложение 3

Схема знака официального утверждения

Образец A
(См. пункт 4.2 настоящих Правил)



a = мин. 8 мм

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 № xxx и под номером официального утверждения 002492. Первые две цифры номера официального утверждения указывают, что официальное утверждение было предоставлено на основании предписаний Правил № xx.

Приложение 4

Образец свидетельства о соответствии СОКиБ

СВИДЕТЕЛЬСТВО О СООТВЕТСТВИИ СИСТЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ
ПРАВИЛАМ № [Правила по кибербезопасности] xxx
№ [Регистрационный номер]
[……. Орган по официальному утверждению]
удостоверяет, что

Изготовитель: .....

Адрес изготовителя: .....

соблюдает положения пункта 7 Правил № xxx

Проверки проведены (дата):

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

Номер протокола:

Свидетельство действительно до [……дата]
Совершено в [……место]
[…….дата]
[…….подпись]

Приложение B

Перечень угроз и соответствующих мер по смягчению последствий

1. Примеры, приведенные в настоящем приложении, не следует рассматривать в качестве обязательных в ходе проведения какой бы то ни было оценки той или иной системы. Настоящее приложение носит информационный характер. Это означает, что в нем приводятся примеры возможных угроз и меры по смягчению их последствий, однако их не следует рассматривать в качестве полного или подходящего руководства для всех систем или конструкций транспортных средств.

2. Настоящее приложение состоит из двух частей. В части A данного приложения описывается один из примеров уязвимости или метода атаки. В части B приложения описывается один из примеров смягчения последствий создаваемых угроз.

3. Эти примеры должны рассматриваться в надлежащих случаях изготовителями транспортных средств и соответствующими поставщиками в процессе проектирования, разработки, тестирования и реализации транспортных средств и их систем. Примеры факторов уязвимости или методов атак, описанные в части A, имеет целью оказать помощь изготовителям, поставщикам и компетентным органам в осознании угроз, например точек их проникновения или брешей в системе безопасности. Примеры смягчения последствий, изложенные в части B, призваны помочь изготовителям, поставщикам и компетентным органам в изучении возможных доступных мер по смягчению последствий в целях уменьшения рисков в случае выявленных угроз, например за счет использования соответствующих промышленных стандартов. Подробная информация о соответствующих системах смягчения последствий содержится в приложении C к настоящей рекомендации.

4. Высокий уровень уязвимости и соответствующие примеры проиндексированы в части A. Та же система индексации используется и в таблицах, содержащихся в части B, с целью увязать каждый случай атаки/фактор уязвимости с соответствующими мерами по смягчению их последствий.

5. Наряду с анализом угроз также рассматриваются возможные последствия атак. Они могут помочь установить степень риска и в то же время выявить дополнительные факторы риска. Возможные последствия атак могут включать следующее:

   - нарушение безопасной работы транспортного средства,
   - отказ некоторых функций транспортного средства,
   - модификация программного обеспечения, снижение эффективности,
   - модификация программного обеспечения, но без последствий для эксплуатации,
   - нарушение целостности данных,
   - нарушение конфиденциальности данных,
   - утрата возможности вывода данных,
   - другие, включая преступные действия.

6. По мере повышения уровня научно-технического прогресса необходимо рассматривать новые угрозы и новые меры по смягчению их последствий. Настоящее приложение, возможно, также придется

периодически обновлять, с тем чтобы его содержание отражало современное состояние этой проблемы.

Часть A. Примеры факторов уязвимости или методов атак, связанных с угрозами

1. Описание угроз и соответствующих факторов уязвимости высокого уровня или методов атаки содержится в таблице 1.

Таблица 1
Перечень примеров факторов уязвимости или методов атак, связанных с угрозами

Описание факторов уязвимости/угроз высокого уровня и подуровней			*Пример факторов уязвимости или методов атак*	
4.3.1 Угрозы в отношении внутренних серверов	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	Данные, хранящиеся на внутренних серверах, утрачены или нарушены («уязвимость» данных)	3.1	Злоупотребление привилегиями штатными сотрудниками **(внутренняя атака)**
			3.2	**Потеря информации в облаке**. В случае атаки или аварии, когда данные хранятся сторонними провайдерами услуг облачных технологий, конфиденциальные данные могут быть утеряны
			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	**Нарушение целостности информации** в результате непреднамеренного обмена данными (например, ошибки на уровне администрации, хранение данных на серверах в гаражах)
4.3.2 Угрозы в отношении транспортных средств, касающиеся их каналов передачи данных	4	Умышленное искажение сообщений или данных, полученных транспортным средством	4.1	**Умышленное искажение сообщений** методом подмены пользователя (например, 802.11p V2X в ходе формирования автоколонн, сообщения ГНСС и т. п.)
			4.2	**Атака Сибиллы** (с целью исказить сообщения, получаемые транспортными средствами, и показать, что по дороге движется как будто много транспортных средств)

Описание факторов уязвимости/угроз высокого уровня и подуровней			*Пример факторов уязвимости или методов атак*	
	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 **манипуляцию** с 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/перехват сеанса связи со **взломом**
			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	**Передача** большого количества бессмысленных **данных** в информационную систему транспортного средства, **в результате чего** нормальное **оказание услуг невозможно**
			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, 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

Описание факторов уязвимости/угроз высокого уровня и подуровней			*Пример факторов уязвимости или методов атак*	
			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 программного обеспечения 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	**Манипуляция с 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 правомерном обновлении	13.1	Атака в виде отказа в обслуживании сервера или сети с целью **воспрепятствовать обновлению важнейшего программного обеспечения** и/или разблокировки конкретных функций пользователя
4.3.4 Угрозы в отношении транспортных средств, касающиеся непреднамеренных действий человека	14	Нарушение конфигурации оборудования или систем правомерным субъектом, например владельцем или организацией технического обслуживания	14.1	**Нарушение конфигурации оборудования** организацией технического обслуживания или владельцем в процессе монтажа/ремонта/ эксплуатации, что приводит к нежелательным последствиям
			14.2	**Неправильное использование** или применение устройств и систем (включая обновления OTA)
	15	Правомерные субъекты способны принимать меры, которые могут невольно облегчить кибератаку	15.1	Невинная жертва (например, владелец, оператор или инженер по техническому обслуживанию) вводится **в заблуждение с целью вынудить его произвести соответствующее действие**, для того чтобы непреднамеренно загрузить вредоносное программное средство или дать возможность взлома
			15.2	**Заданные процедуры обеспечения безопасности** не соблюдаются
4.3.5 Угрозы в отношении транспортных средств, касающиеся взаимодействия с внешними объектами и подключения к ним	16	Манипуляция со средствами взаимодействия функций транспортного средства открывает возможность для кибератаки: это может включать средства телематики; системы, которые дают возможность осуществления дистанционных операций; и системы, использующие средства беспроводной связи ближнего радиуса действия	16.1	Манипуляция с **функциями, предназначенными для дистанционного управления такими системами,** как дистанционный ключ, иммобилизатор и уличная зарядка
			16.2	**Манипуляция со средствами телематики транспортного средства** (например, манипуляция с системой измерения температуры грузов, требующих особого обращения, дистанционного открытия 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 те из них, для которых характерен низкий уровень программного обеспечения, что используется в качестве одного из способов взлома систем транспортных средств

Описание факторов уязвимости/угроз высокого уровня и подуровней			*Пример факторов уязвимости или методов атак*	
	18	Устройства, подключенные к внешним интерфейсам, например порты USB или порты OBD, используемые в качестве одного из средств для атаки систем транспортных средств	18.1	**Внешние интерфейсы**, такие как порты USB или иные порты, используемые в качестве объекта атаки, например за счет внедрения соответствующего кода
			18.2	Программные средства инфицированы **вирусом**, занесенным в систему транспортного средства
			18.3	**Доступ для диагностического контроля (например, программные ключи, вставляемые в порт OBD)**, которые используются для облегчения взлома, например для манипуляции с параметрами транспортного средства (напрямую или опосредованно)
4.3.6 Потенциальные цели или мотивировка атаки	19	Извлечение данных/кода транспортного средства	19.1	Извлечение патентованного или собственного программного обеспечения из систем транспортного средства (**фальсификация** изделия)
			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	Манипуляция с данными/кодом	20.1	Противоправные/несанкционированные изменения в электронном свидетельстве на транспортное средство
			20.2	**Фальсификация персональных** данных. Например в том случае, если пользователь желает выдать себя за другого при передаче данных на входе систем взимания автодорожных сборов или серверное приложение изготовителя
			20.3	Действия в **обход систем мониторинга** (например, взлом/подделка/блокирование таких сообщений, как данные системы регистрации ODR или количество рейсов)
			20.4	Манипуляция с 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/манипуляция с **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

Описание факторов уязвимости/угроз высокого уровня и подуровней			*Пример факторов уязвимости или методов атак*	
	25	Манипуляция с 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 неадекватно	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 атаки** или не удовлетворяет конструктивным критериям предотвращения 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	**Чрезмерное число свободных интернет-портов**, что обеспечивает доступ к сетевым системам
			29.2	Обход **разделенных на части сетей**, что дает возможность 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 передачу произвольных сообщений на шину сети локальных контроллеров (CAN)
	30	Возможность физической утраты данных	30.1	**Ущерб**, причиненный третьей стороной. В случае ДТП или хищения конфиденциальные данные могут быть утеряны или нарушены в результате нанесения физического ущерба
			30.2	Утрата в результате коллизий на уровне **УЦР** (управление цифровыми правами). Данные пользователя могут быть удалены в случае проблем с УЦП

Описание факторов уязвимости/угроз высокого уровня и подуровней			*Пример факторов уязвимости или методов атак*	
			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)
	31	Возможность непреднамеренной передачи данных	31.1	Нарушение целостности информации. В случае **смены пользователя автомобиля** может произойти утечка частных или конфиденциальных данных (например, если автомобиль продан или используется напрокат другими лицами)
	32	Физическая манипуляция с системами, которая может создать возможность для атаки	32.1	**Манипуляция с аппаратными средствами изготовителями комплектного оборудования (OEM)**, например установка на транспортное средство несанкционированного оборудования, что создает возможность перехвата канала связи

Часть B. Примеры смягчения последствий в связи с угрозами

1. Примеры смягчения последствий применительно к «внутренним серверам»

Примеры смягчения последствий, которые связаны с «внутренними серверами», перечислены в таблице B1.

Таблица B1
Примеры смягчения последствий угроз, которые связаны с «внутренними серверами»

Таблица 1 ссылки	*Угрозы, связанные с «внутренними серверами»*	*см.*	*Смягчение последствий*
1.1 и 3.1	Злоупотребление привилегиями штатными сотрудниками (внутренняя атака)	M1	Средства защиты применяют к внутренним системам в целях сведения к минимуму риска угрозы со стороны штатных сотрудников. Примеры средств контроля защиты можно найти в проекте OWASP.
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 защиты применяют к внутренним системам в целях сведения к минимуму несанкционированного доступа. Примеры средств контроля защиты можно найти в проекте 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 личным данным или важнейшим системным данным можно с помощью соответствующей конструкции системы и контроля за доступом. Примеры средств контроля защиты можно найти в проекте OWASP.
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 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 OWASP.
3.2	Потеря информации в облаке. В случае атаки или аварии, когда данные хранятся сторонними провайдерами услуг облачных технологий, конфиденциальные данные могут быть утеряны	M4	Средства 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	Нарушение целостности информации в результате непреднамеренного обмена данными (например, ошибки на уровне администрации, хранение данных на серверах в гаражах)	M5	В целях предотвращения нарушения целостности данных к внутренним системам применяют соответствующие средства защиты. Примеры средств контроля защиты можно найти в проекте OWASP.

2. Примеры смягчения последствий в случае «каналов передачи данных транспортных средств»

Примеры смягчения последствий угроз, которые связаны с «каналами передачи данных транспортных средств», перечислены в таблице B2.

Таблица B2

Примеры смягчения последствий угроз, которые связаны с «каналами передачи данных транспортных средств»

Таблица 1 ссылка	*Угрозы, связанные с «каналами передачи данных транспортных средств»*	*см.*	*Мера по смягчению последствий*
4.1	Умышленное искажение сообщений методом подмены пользователя (например, 802.11p V2X в ходе формирования автоколонн, сообщения ГНСС и т. п.)	M10	Транспортное средство проверяет аутентичность и целостность сообщений, которые оно получает
4.2	Атака Сибиллы (с целью исказить сообщения, получаемые транспортными средствами, и показать, что по дороге движется как будто много транспортных средств)	M11	В целях хранения криптографических ключей обеспечиваются соответствующие средства защиты
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 аутентичность и целостность сообщений, которые оно получает В целях сведения рисков к минимуму защита систем обеспечивается ее конструкцией
5.2	Каналы передачи данных допускают манипуляцию бортового кода/данных транспортного средства	M7	В целях защиты данных/кода системы применяют соответствующие методы контроля за доступом и 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 аутентичность и целостность сообщений, которые оно получает
6.2	Атака/перехват сеанса связи со взломом	M10	Транспортное средство проверяет аутентичность 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	Обеспечивается защита конфиденциальных данных, которые передает и получает транспортное средство
7.2	Получение несанкционированного доступа к файлам или данным	M8	Заблокировать доступ неуполномоченному персоналу к личным данным или важнейшим системным данным можно с помощью соответствующей конструкции системы и контроля за доступом. Примеры средств контроля защиты можно найти в проекте OWASP.
8.1	Передача большого количества бессмысленных данных в информационную систему транспортного средства, в результате чего нормальное оказание услуг невозможно	M13	Применяют меры в целях выявления атаки на функцию отказа в обслуживании и восстановления системы

Таблица 1 ссылка	*Угрозы, связанные с «каналами передачи данных транспортных средств»*	*см.*	*Мера по смягчению последствий*
8.2	Атака методом переполнения, нарушение связи между транспортными средствами в результате блокировки передачи сообщений между транспортными средствами	M13	Применяют меры в целях выявления атаки на функцию отказа в обслуживании и восстановления системы
9.1	Пользователь со стороны может получить привилегированный доступ, например доступ с полномочиями суперпользователя	M9	Применяют меры в целях выявления и предотвращения несанкционированного доступа
10.1	Вирус, занесенный в коммуникационную среду, инфицирует системы транспортного средства	M14	Следует рассмотреть меры по защите систем от внедрения вирусов/вредоносных программ
11.1	Вредоносные внутренние (например, контроллерная сеть – CAN) сообщения	M15	Следует рассмотреть меры по защите систем от вредоносных внутренних сообщений или действий
11.2	Вредоносные сообщения V2X, например сообщения «объект инфраструктуры-транспортное средство» или «транспортное средство-транспортное средство» (например, CAM, DENM)	M10	Транспортное средство проверяет аутентичность 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. Примеры смягчения последствий в связи «процессом обновления»

Примеры смягчения последствий угроз, которые связаны с «процессом обновления», перечислены в таблице B3.

Таблица B3

Примеры смягчения последствий угроз, которые связаны с «процессом обновления»

Таблица 1 Ссылка	*Угрозы, связанные «Процессом обновления»*	*см.*	*Смягчение последствий*
12.1	Нарушение процедур программного обеспечения беспроводной связи. Это включает подделку программы обновления системы или встроенных программ	M16	В целях защиты программного обеспечения используются процедуры смягчения последствий
12.2	Нарушение процедур обновления локального/физического программного обеспечения. Это включает подделку программы обновления системы или встроенных программ		
12.3	Манипуляция с 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 защиты

Таблица 1 Ссылка	*Угрозы, связанные «Процессом обновления»*	*см.*	*Смягчение последствий*
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 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 OWASP.

3. Примеры смягчения последствий в случае «непреднамеренных действий человека»

Примеры смягчения последствий угроз, которые связаны с «непреднамеренными действиями человека», перечислены в таблице B4.

Таблица B4

Примеры смягчения последствий угроз, которые связаны с «непреднамеренными действиями человека»

Таблица 1 ссылка	*Угрозы в случае «непреднамеренных действий человека»*	*см.*	*Смягчение последствий*
14.1	Нарушение конфигурации оборудования организацией технического обслуживания или владельцем в процессе монтажа/ ремонта/эксплуатации, что приводит к нежелательным последствиям	M17	В целях определения и контроля процедур технического обслуживания принимают соответствующие меры
14.2	Неправильное использование или применение устройств и систем (включая обновления OTA)		
15.1	Невинная жертва (например, владелец, оператор или инженер по техническому обслуживанию) вводится в заблуждение с целью вынудить его произвести соответствующее действие, для того чтобы непреднамеренно загрузить вредоносное программное средство или дать возможность взлома	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 безопасность процедур и следят за их применением.

4. Примеры мер по смягчению последствий в случае «взаимодействия с внешними объектами и подключения к ним»

Примеры мер по смягчению последствий угроз, которые связаны с «взаимодействием с внешними объектами и подключением к ним», перечислены в таблице B5.

Таблица B5

Примеры мер по смягчению последствий угроз, которые связаны с «взаимодействием с внешними объектами и подключением к ним»

Таблица 1 ссылки	*Угрозы в случае» взаимодействия с внешними объектами»*	*см.*	*Смягчение последствий*
16.1	Манипуляция с 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 защиты.

Таблица 1 ссылки	*Угрозы в случае» взаимодействия с внешними объектами»*	*см.*	*Смягчение последствий*
16.2	Манипуляция со средствами телематики транспортного средства (например, манипуляция с системами измерения температуры грузов, требующих особого обращения, дистанционного открытия дверей грузового отделения)		
16.3	Помехи в работе систем беспроводной связи ближнего радиуса действия или датчиков		
17.1	Поврежденные приложения или те из них, для которых характерен низкий уровень защиты программного обеспечения, что используется в качестве одного из способов взлома систем транспортных средств	M21	Программное обеспечение оценивают, удостоверяют его подлинность и обеспечивают защиту его целостности. В целях сведения риска, связанного с программным обеспечением третьей стороны, которое предназначено для данного транспортного средства или которое предполагается установить на нем, применяют соответствующие средства защиты
18.1	Внешние интерфейсы, такие как USB или иные порты, используемые в качестве объекта атаки, например за счет внедрения соответствующего кода	M22	К внешним интерфейсам применяют соответствующие меры защиты
18.2	Программные средства инфицированы вирусом, занесенным в систему транспортного средства		
18.3	Доступ для диагностического контроля (например, программные ключи, вставляемые в порт OBD), которые используются для облегчения взлома, например для манипуляции с параметрами транспортного средства (напрямую или опосредованно)	M22	К внешним интерфейсам применяют соответствующие меры защиты

5. Примеры мер по смягчению последствий в случае «потенциальных целей или мотивировки атаки»

Примеры мер по смягчению последствий угроз, которые связаны с «потенциальными целями или мотивировкой атаки», перечислены в таблице B6.

Таблица B6

Примеры мер по смягчению последствий угроз, которые связаны с «потенциальными целями или мотивировкой атаки»

Таблица 1 ссылка	*Угрозы, которые связаны с «потенциальными целями или мотивировкой атаки»*	*см.*	*Смягчение последствий*
19.1	Извлечение патентованного или собственного программного обеспечения из систем транспортного средства (фальсификация изделия/хищение программного обеспечения)	M7	В целях защиты доступа к данным/коду системы применяют соответствующие средства защиты и конструктивные особенности. Примеры средств контроля защиты можно найти в проекте 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 личным данным или важнейшим системным данным можно с помощью соответствующей конструкции системы и контроля за доступом. Примеры средств контроля защиты можно найти в проекте OWASP.
19.3	Извлечение криптографических ключей	M11	В целях хранения криптографических ключей обеспечиваются соответствующие средства защиты

Таблица 1 ссылка	*Угрозы, которые связаны с «потенциальными целями или мотивировкой атаки»*	*см.*	*Смягчение последствий*
20.1	Противоправные/несанкционированные изменения в электронном свидетельстве на транспортное средство	M7	В целях защиты доступа к данным/коду системы применяют соответствующие средства защиты и конструктивные особенности. Примеры средств контроля защиты можно найти в проекте OWASP.
20.2	Фальсификация персональных данных. Например, в том случае, если пользователь желает выдать себя за другого при передаче данных на входе систем взимания автодорожных сборов или серверное приложение изготовителя		
20.3	Действия в обход систем мониторинга (например, взлом/подделка/блокирование таких сообщений, как данные системы регистрации ODR или количество рейсов)	M7	В целях защиты доступа к данным/коду системы применяют соответствующие средства защиты и конструктивные особенности. Примеры средств контроля защиты можно найти в проекте OWASP.
20.4	Манипуляция с 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/манипуляция журналов регистрации системных событий	M7	В целях защиты доступа к данным/коду системы применяют соответствующие средства защиты и конструктивные особенности. Примеры средств контроля защиты можно найти в проекте OWASP.
22.2	Внедрение вредоносного программного обеспечения или создание условий для злонамеренной работы вредоносных программ	M7	В целях защиты доступа к данным/коду системы применяют соответствующие средства защиты и конструктивные особенности. Примеры средств контроля защиты можно найти в проекте OWASP.
23.1	Фабрикация программного обеспечения системы контроля или информационной 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	Применяют меры в целях выявления атаки на функцию отказа в обслуживании и восстановления 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 доступа к данным/коду системы применяют соответствующие средства защиты и конструктивные особенности. Примеры средств контроля защиты можно найти в проекте OWASP.
25.2	Несанкционированный доступ в целях фальсификации параметров зарядки, таких как напряжение зарядки, расход энергии на подзарядку, температура батареи и т. д.		

6. Примеры мер по смягчению последствий в случае «потенциальных факторов уязвимости, которыми можно воспользоваться в случае недостаточной защиты или надежности»

Примеры мер по смягчению последствий угроз, которые связаны с «потенциальными факторами уязвимости, которыми можно воспользоваться в случае недостаточной защиты или надежности», перечислены в таблице B7.

Таблица B7

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

Таблица 1 ссылка	*Угрозы в случае «потенциальных факторов уязвимости, которыми можно воспользоваться в случае недостаточной защиты или надежности»*	*см.*	*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. Примеры средств защиты можно найти в стандарте SAE J3061
26.2	Недостаточное использование шифровальных алгоритмов для защиты чувствительных систем		
26.3	Использование криптографических алгоритмов, которые уже устарели		
27.1	Аппаратное или программное обеспечение, разработанное таким образом, что оно создает возможность атаки или не удовлетворяет конструктивным критериям предотвращения 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.
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		
29.1	Чрезмерное число свободных интернет-портов, что обеспечивает доступ к сетевым системам		
29.2	Обход разделенных на части сетей, что дает возможность 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 передачу произвольных сообщений на шину сети локальных контроллеров (CAN)	M23	В процессе разработки программного обеспечения и аппаратных средств соблюдают современные виды практики в области кибербезопасности.

7. Примеры мер по смягчению последствий в случае «потери данных/нарушения данных на транспортном средстве»

Примеры мер по смягчению последствий угроз, которые связаны с «потерей данных/нарушением данных на транспортном средстве», перечислены в таблице B8.

Таблица B8

Примеры мер по смягчению последствий угроз, которые связаны с «потерей данных/нарушением данных на транспортном средстве»

Таблица 1 ссылка	*Угрозы в случае «потери данных/нарушения данных на транспортном средстве»*	*см.*	*Смягчение последствий*
30.1	Ущерб, причиненный третьей стороной. В случае ДТП или хищения конфиденциальные данные могут быть утеряны или нарушены в результате нанесения физического ущерба	M24	В целях хранения частных и конфиденциальных данных соблюдают современные виды практики. Примеры средств защиты можно найти в стандарте 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)		
31.1	Нарушение целостности информации. В случае смены пользователя автомобиля может произойти утечка частных или конфиденциальных данных (например, если автомобиль продан или используется напрокат другими лицами)		

8. Примеры мер по смягчению последствий в случае «физической манипуляция с системами, которая может создать возможность для атаки»

Примеры мер по смягчению последствий, которые связаны с «физической манипуляцией с системами, которая может создать возможность для атаки», перечислены в таблице B9.

Таблица B9

Примеры мер по смягчению последствий, которые связаны с «физической манипуляцией с системами, которая может создать возможность для атаки»

Таблица 1 ссылка	*Угрозы в случае «физической манипуляции с системами, которая может создать возможность для атаки»*	*см.*	*Смягчение последствий*
32.1	Манипуляция с аппаратными средствами изготовителями комплектного оборудования (OEM), например установка на транспортное средство несанкционированного оборудования, что создает возможность перехвата канала связи	M9	Применяют меры по предупреждению и выявлению случаев несанкционированного доступа

Приложение C

Перечень средств защиты, связанной со смягчением последствий

1. Введение

1.1 Это приложение носит информационный характер.

1.2 Этим приложением могут пользоваться, в случае необходимости, технические службы и другие субъекты в целях оказания им помощи в понимании возможных средств защиты.

1.3 Примеры, приведенные в настоящем приложении, не следует рассматривать в качестве обязательных в ходе проведения оценки той или иной системы. Приведенные здесь примеры не обязательно носят исчерпывающий характер, который соответствовал бы всем системам или конструктивным особенностям транспортных средств.

1.4 По мере повышения уровня научно-технического прогресса необходимо рассматривать новые средства защиты. Настоящее приложение, возможно, также придется периодически обновлять, с тем чтобы его содержание отражало современное состояние научно-технического прогресса.

2. Установление связи между смягчением последствий высокого уровня, содержащихся в приложении B, и более детализированными примерами соответствующих средств защиты

2.1 В нижеследующей таблице приводится дополнительная подробная информация на примере средств защиты в случае «смягчения последствий». Перечень средств защиты в этой таблице не является исчерпывающим. Аналогичным образом применение всех перечисленных средств защиты может оказаться ненужным. Выбор будет зависеть от оценки рисков и любых юридических, договорных и нормативных требований в конкретных условиях эксплуатации интеллектуальных транспортных систем/автоматизированных систем управления.

ИД	*Смягчение последствий*	*Средства защиты, которые могут подойти, и примеры с разъяснением*
M1	В целях сведения к минимуму риска атаки штатным персоналом к серверным системам применяют соответствующие средства защиты	3.1 Политика в области безопасности 3.2 Организационная безопасность 3.3 Безопасность людских ресурсов и осведомленность в вопросах безопасности 3.4 Управление имуществом 3.5 Контроль за доступом · применение принципа двойного контроля · средства контроля за доступом на основе ролей (принцип «надо знать, «разделение обязанностей») и соответствующая подготовка сотрудников 3.6 Криптобезопасность 3.7 Физическая безопасность и защита информации от утечки 3.8 Мониторинг · занесение записей сотрудниками в журнал/ механизмы мониторинга · информационная безопасность и управление событиями 3.10 Защита программного обеспечения 3.12 Устранение инцидентов, связанных с нарушением системы защиты 3.13 Обмен информацией
M2	В целях сведения к минимуму риска несанкционированного доступа к серверным	3.5 Контроль за доступом и аутентификация 3.6 Криптобезопасность 3.7 Физическая безопасность и защита информации от утечки

ИД	*Смягчение последствий*	*Средства защиты, которые могут подойти, и примеры с разъяснением*
	системам применяют соответствующие средства защиты	3.8 Мониторинг · Мониторинг серверных систем и сообщений 3.9 Проектирование системы · надежная конфигурация серверов (например усиление защиты системы) · защита внешних выходов в Интернет, включая аутентификацию/проверку получаемых сообщений и выделение каналов связи с криптографической защитой · управление рисками и системой защиты облачных серверов (в случае использования) 3.10 Защита программного обеспечения 3.12 Устранение инцидентов, связанных с нарушением системы защиты · Информационная безопасность и управление событиями 3.13 Обмен информацией
M3	Средства 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.	3.5 Контроль за доступом · контроль за доступом сотрудников на основе ролей 3.8 Мониторинг 3.9 Проектирование системы · применение методов минимизации данных в целях уменьшения воздействия в случае потери данных · усиление защиты систем в целях сведения до минимума несанкционированного физического доступа · введение в действие соразмерной физической защиты и мониторинга 3.10 Защита программного обеспечения 3.12 Устранение инцидентов, связанных с нарушением системы защиты 3.13 Обмен информацией
M4	В целях сведения к минимуму рисков, связанных с облачной обработкой компьютерных данных, применяют соответствующие средства защиты	3.1 Политика в области безопасности 3.2 Организационная безопасность 3.3 Безопасность людских ресурсов и осведомленность в вопросах безопасности 3.4 Управление имуществом 3.5 Контроль за доступом 3.6 Криптобезопасность 3.7 Физическая безопасность и защита информации от утечки 3.8 Мониторинг · мониторинг серверных систем 3.9 проектирование системы · управление рисками и системой защиты облачных серверов · применение методов минимизации данных в целях уменьшения воздействия в случае потери данных 3.10 Защита программного обеспечения 3.11 Безопасные взаимоотношения с поставщиками 3.12 Устранение инцидентов, связанных с нарушением системы защиты · информационная безопасность и управление событиями 3.13 Обмен информацией
M5	В целях предотвращения нарушения целостности данных к внутренним системам применяют соответствующие средства защиты	3.1 Политика в области безопасности 3.2 Организационная безопасность 3.3 Безопасность людских ресурсов и осведомленность в вопросах безопасности · надлежащие процедуры организации, передачи и утилизации массивов данных · соответствующая подготовка сотрудников, в особенности тех, которые занимаются обработкой массивов данных 3.4 Управление имуществом 3.5 Контроль за доступом 3.6 Криптобезопасность 3.7 Физическая безопасность и защита информации от утечки 3.8 Мониторинг 3.9 Проектирование системы · применение методов минимизации и целевого ограничения данных в порядке снижения воздействия в случае потери данных 3.10 Защита программного обеспечения 3.12 Устранение инцидентов, связанных с нарушением системы защиты 3.13 Обмен информацией

ИД	*Смягчение последствий*	*Средства защиты, которые могут подойти, и примеры с разъяснением*
M6	В целях сведения к минимуму воздействия атаки на транспортное средство применяют соответствующий принцип безопасности на этапе проектирования	3.1 Политика в области безопасности 3.5 Контроль за доступом · процедуры контроля за доступом и считыванием/записью, установленные для файлов и данных транспортного средства 3.6 Криптобезопасность 3.7 Физическая безопасность и защита информации от утечки 3.8 Мониторинг · мониторинг системы 3.9 Проектирование системы · проверка целостности и аутентификации сообщения · например усиление защиты систем · защита активной памяти · сегментация сети и определение пределов доверия 3.10 Защита программного обеспечения · методы проверки целостности программного обеспечения 3.12 Устранение инцидентов, связанных с нарушением системы защиты 3.13 Обмен информацией
M7	В целях защиты данных/кода системы применяют соответствующие методы контроля за доступом и соответствующие конструктивные особенности	3.5 Контроль за доступом · процедуры контроля за доступом и считыванием/записью, установленные для файлов и данных транспортного средства 3.6 Криптобезопасность 3.7 Физическая безопасность и защита информации от утечки 3.8 Мониторинг · мониторинг системы 3.9 Проектирование системы · защита активной памяти · сегментация сети и определение пределов доверия · подтверждение ввода сигнала на основе приложения (с точки зрения вида данных/сигнала, ожидаемых приложением) · безопасное хранение конфиденциальной информации 3.10 Защита программного обеспечения · методы проверки целостности программного обеспечения · проверка программного обеспечения 3.12 Устранение инцидентов, связанных с нарушением системы защиты 3.13 Обмен информацией
M8	Разработка системы и контроля за доступом должна исключать возможность несанкционированного доступа к личным данным или важнейшим данным системы.	3.5 Контроль за доступом · контроль за доступом на основе ролей 3.6 Криптобезопасность 3.8 Мониторинг 3.9 Проектирование системы · усиление защиты систем в целях сведения до минимума и предотвращения несанкционированного доступа · введение в действие соразмерной физической защиты и мониторинга 3.10 Защита программного обеспечения 3.13 Обмен информацией
M9	Применяют меры по предупреждению и выявлению случаев несанкционированного доступа	3.5 Контроль за доступом · многофакторная аутентификация приложений, предусматривающих доступ с полномочиями суперпользователя · применение принципа «наименьшей привилегии доступа», например, за счет разделения административных счетов 3.8 Мониторинг · мониторинг системы 3.9 Проектирование системы · введение в действие принципа пределов доверия и контроля за доступом · недопущение однотипной сети (применение глубокоэшелонированной защиты и принципа разделения сетей) 3.10 Защита программного обеспечения 3.13 Обмен информацией
M10	Транспортное средство проверяет подлинность и целостность сообщений, которые оно получает	3.5 Контроль за доступом · процедуры контроля за доступом и считыванием/записью, установленные для файлов и данных транспортного средства 3.6 Криптографическая защита · шифрование сообщений, содержащих конфиденциальные данные

ИД	*Смягчение последствий*	*Средства защиты, которые могут подойти, и примеры с разъяснением*
		3.8 Мониторинг · мониторинг системы · ограничение и мониторинг сообщений и протоколов 3.9 Проектирование системы · аутентификация сообщения для всех полученных сообщений · проверка целостности сообщения и аутентификация · проверки последовательности с использованием других датчиков транспортного средства (например датчик температуры, радар…) · использование методов проверки целостности, таких как хеширование, надежные протоколы и фильтрация пакетов · использование методов защиты от атак с повторным навязыванием сообщения, таких как отметки времени или использование свойства новизны ключа · принципы управления сеансом во избежание перехвата сеанса · усиление защиты операционной системы · защита активной памяти · использование сочетания шлюзов, аппаратных средств сетевой защиты, механизмов отражения или выявления угроз и мониторинг в целях защиты систем · сегментация сети и определение пределов доверия 3.10 Защита программного обеспечения · методы проверки целостности программного обеспечения 3.13 Обмен информацией
M11	В целях хранения криптографических ключей обеспечиваются соответствующие средства защиты	3.6 Криптобезопасность · активное применение и обеспечение защиты криптографических ключей · рассмотрение возможности использования модуля аппаратной защиты (HSM), системы обнаружения попыток взлома и методы аутентификации устройств в целях снижения уязвимости
M12	Конфиденциальные данные, передаваемые на транспортное средство или транспортным средством подлежат соответствующей защите	3.6 Криптобезопасность · шифрование сообщений, содержащих конфиденциальные данные 3.9 Проектирование системы · применение методов минимизации данных к сообщениям 3.10 Защита программного обеспечения · проверка на уязвимость программного обеспечения и систем, используемых для защиты конфиденциальной информации
M13	Принимают меры по выявлению атаки на функцию отказа в обслуживании и восстановлению системы	3.8 Мониторинг 3.9 Проектирование системы · проверка соответствия объема получаемых данных ожидаемым значениям · аутентификация данных · присвоение метки времени сообщениям и установка истечения времени, отведенного на сообщения · применение мер по ограничению скорости передачи в зависимости от контекста · установить функцию подтверждения сообщения для сообщений V2X (в настоящее время не стандартизована) · резервная стратегия в случае потери связи 3.10 Защита программного обеспечения 3.12 Устранение инцидентов, связанных с нарушением системы защиты 3.13 Обмен информацией
M14	Меры по защите от внедренных вирусов/вредоносных программ подлежат рассмотрению	3.8 Мониторинг · мониторинг системы 3.9 Проектирование системы · аутентификация сообщения и проверка целостности · подтверждение ввода для всех сообщений · определение пределов доверия и контроль за доступом · недопущение однотипной сети (применение глубокоэшелонированной защиты и принципа разделения сетей) 3.10 Защита программного обеспечения 3.12 Устранение инцидентов, связанных с нарушением системы защиты 3.13 Обмен информацией

ИД	*Смягчение последствий*	*Средства защиты, которые могут подойти, и примеры с разъяснением*
M15	Меры по выявлению злонамеренных внутренних сообщений или деятельности подлежат рассмотрению	3.8 Мониторинг · мониторинг системы 3.9 Проектирование системы · аутентификация сообщения и проверка целостности · подтверждение ввода для всех сообщений · определение пределов доверия и контроль за доступом · недопущение однотипной сети (применение глубокоэшелонированной защиты, изоляции компонентов и принципа разделения сетей) 3.10 Защита программного обеспечения 3.12 Устранение инцидентов, связанных с нарушением системы защиты 3.13 Обмен информацией
M16	В целях защиты программного обеспечения используются процедуры смягчения последствий	3.6 Криптобезопасность · эффективное применение ключей и защита любых используемых методов криптографии 3.8 Мониторинг 3.9 Проектирование системы 3.10 Защита программного обеспечения · введение в действие надежных процедур, включая конфигурацию шаблонов и соответствующие принципы · использование надежной связи в целях обновления · обеспечение достоверности обновлений · версия и временная метка внесения обновлений · обеспечение криптографической защиты и подтверждение обновлений программного обеспечения · обеспечение контроля конфигурации и возможности отмены обновлений 3.13 Обмен информацией
M17	В целях определения и контроля процедур технического обслуживания принимаются соответствующие меры	3.3 Безопасность людских ресурсов и осведомленность в вопросах безопасности · надлежащая подготовка технического персонала 3.8 Мониторинг 3.9 Проектирование системы · обеспечение использования системы конфигурации шаблонов и соответствующих принципов · обязательная проверка конфигураций · допуск только безопасного комплекта инструкций на борту транспортного средства · применение методов аутентификации сообщений и устройств · введение в действие надлежащих средств контроля данных 3.10 Защита программного обеспечения 3.12 Устранение инцидентов, связанных с нарушением системы защиты 3.13 Обмен информацией
M18	В целях определения и контроля ролей и привилегий, касающихся доступа на основе принципа наименьшей привилегии, принимаются соответствующие меры	3.1 Политика в области безопасности 3.2 Организационная безопасность 3.3 Безопасность людских ресурсов и осведомленность в вопросах безопасности 3.4 Управление имуществом 3.5 Контроль за доступом и аутентификация
M19	Организации обеспечивают безопасность процедур и следят за их применением	3.1 Политика в области безопасности 3.2 Организационная безопасность 3.3 Безопасность людских ресурсов и осведомленность в вопросах безопасности · наличие соответствующей программы безопасности, определяющей процедуры · налаживание процесса разработки и технического обслуживания системы безопасности на этапах пересмотра, перекрестной проверки и утверждения шлюзов/этапов · определение потребностей в подготовке сотрудников по вопросам ознакомления с конкретными аспектами информационного пространства и безопасности применительно к их роли, особенно тех, на кого возложены функции разработки и инженерного сопровождения, и последующее удовлетворение этих потребностей

ИД	*Смягчение последствий*	*Средства защиты, которые могут подойти, и примеры с разъяснением*
M20	В случае систем, оснащенных функцией дистанционного доступа, применяют соответствующие средства защиты	3.5 Контроль за доступом · права на контроль за доступом, установленные и осуществляемые применительно к дистанционным системам транспортного средства 3.8 Мониторинг · мониторинг системы на предмет неожиданных сообщений/поведения 3.9 Проектирование системы · применение методов аутентификации сообщений и устройств · допуск только безопасного комплекта инструкций на борту транспортного средства · использование методов проверки целостности, таких как хеширование, надежные протоколы и фильтрация пакетов · использование методов защиты от атак с повторным навязыванием сообщения, таких как отметки времени или использование свойства новизны ключа · применение принципа разделения сети 3.10 Защита программного обеспечения · проверка программного обеспечения и аппаратных средств в целях снижения уязвимости 3.12 Устранение инцидентов, связанных с нарушением системы защиты 3.13 Обмен информацией
M21	Программное обеспечение оценивают, удостоверяют его подлинность и обеспечивают защиту его целостности	3.8 Мониторинг 3.9 Проектирование системы 3.10 Защита программного обеспечения 3.13 Обмен информацией
M22	К внешним интерфейсам применяют соответствующие средства защиты	3.8 Мониторинг · мониторинг системы на предмет неожиданных сообщений/поведения 3.9 Проектирование системы · применение методов аутентификации сообщений и устройств · допуск только безопасного комплекта инструкций на борту транспортного средства · обеспечение систем защиты границ и контроля за доступом между внешними интерфейсами и системами других транспортных средств · усиление защиты систем в целях ограничения доступа 3.10 Защита программного обеспечения 3.12 Устранение инцидентов, связанных с нарушением системы защиты 3.13 Обмен информацией
M23	В процессе разработки программного обеспечения и аппаратных средств соблюдают современные виды практики в области кибербезопасности	3.2 Организационная безопасность · наличие активной программы выявления важнейших факторов уязвимости · организационный план с указанием способов поддержания безопасности в течение всего срока эксплуатации систем 3.6 Криптобезопасность 3.7 Физическая безопасность и защита информации от утечки 3.9 Проектирование системы · применение надежной практики кодирования для разделения сети · оценка рисков в вопросах безопасности и надлежащее и соразмерное управление ими, в том числе теми, которые специфичны для производственно-сбытовой цепочки · надежные методологии проектирования, включая гарантии того, что требования к конструктивным особенностям сети будут удовлетворены в результате соответствующей реализации 3.10 Защита программного обеспечения · шифрование кода программного обеспечения · прием только тех заявлений на получение разрешения, которые обеспечивают приемлемый уровень проверки программного обеспечения в части снижения уязвимости · программное обеспечение и его конфигурации подлежат оценке с точки зрения безопасности, аутентификации и защиты целостности 3.11 Безопасные взаимоотношения с поставщиками · возможность убедиться и подтвердить аутентичность и происхождение поставок · организации, включая поставщиков, в состоянии гарантировать их процессы и продукты, связанные с безопасностью

ИД	*Смягчение последствий*	*Средства защиты, которые могут подойти, и примеры с разъяснением*
		3.13 Обмен информацией
M24	В целях хранения частных и конфиденциальных данных соблюдают современные виды практики	3.6 Криптобезопасность 83. Мониторинг 3.9 Проектирование системы · системы должны быть разработаны таким образом, чтобы конечные пользователи могли иметь эффективный и надлежащий доступ к своим персональным данным, стирать их и обращаться с ними по своему усмотрению · необходимость разработки мер с целью обеспечить надежное стирание данных пользователя после перехода прав собственности 3.10 Защита программного обеспечения 3.13 Обмен информацией
M25	Системы следует проектировать таким образом, чтобы они надлежащим образом реагировали в случае выявления атаки на транспортное средство.	3.8 Мониторинг 3.9 Проектирование системы · оценка рисков в вопросах безопасности и надлежащее и соразмерное управление ими · наличие встроенной функции дублирования или создания резервных копий в случае сбоев в работе системы · важнейшие системы безопасности должны сохранять надежность при отказах · рекомендуются меры по обеспечению доступности данных 3.10 Защита программного обеспечения 3.12 Устранение инцидентов, связанных с нарушением системы защиты 3.13 Обмен информацией

3. Дополнительная информация по средствам защиты

В нижеследующем разделе содержится дополнительная детализированная информация или соображения, касающиеся примеров средств защиты, которые содержатся в вышеупомянутой таблице.

Выбор соответствующих средств защиты и применение содержащегося здесь руководства будет зависеть от конструкции транспортного средства, которая определяется данным типом транспортного средства, оценки присущего ему риска и любых уместных правовых, договорных или нормативных факторов.

3.1 Политика в области безопасности

3.1.1 В этой связи можно воспользоваться Руководством по политике в области безопасности, определенной в стандарте ISO/SAE 21434.

3.1.2 Можно также воспользоваться нижеследующими вариантами:

Политика в области кибербезопасности определяется и утверждается руководством и доводится до сведения работников

Действующая политика подлежит пересмотру через запланированные интервалы времени или в том случае, когда происходят существенные изменения, которые предполагают необходимость учета их целесообразности, адекватности и эффективности.

3.2 Организационная безопасность

В этом случае можно использовать следующие варианты:

Роли и обязанности в области кибербезопасности подлежат определению и распределению

Разделение функций с целью сузить возможности несанкционированного/непреднамеренного изменения/неправильного использования имущества организации

В случае таких мероприятий, как устранение инцидентов, связанных с нарушением системы защиты, устанавливают надлежащий контакт с соответствующими органами

В целях эффективного управления базой знаний в области кибербезопасности устанавливают контакты со специализированными группами, форумами специалистов по проблемам безопасности и профессиональными ассоциациями

3.3 Безопасность людских ресурсов и осведомленность в вопросах безопасности

3.3.1 В этом случае можно использовать следующие варианты:

Определение потребностей в подготовке сотрудников по конкретным проблемам информационных технологий и безопасности в зависимости от их роли, особенно тех, на кого возложены функции разработки и инженерного сопровождения, и последующего удовлетворения этих потребностей

Наличие соответствующей программы безопасности, определяющей процедуры

Соответствующая подготовка сотрудников, в особенности тех, которые занимаются обработкой массивов данных

Надлежащая подготовка технического персонала

Механизмы регистрации/мониторинга операций сотрудников

Налаживание процесса разработки и технического обслуживания системы безопасности на этапах пересмотра, перекрестной проверки и утверждения шлюзов/этапов.

3.3.2 Конкретные вопросы, связанные с «вариантами завершения срока службы»:

Надлежащие процедуры организации, передачи и утилизации массивов данных

Разработка мер с целью обеспечить надежное стирание данных пользователя после перехода прав собственности

3.4 Управление имуществом

3.4.1 В этом случае можно использовать следующие варианты:

Имущество, связанное с системами транспортного средства, следует идентифицировать, а соответствующий перечень этого имущества следует составить и вести на постоянной основе.

Имущество, содержащееся в этом перечне, должно принадлежать на праве собственности.

Правила приемлемого использования этих систем транспортных средств и соответствующего имущества, связанного с данными системами транспортных средств, следует идентифицировать, оформлять документально и выполнять.

Когда необходимости в этом имуществе больше нет, от него следует избавляться, используя в этих целях официальные процедуры.

3.5 Контроль за доступом

3.5.1 В этом случае можно использовать следующие варианты:

3.5.1.1 Вопросы, имеющие отношение к «механизмам контроля за доступом»

– Определение пределов доверия и контроль за доступом

– Применение принципа наименьшей привилегии в целях сведения риска до минимума

– Введение в действие средств контроля за доступом на основе ролей (принцип «надо знать», «разделение обязанностей»)

– Процедуры контроля за доступом и считыванием/записью, установленные для файлов и данных транспортного средства

– Права на контроль за доступом, установленные и осуществляемые применительно к дистанционным системам транспортного средства

– Обеспечение систем защиты границ и контроля за доступом между внешними интерфейсами и системами других транспортных средств

– Обеспечение систем защиты границ и контроля за доступом между собственным программным обеспечением (приложениями) и системами Других транспортных средств

– Принцип двойного контроля

– Многофакторная аутентификация приложений, предусматривающих доступ с полномочиями суперпользователя

– Контроль за доступом к системе и приложениям

a) Ограничение на доступ к информации

b) Безопасные процедуры входа в систему

c) Система использования пароля для пользователей/водителей

d) Использование привилегированных вспомогательных программ

f) Контроль за доступом к исходному коду транспортного средства

3.5.1.2 Вопросы, имеющие отношение к «аутентификации устройств и приложений»

– Применение методов аутентификации устройств

– Аутентификация устройств и оборудования

– Обязательная проверка конфигураций

– Разработка процедур, определяющих те прикладные программы, которые допускаются, что они могут делать и при каких условиях

3.5.1.3 Вопросы, имеющие отношение к «разрешению»

– Обеспечение наличия соответствующих механизмов разрешения в случае ролей, предусматривающих доступ к транспортному средству

– Обеспечение четкого определения бортовым приложением типов пользователей и соответствующих прав этих пользователей

– Обеспечение наличия действующего положения, предусматривающего наименьшую привилегию

– Обеспечение надлежащей работы механизмов разрешения, их надежной работы в случае сбоя и отсутствия возможности обойти защиту

3.6 Криптобезопасность

3.6.1 В этом случае можно использовать следующие варианты:

3.6.1.1 Вопросы, имеющие отношение к «использованию криптографических ключей»

– Активное применение и защита криптографических ключей

– Эффективное применение ключей и защита любых используемых методов криптографии

3.6.1.2 Вопросы, имеющие отношение к «шифрованию сообщений и программного обеспечения»

– Шифрование сообщений, содержащих конфиденциальные данные, включая обновление программного обеспечения

– Шифрование кода программного обеспечения

– Исключение возможности передачи конфиденциальных данных открытым текстом как по внутренним, так и по внешним каналам

– Обеспечение использования приложением известных методов эффективного шифрования

3.7 Физическая безопасность и защита информации от утечки

3.7.1 Дополнительные вопросы не определены.

3.8 Мониторинг

3.8.1 В случае мониторинга можно применять руководство по мониторингу в условиях эксплуатации, указанное в стандарте ISO/SAE 21434.

3.8.2 В этом случае можно использовать следующие варианты:

– Мониторинг системы на предмет неожиданных сообщений/поведения

– Введение в действие соразмерной физической защиты и мониторинг

– Мониторинг серверных систем и сообщений

– Системы обнаружения имитации датчика и реагирования на нее

– Принципы управления сеансом во избежание его перехвата

– Защита от программ, нарушающих работу системы

– Вход в систему и мониторинг

– Контроль за работой оперативного программного обеспечения

– Соображения, касающиеся аудиторской проверки информационных систем

3.9 Проектирование системы

3.9.1 В этом случае можно использовать следующие варианты:

3.9.1.1 Вопросы, имеющие отношение к «проектированию сети»

– Недопущение однотипной сети (применение глубокоэшелонированной защиты и принципа разделения сетей)

– Сегментация сети и определение пределов доверия

– Защита внешних выходов в Интернет, включая аутентификацию/проверку получаемых сообщений и выделение каналов связи с криптографической защитой

– Использование программы «песочница» в целях защиты при выполнении чужой программы

– Использование сочетания шлюзов, аппаратных средств сетевой защиты, механизмов отражения или выявления угроз и мониторинг в целях защиты систем

– Обеспечение аутентификации всех внутренних и внешних подключений (пользователь и объект) в соответствующей и надлежащей форме; при этом следует убедиться в том, что этот контроль невозможно обойти

– Исключение возможности отображения сообщения, подтверждающего аутентификацию, в форме открытого текста.

3.9.1.2 Вопросы, имеющие отношение к «контролю данных, хранящихся на транспортных средствах и серверах и передаваемых ими»

а) Общие положения

– Введение в действие надлежащих средств контроля данных

– Исключение возможности нарушения конфиденциальной информации

– Применение методов минимизации и целевого ограничения данных в применение методов минимизации данных к сообщениям

– Методы минимизации данных, применяемые к сообщениям

– Необходимость разработки систем таким образом, чтобы конечные пользователи могли иметь эффективный и надлежащий доступ к своим персональным данным, стирать их и обращаться с ними по своему усмотрению

– Применение соответствующих методов в целях предотвращения злонамеренной манипуляции с важнейшими системными данными

– Применение строгих письменных разрешений и мер аутентификации по обновлению параметров транспортного средства и доступа к ним

– Обязательная установка надежного флажка, препятствующего случайной передаче данных в сеть транспортного средства

b) Использование криптографии

– Разработка и реализация принципов использования криптографического контроля в целях защиты информации. Она включает идентификацию данных, которые сохраняются и нуждаются в соответствующей защите,

– Обеспечение безопасного хранения конфиденциальной информации

– Шифрование конфиденциальных данных и надлежащее и безопасное использование ключей

– Использование системы активной защиты памяти

– Рассмотрение возможности использования модуля аппаратной защиты (HSM), системы обнаружения попыток взлома и методы аутентификации устройств в целях снижения уязвимости

c) Аутентификация

– Следить за тем, чтобы в тех случаях, когда передается подтверждение аутентификации или иной конфиденциальной информации, эта информация принималась только с использованием защищенных информационных протоколов и каналов по коммуникационному каналу транспортного средства

– Обеспечивать, чтобы при передаче всех страниц соблюдалось требование, предусматривающее аутентификацию конфиденциальной информации

d) Файлы куки

– Следить за тем, чтобы во всех ли случаях перехода состояния в коде данного приложения должным образом проверялись файлы куки и обеспечивалось их использование

– Исключать возможность несанкционированных действий за счет манипулирования файла куки

– Убедиться в том, что файлы куки содержат как можно меньше частной (пользователь/водитель) информации

– Обеспечивать шифрование всего файла куки в том случае, если в нем все же остается конфиденциальная информация

– Определять все файлы куки, которые используются данным приложением, их названия и причину, по которой они нужны

e) Подтверждение данных

– Убедиться в том, что данные сеанса подтверждаются

– Убедиться в наличии механизма подтверждения данных

– Убедиться в том, что все входные сигналы, которые могут (и будут) изменены злонамеренным пользователем, такие как HTTP-заголовки, поля с входными данными, скрытые поля, выпадающие списки и другие веб-компоненты, подтверждены должным образом

– Убедиться в наличии надлежащего контроля с продольным ходом всех входных данных

– Убедиться в подтверждении всех полей, файлов куки, HTTP-заголовков/тел и полей формы

– Убедиться в том, что данные хорошо сформированы и содержат, по возможности, только известные надежные сим

– Убедиться в том, что подтверждение данных производится со стороны сервера

– Проверить, где производится подтверждение данных, и используется ли централизованная или децентрализованная модель

– Убедиться в отсутствии в модели подтверждения данных соответствующих вариантов обхода,

– Золотое правило: все внешние сигналы независимо от их характера проверяются и подтверждаются

3.9.1.3 Вопросы, имеющие отношение к «контролю сообщений»

a) Допуск только безопасного комплекта инструкций на борту транспортного средства

b) Аутентификация сообщения и проверка целостности

– Аутентификация данных

– Проверка соответствия объема получаемых данных ожидаемым значениям

– Ограничение и мониторинг сообщений и протоколов,

– Применение мер по ограничению скорости передачи в зависимости от контекста

– Подтверждение ввода для всех сообщений

c) Подтверждение ввода сигнала на основе приложения (с точки зрения вида данных/сигнала, ожидаемых приложением

d) Проверки последовательности с использованием других датчиков транспортного средства (например, датчик температуры, радар…)

e) Определение сообщений подтверждения для сообщений V2X (в настоящее время не стандартизованы)

f) Использование методов защиты от атак с повторным навязыванием сообщения, таких как отметки времени или использование свойства новизны

g) Присвоение метки времени сообщениям и установка истечения времени, отведенного на сообщения

h) В тех случаях, когда осуществляется передача подтверждения аутентификации или иной конфиденциальной информации, эту информацию необходимо принимать только с использованием метода HTTP «POST» и не использовать метод HTTP «GET»

i) Любую страницу, которая, по мнению предприятия или группы по разработке, не вписывается в сферу аутентификации, следует пересматривать с целью оценить возможность нарушения безопасности

3.10 Безопасность программного обеспечения системы – приобретение, разработка и техническое обслуживание

3.10.1 В этом случае возможны следующие варианты:

– Обеспечивать использование надежной связи в целях обновления

– Обеспечивать криптографическую защиту и подтверждать обновления программного обеспечения

– Вводить в действие надежные процедуры, включая конфигурацию шаблонов и соответствующие принципы

– Обеспечивать контроль конфигурации и возможности отмены обновлений

– Версия и временна́я метка внесения обновлений

– Обеспечивать достоверность обновлений

– Вводить в действие надежные процедуры обновления, включая конфигурацию шаблонов и соответствующие принципы обновления

– В случае обновлений прикладные программы следует пересматривать и проверять с целью убедиться в отсутствии отрицательного воздействия на безопасность транспортного средства и организацию.

3.10.1.1 Вопросы, имеющие отношение к «разработке безопасного программного обеспечения»

a) Применение надежных видов практики кодирования

– Обеспечивать отсутствие в коде готовых приложений возможности разработки/отладки средств системы защиты

– Обеспечивать отсутствие возможности возврата системных ошибок на запрос пользователя/водителя/ЧМИ

– Обеспечивать наличие соответствующей позиции по умолчанию во всех логических решениях

– Обеспечивать отсутствие в скомпонованных каталогах инструментов, которыми можно воспользоваться в среде разработки

– Управление памятью

– Проверка вводимых данных

– Кодирование выхода

– Предотвращение модификации кода

b) Обработка ошибок

– Обработка ошибок, исключительных ситуаций и регистрация

– Убедиться в том, что сбой в работе приложения не приводит к нарушению безопасности и что на случай сбоя есть соответствующие варианты избыточности

– Обеспечивать высвобождение ресурсов в случае ошибки

– Исключать возможность ввода конфиденциальной информации в случае ошибки

– Производить поиск любых запросов, адресованных базовой операционной системе, или запросов на открытие файла и анализировать возможности ошибки

– Обеспечивать регистрацию ошибок приложения

c) Применять методы тестирования программного обеспечения и проверки целостности

– Проверять приложение по регистрации отладки в целях регистрации конфиденциальных данных

– Проверять структуру файла на предмет наличия каких-либо компонентов, которые не должны быть доступны напрямую, но которыми может воспользоваться пользователь

– Проверять все случаи распределения/объединения памяти

– Проверять приложение динамического SQL и выяснять, не подвержено ли оно атаке методом внедрения

– Искать закомментированный код (закоментированный код тестирования), который может содержать конфиденциальную информацию

d) Управление сеансом

– Проверять возможность аннулирования сеанса

– Проверять каким образом и когда создан сеанс пользователя и каким образом он оказался неудостоверенным или удостоверенным

– Проверять идентификатор сеанса связи (ИД) с целью выяснить, достаточно ли он сложен и позволяет ли он удовлетворять установленным требованиям с точки зрения надежности

– Определять действия, которые заложены в приложении, в случае неудостоверенного ИД

– Определять, каким образом осуществляется управление в условиях многопотоковой/многопользовательской среды

– Определять время ожидания в режиме простоя сеанса HTTP

– Определять, как реализуются функциональные возможности в случае завершения сеанса

3.10.1.2 Вопросы, имеющие отношение к «тестированию программного обеспечения с защищенным доступом»

– Тестирование функциональных возможностей следует проводить в процессе разработки

– В случае новых систем, обновлений и версий программного обеспечения следует разработать соответствующие параметры утверждения программ тестирования и связанные с ними критерии.

3.11 Безопасные взаимоотношения с поставщиками

3.11.1 В этой связи можно воспользоваться Руководством по политике в области разработки распределенных приложений, указанной в стандарте ISO/SAE 21434.

3.11.2 В этом случае возможны также следующие варианты:

– Требования к кибербезопасности в целях смягчения рисков, связанных с изделиями/системой поставщика, для изделий/системы изготовителей согласуются с поставщиком и оформляются документально

– Все требования к кибербезопасности разрабатываются и согласуются с каждым поставщиком, который может получить доступ, обрабатывать, хранить, передавать или предоставлять соответствующие компоненты инфраструктуры для изготовителей

– Соглашения с поставщиками включают требования, касающиеся устранения рисков, связанных с услугами и продуктами информационно-коммуникационной технологии в рамках производственно-сбытовой цепочки

– Изготовитель осуществляет регулярный мониторинг, ревизию и аудиторскую проверку работы поставщика по оказанию ему своих услуг

– Изменения в системе оказания услуг поставщиками, включая техническое обслуживание и совершенствование существующей политики, процедур и средств контроля в области кибербезопасности, регламентируются с учетом важности деловой информации, систем, компонентов и задействованных процессов, а также повторной оценки рисков

3.12 Устранение инцидентов, связанных с нарушением системы защиты

3.12.1 В этой связи можно воспользоваться Руководством по устранению инцидентов, связанных с нарушением системы киберзащиты транспортных средств, указанным в стандарте ISO/SAE 21434.

3.12.1 В данном случае возможны также следующие варианты:

– В целях обеспечения оперативного, эффективного и упорядоченного реагирования на инциденты, связанные с нарушением системы защиты, необходимо разработать соответствующие управленческие обязанности и процедуры.

– Инциденты, связанные с нарушением системы защиты, следует доводить до сведения по соответствующим каналам управления как можно скорее.

3.13 Обмен информацией

3.13.1 Руководство по структурированному обмену информацией можно найти в серии ITU-T X.1500 под названием «Structured Cybersecurity Information Exchange (CYBEX) Techniques»

3.13.2 ниже указаны ссылки из серии ITU-T X.1500, которые можно использовать для структурированного обмена информацией в целях укрепления системы киберзащиты посредством согласованного, всестороннего, глобального, своевременного и надежного обмена информацией, касающейся факторов уязвимости, слабых мест, характера атак и т. п.:

– X.1520 Общеизвестные уязвимости и незащищенность (CVE)

– X.1521 Система оценки общеизвестных уязвимостей (CVSS)

– X.1524 Перечень общеизвестных слабых мест (CWE)

– X.1525 Система оценки слабых мести (CWSS)

– X.1544 Перечень и классификация характеристик общеизвестных схем атак (CAPEC)

Приложение D

Перечень справочных документов

Нижеприведенный перечень содержит ссылки на документы, которые были положены в основу и использованы для подготовки настоящего документа:

ENISA report «Cyber Security and Resilience of Smart Cars»	TFCS-03-09
UK DfT Cyber Security principles	TFCS-03-07
NHTSA Cyber Security Guideline	TFCS-03-08
IPA «Approaches for Vehicle Information Security» (Япония)	TFCS-04-05
Руководящие положения ЕЭК ООН о кибербезопасности и защите данных (ИТС/АВ)	ECE/TRANS/WP.292017/46

SAE J 3061

ISO/SAE 21434 Road vehicles – Cybersecurity Engineering (на стадии разработки)

ISO/IEC 19790

ISO/IEC 27000 series

ISO/IEC 26262

ISO/IEC 19790 «Security requirements for cryptographic modules»

US Auto ISAC (report by Booz Allen Hamilton) https://www.automotiveisac.com/best-practices/

«OWASP»

GSMA CLP.11 IoT security guidelines and CLP.17 IoT Security Assessment